FERRET V5.0

OpenVMS Security Manager
by Saiga Systems Software Inc.

Quick links:

Saiga Systems

#913, 105 - 150 Crowfoot Crescent NW
Calgary, Alberta, Canada
T3G 3T2

Technical Support

North America	(866) 573-8182
International	(403) 248-2004
E-mail	support@saiga.com

All Other Departments

North America	(800) 561-8876
International	(403) 263-1151
Fax	(403) 263-0744
E-mail	sales@saiga.com

WWW	http://www.saiga.com/
Listserver	cohort@saiga.com

June 1, 2004

The information in this document is subject to change without notice and should not be construed as a commitment by Saiga Systems Inc. Saiga Systems Inc. assumes no responsibility for any errors or omissions that may appear in this document.

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

Copyright © 2004 by Saiga Systems Inc.
All rights reserved

DEC, DECNET, VAX, OpenVMS, Alpha AXP and VAXCLUSTER are trademarks of Compaq.

Table of Contents

Using FERRET to manage your system security

This chapter shows you how FERRET can help you tighten security by controlling your user authorization file. FERRET helps you pinpoint potential security and resource problems, highlight changes to your UAF, audit your UAF and update fields when new software requires changes to many accounts. It helps you do your job better and makes your life easier.

Here are 11 ways FERRET can help you:

- Audit your UAF for security or performance problems
- Highlight differences between one node's UAF and another
- Detect accounts with excessive numbers of login failures
- Detect unauthorized changes to your UAF
- Detect inactive accounts
- Detect accounts with duplicate UIC's
- Detect accounts with no passwords
- Detect accounts whose passwords aren't being changed frequently
- Detect accounts which should be DISUSERED but aren't
- Update a field in one or more accounts
- Generate readable reports based on selection criteria you specify

Audit your UAF
With FERRET, you can run an extensive audit check on your UAF looking for potential security or performance problems. FERRET detects inactive accounts, accounts with duplicate UIC's, accounts with no password and a host of other potential problems. You can automate this process so your UAF is audited every night automatically.

Highlight differences
FERRET compares your current UAF with an earlier version or with a UAF on another node and shows you the differences. It shows new accounts, deleted accounts and modifications to existing accounts. You can set up a process so you will be automatically informed if unauthorized changes are made to your UAF. With the differences report, you'll **know** you're the only one making changes to your UAF.

Update UAF fields
You can modify one or more accounts in your UAF quickly and easily. Just specify selection criteria, describe the change you want to make and FERRET will update every account which matches your criteria. You can even confirm each change before it's made. It's easy and it's fast.

Generate readable reports
You can generate a vast array of readable UAF reports. Just list the fields you want to see, specify selection criteria and FERRET generates the report in user name or UIC sequence. You can list memory-based parameters such as WSDEFAULT, WSQUOTA, WSEXTENT and PGFLQUOTA as well as resource limits, privileges, access times, flags as well as login and password information.

You can store report specifications in a file so you can generate a report repeatedly.

Easy to use
FERRET is easy to set up and use. It comes with a tutorial, on-line HELP, extensive error messages and a comprehensive user guide and reference manual.

Field-proven
FERRET is highlighting problems and updating UAF's at dozens of sites in North America. It's solidly engineered, rigorously tested and fully field-proven by system managers like yourself.

Fully supported
With an annual support agreement, you'll always have someone to call if you have any problems with FERRET. For a single low annual fee, you get unlimited TOLL-FREE telephone support from our experienced software developers, yearly software updates and a subscription to our quarterly newsletter packed with tips showing you how to use FERRET to tighten security on your system. Our support lines are open Monday to Friday from 8 a.m. to 5 p.m. Mountain Standard Time except normal business holidays.

Installing FERRET

Ferret is easy to install on your Alpha AXP or VAX system using the Digital supplied VMSINSTAL procedure. It only takes a few minutes and can be safely done while there are users on the system. For the complete installation instructions refer to the Product Installation Guide.

Getting Started

This chapter shows you how to get started after you have installed FERRET.

From the command line interface you can audit your UAF, copy records from one UAF to another, list differences between two UAF's and generate readable reports. To use this interface, you should refer to the chapter "FERRET Commands". Here are some examples of DCL commands:

To audit your UAF, type:

```
$ FERRET/REPORT=AUDIT
```

To list differences between your current UAF to an earlier version, type:

```
$ FERRET/REPORT=DIFFERENCES/UAF_FILE=file-spec
```

To display which version of FERRET you are running, type:

```
$ FERRET/VERSION
```

Here is a procedure to generate sample reports from the DCL interface.

1. Enable the FERRET command verb.

   ```
   $ SET COMMAND FERRET_CDU:FERRET
   ```

2. Specify a report

   ```
   $ FERRET/REPORT=AUDIT/OUTPUT
   ```

3. Print the report.

   ```
   $ PRINT FERRET.LIS
   ```

There are three sample command procedures in the FERRET_COM: directory: MONTHLY_AUDIT.COM, WEEKLY_AUDIT.COM and DAILY_AUDIT.COM. These procedures can be used directly or modified to suit your site's needs.

New with Version 5.0

Ferret V5.0 incorporates several of the most frequently requested changes and enhancements since V4.1 was released. Since V4.1 was not a major release and many sites are still running V4.0 the new features added to V4.1 are also included in this section.

* Because of changes made to the compilers that support dynamic tables Ferret Version 5 it is the first Version of Ferret to have a minimum Version of OpenVMS requirement. Ferret V5 requires OpenVMS 7.1 or higher and it requires Version 7.3 or higher of the OpenVMS Fortran Run-time Libraries (RTL) which are distributed with the operating system. At the time this manual was produced Ferret V5 was only available for AXP systems. A VAX version is currently under development.

* Several more checks are made for bad passwords during the audit report. All of the following checks are also performed with the suspect password reversed. These include SYSUAF account name, SYSUAF owner name (spaces removed), SYSUAF owner name (spaces changed to underbars "_") and if there is more than 1 word/name in the SYSUAF owner name each of them is also individually tested.

* Previous versions of Ferret had a limit of 5,000 entries in the bad passwords file. This list is now allocated dynamically and there is no limit on the number of bad passwords that can be checked for.

* A dictionary of passwords published on an internet security site that contains almost 2,500 passwords the author found in multiple password cracking programs has been included. Any passwords included in this list that were not valid OpenVMS passwords have been removed. This list can be used as an extra check to help guarantee that users do not have easily guessed passwords set. Since checking all these passwords takes a significant amount of resources the default is to run the audit report with the older, smaller list. A new qualifier, /password_file, has been added to allow users to specify the name of the bad password dictionary the audit report should use; users may specify the enhanced dictionary included with Version 5, their own dictionary or if this qualifier is not specified Ferret will use the default dictionary. We recommend running the audit report, with the larger dictionary specified, at least once a month. Sites with high security concerns should consider checking for bad passwords with this list on a weekly basis. A new WEEKLY_AUDIT.COM procedure has been added as an example of how this might be done.

* Report specification files have had three enhancements made with this release:

    * if the first line of the specification file is NOHEAD the report will be generated as a flat ASCII file with no headings or page breaks. Previously a logical name had to be defined to suppress headings and all reports would be generated as flat files until the logical name was deassigned.
    * In previous versions of Ferret UICs were reported in their ASCII text representation

by default; to have them displayed as numeric values the /type=numeric qualifier was necessary. A new specification item, octal_uic, has been added which will add the UIC in numeric format to the report. It is possible to specify both UIC and OCTAL_UIC in the same report to have UICs included in both formats.

* the size of each individual report item can now be control in the specification file by following the item with a comma and the field size desired. For example the following specification file is generated as a flat file, with no headings or page breaks, and the device, directory and clitables fields are all set to be smaller than the ferret default values.

```
NOHEAD
USERNAME
UIC
OCTAL_UIC
I_LASTLOGIN
N_LASTLOGIN
LOGFAILS
EXPIRATION
DEVICE,8
DIRECTORY,10
CLITABLES,5
```

* it is now possible to specify a UIC range for selection criteria. Simply specify the starting value, in octal, a colon and the ending value, also octal. Ranges can be specified for UIC groups, UIC members or both. For example to specify UIC members 1 to 10 of the UIC groups 100 to 777:

```
/UIC="[100:777,1:10]"
```

a list of values can still be entered, however, a range cannot include a wildcard. The following is a valid example:

```
/UIC=("[100,*]","[250:300,1:10]","[1000,475]")
```

while this is not valid:

```
/UIC=("[100,*]","[250:300,*]","[1000,475]")
```

* searching for, or excluding, blanks in several text fields in the UAF was documented but was not working properly. It is assumed this problem was introduced by a change in the system string matching routines. It should now be working properly and you can specify " " for blank value for the following UAF items: account, cli, clitables, data, device, directory, lgicmd, owner and username. These values can also be negated. For example to find all SYSUAF records with no owner:

```
$Ferret /report /list=(user,owner) /owner=" "
```

or to find all records where the user data field is not blank

```
$Ferret /report /list=(user,data) /data=("-"," ")
```

New with Version 4.1

Enhancements and fixes included in Version 4.1 of Ferret include:

* When generating Ferret reports with the report generator V4 only allowed the reports to be sorted by username or UIC. Version 4.1 supports sorting by almost all UAF fields; a complete list of the supported fields can be found in the qualifier reference section for /sort.

* A new /descending qualifier has been added to change the sort order on list reports from ascending to descending order. For example it is now possible to generate a list of users and their working set values sorted in descending order by working set size.

* When using Ferret to copy accounts from one UAF file to another identifiers were not copied unless the two UAF files shared a common rights file. A new rights utility has been added that allows you to generate a file of all the rights held by a user or group of users and then use this file as input on another node to add those identifiers for those users; Ferret will also add the actual identifier if it doesn't exist.

* If Ferret was used to update the /pwdlifetime field a new calculated date was stored in this field instead of the delta time. This problem has been fixed with V4.1.

Using FERRET on a VAXCLUSTER

This chapter shows you how to use FERRET on VAXCLUSTER systems.

Common SYSUAF.DAT
If you have a common SYSUAF.DAT for your cluster, you can use FERRET as if you were on a single Alpha AXP or VAX. FERRET will automatically find your SYSUAF.DAT using the OpenVMS-supplied logical "SYSUAF".

Multiple SYSUAF.DAT files
On the other hand, if your cluster has a separate SYSUAF.DAT for each node, you will have to specify each SYSUAF.DAT rather than allowing FERRET to use the default SYSUAF.DAT on your current node. To do this, specify the UAF file as a **parameter** after your command and qualifiers. For example:

```
$ FERRET/REPORT=ACCESS/OUTPUT=NODE2_ACCESS-
_$  NODE2::$4$DUA0:[SY0.SYSCOMMON.SYSEXE]SYSUAF.DAT
```

to create an access report for the users on NODE2 by running FERRET on a SYSUAF on a different node.

If you don't specify the UAF as a parameter, FERRET will use the SYSUAF.DAT on your current node.

STARTUP command procedure
The FERRET installation procedure creates a file, FERRET_STARTUP.COM and copies it to the SYS$MANAGER directory. This command procedure must be executed on every node.

Solving FERRET problems

This chapter shows you how to resolve problems with FERRET.

If you have a problem running FERRET, please do the following:

Verify that FERRET logicals are defined
Verify that your process has the necessary privileges
Verify that the command definition is installed and compatible
Call Technical Support at Saiga Systems

Verify that FERRET logicals are defined
FERRET uses six logicals to access data files and executables. Normally, these logicals are defined as part of the system startup. However, to ensure the logicals are defined, type the following command:

```
$ @SYS$MANAGER:FERRET_SYSTEM_LOGICALS.COM
```

This procedure is created as part of the FERRET installation procedure. If the logicals were already defined, you will see the following message:

%DCL-I-SUPERSEDE, previous value of {logical_name} has been superseded

repeated five times.

To verify that the FERRET logicals are defined, type the following command:

```
$ SHOW LOGICAL FERRET*
```

You should see output similar to the following:

```
(LNM$PROCESS_TABLE)

(LNM$JOB_xxxxxx)

(LNM$GROUP_xxxxxx)

(LNM$SYSTEM_TABLE)

  "FERRET_CDU"     = "ddcu:[FERRET.CDU]"
  "FERRET_COM"     = "ddcu:[FERRET.COM]"
  "FERRET_DAT"     = "ddcu:[FERRET.DAT]"
  "FERRET_DOC"     = "ddcu:[FERRET.DOC]"
  "FERRET_EXE"     = "ddcu:[FERRET.EXE]"
  "FERRET_PASSWORD"= "FERRET_DAT:FERRET_PASSWORD.DAT"
```

where "ddcu:" is the disk drive on which FERRET is installed. This output indicates that the FERRET logicals are properly defined in the SYSTEM table.

Verify that your account has the necessary privileges
FERRET data collection requires OpenVMS privileges such as SYSPRV to run. Ensure that you have sufficient privileges in your account.

To ensure your process has all the necessary privileges, type the following command:

```
$ @FERRET_COM:SET_PRV.COM
```

If you see the following message:

%SYSTEM-W-NOTALLPRIV, not all requested privileges authorized

the account you are logged into does not have all the privileges necessary to run FERRET. You must log into an account which does have all the privileges. Normally, the SYSTEM account will have (or be able to acquire) all the necessary privileges to run FERRET.

If your process does not have all the necessary privileges, FERRET will list the additional privilege(s) you need when you enter a command.

To find out what privileges your process has, type the command:

```
$ SHOW PROCESS/PRIVILEGES
```

To give your process specific privileges, type the command:

```
$ SET PROCESS/PRIVILEGE=privilege_name
```

Verify that the software license is installed
FERRET will not run unless there is a license installed. To check this type the following command:

```
$ SHOW LOGICAL PKMS*
```

In the LNM$SYSTEM_TABLE you should see at least one of the following logicals defined.

```
PKMS$FERRET-VAX
PKMS$FERRET-AXP
PKMS$COHORT-VAX
PKMS$COHORT-AXP
```

If you don’t see a logical for the license check the system manager directory for the license startup file and execute it if it exists.

```
$ DIRECTORY SYS$MANAGER:*PKMS*.*
$ @SYS$MANAGER:FERRET-VAX_PKMS_START
```

If there is no license startup file load your paper license key (printed on pale gray paper):

```
$ @SYS$MANAGER:SAIGA_LICENSE
```

remember that the license load is case sensitive - enter all values exactly as printed on the license.

Verify that command definitions are installed and compatible.
If you receive either of the following messages when you type a command:

```
%DCL-W-IVVERB, unrecognized command verb - check validity and spelling
 \FERRET\

%CLI-F-SYNTAX, error parsing 'qualifier_name'
-CLI-F-ENTNF, specified entity not found in command tables
```

where "qualifier_name" is one of the FERRET qualifiers, FERRET's command definition has not been installed in the system or process table or the command definition version you are using is not compatible with the FERRET executable version.

To add the command definition to your process table, type the following command:

```
$ @FERRET_COM:INSTALL_CDU.COM
```

Obtaining Technical Support

If you try the above suggestions and still continue to have problems, please contact Saiga Systems Technical Support :

by telephone at 1-866-573-8182 (toll-free) between 8:00 am and 5:00 pm Mountain Time
by e-mail at support@saiga.com
international users may reach us at 403-248-2004

Please have the following information available or include it in your e-mail:

whether you are running on Alpha, VAX or both and what version of OpenVMS
your company name
FERRET version (from FERRET/VERSION output)

We will verify that you have a support agreement and speak to you or reply to your e-mail as quickly as possible.

You may wish to check our web page for known problems and patches:

WWW http:/www.saiga.com/

Detecting security and performance problems

This chapter shows you how to detect potential security and performance problems using FERRET. It lists dozens of items you can look for, explains how to use FERRET and refers you to more detailed information in the chapters which follow.

Checking for login failures
A high number of login failures may indicate that:

- an inexperienced user is having trouble
- a cable is incorrectly or incompletely wired
- someone is trying to "hack" into the account

Use the command:

```
$ FERRET/REPORT/LIST=(USER,LOGFAILS)/LOGFAILS=n:
```

to obtain a list of accounts with *n* or more login failures. Please note that the login failure count is set to zero when the user successfully logs in. Refer to the chapter "Generating customized reports" for more information.

Finding accounts with the same UIC

Although OpenVMS allows you to create accounts with duplicate UIC's, having duplicate UIC's compromises security and complicates the task of controlling disk storage. Use the command:

```
$ FERRET/REPORT=AUDIT
```

to audit your UAF. The audit will provide a list of accounts with the same UIC. Refer to the chapter "Auditing your UAF" for more information.

Finding accounts with the same default disk

If you need to move several or all users on a particular disk to a new disk, having a list of who uses that disk can be a real life-saver. Use the command:

```
$ FERRET/REPORT/LIST=(USER,DEVICE)/DEVICE=device
```

to obtain a list of accounts with the same default disk device. Refer to the chapter "Generating customized reports" for more information.

Finding accounts which cannot be logged into (DISUSER)

Use either of the commands:

```
$ FERRET/REPORT/LIST=(USER,FLAGS)/FLAGS=DISUSER/FORMAT=ROW
$ FERRET/REPORT=FLAGS/FLAGS=DISUSER
```

to obtain a list of accounts which cannot be logged into. Refer to the chapter "Generating customized reports" for more information.

Finding captive accounts

Use the command:

```
$ FERRET/REPORT/LIST=(USER,FLAGS)/FLAGS=CAPTIVE/FORMAT=ROW
```

to obtain a list of accounts which are captive accounts. Refer to the chapter "Generating customized reports" for more information.

Finding accounts which have expired or are about to

Use the command:

```
$ FERRET/REPORT/LIST=(USER)/EXPIRATION=1
```

to obtain a list of accounts which cannot be logged into because the account has expired or will expire tomorrow. Refer to the chapter "Generating customized reports" for more information.

Listing memory limits and quotas

Lack of memory can severely impact a user's response time. Excessive memory allocation for many users can impact the performance of the system as a whole. Use the command:

```
$ FERRET/REPORT/SPECIFICATION=FERRET_DAT:MEMLQ.SPC
```

to obtain a list of memory-related limits and quotas. Refer to the chapter "Generating customized reports" for more information. The sample report specification file MEMLQ.SPC produces a report titled "FERRET Memory Report" containing the following fields:

USER
WSDEFAULT
WSQUOTA
WSEXTENT
PGFLQUOTA

Listing resource limits and quotas

Lack of adequate resources can severely impact a user's response time. Excessive resource allocation for many users can impact the performance of the system as a whole. Use the command:

```
$ FERRET/REPORT/SPECIFICATION=FERRET_DAT:RESLQ.SPC
```

to obtain a list of resource limits and quotas. The sample report specification file RESLQ.SPC produces a report titled "FERRET Resource Report" containing the following fields:

USER
ASTLM
BIOLM

(continued)

BYTLM
CPUTIME
DIOLM
ENQLM
FILLM
JTQUOTA
MAXACCTJOBS
MAXDETACH
MAXJOBS
PRCLM
SHRFILLM
TQELM

Refer to the chapter "Generating customized reports" for more information.

Listing default priorities

High priorities, especially for compute-intensive jobs, can impact the performance of the system as a whole. Use the command:

```
$ FERRET/REPORT/SPECIFICATION=FERRET_DAT:PRIORITY.SPC
```

to obtain a list of default priorities. The sample report specification file PRIORITY.SPC produces a report titled "FERRET Priority Report" containing the following fields:

USER
PRIORITY
QUEPRI

Refer to the chapter "Generating customized reports" for more information. QUEPRI is included in this report because it is a valid UAF field, however, it is not used any longer in recent versions of OpenVMS.

Listing account reference information

Use the command:

```
$ FERRET/REPORT/SPECIFICATION=FERRET_DAT:REF.SPC
```

to obtain a list of account reference information. The sample report specification file REF.SPC produces a report titled "FERRET Reference Report" containing the following fields:

USER
UIC
ACCOUNT
OWNER

Refer to the chapter "Generating customized reports" for more information.

Listing login information

Use the command:

```
$ FERRET/REPORT/SPECIFICATION=FERRET_DAT:LOGIN.SPC
```

to obtain a list of login items. The sample report specification file LOGIN.SPC products a report titled "FERRET Login Report" containing the following fields:

USER
UIC
I_LASTLOGIN, Last interactive login date
N_LASTLOGIN, Last non-interactive login date
LOGFAILS, Number of login failures
EXPIRATION, Expiration date of the account
DEVICE, Default login device
DIRECTORY, Default login directory
CLITABLES, CLI table

Refer to the chapter "Generating customized reports" for more information.

Listing password information

Use the command:

```
$ FERRET/REPORT/SPECIFICATION=FERRET_DAT:PASSWORD.SPC
```

to obtain a list of password information. The sample report specification file PASSWORD.SPC products a report titled "FERRET Password Report" containing the following fields:

USER
UIC
PWDMINIMUM, minimum password length
PWDLIFETIME, password lifetime
P_PWDDATE, primary password expiration date
S_PWDDATE, secondary password expiration date

Refer to the chapter "Generating customized reports" for more information.

Finding inactive accounts

Accounts which aren't logged into regularly should be disusered to prevent security problems. Use the command:

```
$ FERRET/REPORT/LIST=(USER,I_LASTLOGIN,N_LASTLOGIN)-
_$ /I_LASTLOGIN=-45/N_LASTLOGIN=-45
```

to obtain a list of accounts which haven't had an interactive or non-interactive login in the past 45 days. Refer to the chapter "Generating customized reports" for more information.

Disabling inactive accounts

Accounts which aren't logged into regularly should be disusered to prevent security problems. Use the command:

```
$ FERRET/MODIFY=FLAGS/SET=DISUSER-
_$ /I_LASTLOGIN=-90/N_LASTLOGIN=-90
```

to DISUSER accounts which haven't had an interactive or non-interactive login in the past 90 days. Refer to the chapter "Modifying fields in one or more accounts" for more information.

Finding accounts with unusual privileges

In general, you should grant as few privileges as possible while allowing users to accomplish their processing. Use either of the commands:

```
$ FERRET/REPORT/FORMAT=ROW/LIST=(USER,PRIVILEGES)-
_$ /PRIVILEGES=(BUGCHK,BYPASS,CMEXEC,CMKRNL,READALL,SETPRV)

$ FERRET/REPORT=PRIVILEGES-
_$ /PRIVILEGES=(BUGCHK,BYPASS,CMEXEC,CMKRNL,READALL,SETPRV)
```

to obtain a list of accounts with any of the unusual privileges listed above. Refer to the chapter "Generating customized reports" for more information.

Finding accounts with unusual privileges in a group

The members of a group should have approximately the same privileges. Use the commands:

```
$ FERRET/REPORT=PRIVILEGES/UIC=[n,*]/OUTPUT
$ FERRET/REPORT=PRIVILEGES/ACCOUNT=name/OUTPUT
```

to obtain a list of privileges for each account in group *n* or with the account "name". If one account has significantly more privileges than the others, it will stand out on the listing. Refer to the chapter "Displaying privilege information" for more information.

Finding accounts with non-default privileges

In general, you should grant as few privileges as possible while allowing users to accomplish their processing. Use the command:

```
$ FERRET/REPORT=PRIVILEGES/PRIVILEGES=ELEVATED
```

to obtain a list of accounts with any privileges other than the default privileges of TMPMBX and NETMBX. Refer to the chapter "Displaying privilege information" for more information. You can control which privileges are considered elevated using the FERRET_ELEVATED.DAT file.

Finding accounts with non-standard CLI names

Use the command:

```
$ FERRET/REPORT/LIST=(USER,CLI,CLITABLE)/CLI=-DCL
```

to obtain a list of accounts which do not have the standard CLI of "DCL". The vast majority of accounts use DCL so this report will have no entries on most systems. Refer to the chapter "Generating customized reports" for more information.

Finding accounts with high default priorities

Accounts which run compute-intensive jobs and have high default priorities can severely impact other user's response. Use the command:

```
$ FERRET/REPORT/LIST=(USER,PRIORITY)/priority=n:
```

to obtain a list of accounts which have a base priority of *n* or more. The default priority is 4 so specifying 5: (5 or higher) will produce a useful report. Refer to the chapter "Generating customized reports" for more information.

Finding accounts which don't require passwords

Accounts which don't require passwords are potential security problems. Ensure that these accounts are not available for general use or have the flag CAPTIVE. Use the command:

```
$ FERRET/REPORT/LIST=USER/PWDMINIMUM=0
```

to obtain a list of accounts which don't require a password. Refer to the chapter "Generating customized reports" for more information.

Finding accounts whose passwords haven't changed recently

The older a password is, the more likely it is to be compromised. Use the command:

```
$ FERRET/REPORT/LIST=USER/P_PWDDATE=-n/S_PWDDATE=-n
```

to obtain a list of accounts whose passwords haven't been changed in the last *n* days (n must be a delta time). Refer to the chapter "Generating customized reports" for more information.

Finding accounts which should have the LOCKPWD flag

The accounts DECNET and SYSTEST_CLIG should have the LOCKPWD set. Use the command:

```
$ FERRET/REPORT/LIST=(USER,FLAGS)/FLAGS=LOCKPWD/FORMAT=ROW
```

to obtain a list of accounts whose passwords are locked. Refer to the chapter "Generating customized reports" for more information.

Finding accounts whose passwords have expired

Use the command:

```
$ FERRET/REPORT/LIST=USER/PWDEXPIRED
```

to obtain a list of accounts whose passwords have expired. Refer to the chapter "Generating customized reports" for more information.

Finding accounts whose passwords are too short

The fewer characters a password contains, the more likely it can be guessed by a hacker. Use the command:

```
$ FERRET/REPORT/LIST=(USER,PWDMINIMUM)/PWDMINIMUM=:n
```

to obtain a list of accounts whose passwords contain *n* or fewer characters. Refer to the chapter "Generating customized reports" for more information.

Finding accounts whose passwords are poorly chosen

Although OpenVMS now screens passwords set using SET PASSWORD against a dictionary, existing passwords are not screened until they are changed and the AUTHORIZE utility still accepts poor passwords. Use the commands:

```
$ FERRET/REPORT/LIST=USER/P_PASSWORD=(text-string,...)
$ FERRET/REPORT/LIST=USER/S_PASSWORD=(text-string,...)
```

to obtain a list of accounts whose passwords are one of a list of easily guessed words or phrases. You can check up to 64 passwords in each run. (Note that the FERRET audit report checks up to 5,000 passwords in a single run using the FERRET_DAT:FERRET_PASSWORD.DAT file).

NOTE: This FERRET facility is intended to supplement the existing OpenVMS facility, not as a substitute for it.

Refer to the chapter "Generating customized reports" for more information. Appendix K contains a list of the sample poor passwords supplied with FERRET.

Finding privileged accounts with AUTOLOGIN set

Obviously, a privileged account should never have the AUTOLOGIN flag set. Use the commands:

```
$ FERRET/REPORT/LIST=(USER,PRIVILEGES)/FLAG=AUTOLOGIN-
_$ /UIC=[1,*]

$ FERRET/REPORT/LIST=(USER,PRIVILEGES)/FLAG=AUTOLOGIN-
_$ /PRIVILEGES=SYSPRV
```

to obtain lists of accounts which are privileged and have the AUTOLOGIN flag set. If you have privileged accounts with UIC groups greater than "1", you must repeat the first command for each group. Refer to the chapter "Generating customized reports" for more information.

Auditing your UAF

This chapter shows you how to check your user authorization file for potential problems using the /REPORT=AUDIT command.

Contents of the audit report
When you run an audit report, FERRET performs a number of checks on your UAF file and reports all accounts that fail any of the checks. By default all checks are performed, however, use the /EXCLUDE qualifier to omit any classes you desire.

DISUSER

Accounts which are marked DISUSERED

Accounts which Digital recommends be DISUSERED but are active. The usernames checked are the default OpenVMS accounts DEFAULT, FIELD, SYSTEST, SYSTEST_CLIG. The standard account SYSTEM is not flagged since most systems keep this account active.

EXPIRED

Accounts which have expired. To modify the default account expiration date, use the /EXPIRATION qualifier.

FILE

The audit reports if the UAF doesn't have the file ownership and protection specified in the OpenVMS documentation.

LOGFAIL

Accounts with more than 4 login failures. Use the qualifier /LOGFAILS to over-ride this default limit.

LOGIN

Accounts which have been inactive for at least 30 days. Use the qualifiers /I_LASTLOGIN and /N_LASTLOGIN to over-ride this default limit.

PASSWORD

Accounts whose passwords haven't been changed in 90 days. Use the qualifiers /P_PWDDATE and /S_PWDDATE to over-ride this default limit.

Accounts whose passwords have expired.

Accounts with minimum password length less than 6 characters. Use the qualifier /PWDMINIMUM to over-ride the default limit.

Accounts with password lengths of zero (no password required).

The SYSTEM account is reported if it has a password less than 8 characters long or the password lifetime is more than 30 days.

Accounts with a password on a list of poor passwords. There is a file called FERRET_PASSWORD.DAT in the [FERRET.DAT] directory which contains a list of poor passwords; any account with a password contained in this file is reported. FERRET has a rudimentary password-guessing facility and also reports accounts that have a password the same as, or the reverse of, the username, owner name or account name. If owner name or account have more than one word a check is also made for the two words with no spaces, an underbar "_" instead of spaces and for each individual word. A more comprehensive bad password list, bad_passwd_dictionary.dat, has been added with V5 of Ferret; to check against this list add /password_file=bad_passwd_dictionary.dat to the command line of the audit report.

PRIORITY

Accounts with a base priority greater than 4. Use the qualifier /PRIORITY to over-ride the default limit.

UIC

Accounts with the same UIC as another account, with no UIC or a UIC of zero [0,0].

NOTE: FERRET's password checking is a supplement to the OpenVMS password dictionary. It is not intended to replace it.

If an account is DISUSERED, the audit will not flag last login dates or password change dates.

For an account to be flagged as inactive, both interactive and non-interactive last login dates must be older than the specified date. If either is more recent, the account will not be flagged as inactive.

For duplicate UIC's, only the first duplicate is shown regardless of how many there are.

If an account does not have interactive access, the audit will not flag the account as inactive.

Enter the command:

```
$ FERRET/REPORT=AUDIT[/EXCLUDE=([DISUSER,][EXPIRED,][FILE,][LOGIN,]
        [LOGFAIL,][PASSWORD,][PRIORITY,][UIC])
```

to audit your current UAF; use /EXCLUDE to control which checks FERRET makes. You can specify /OUTPUT, /SORT, /TITLE and /TYPE, if you wish. You cannot specify /LIST, /FORMAT, /TRUNCATE, /WIDTH or /SPECIFICATION.

The audit report is a row-formatted report since it contains a variable number of fields.

FERRET_PASSWORD.DAT

The file FERRET_PASSWORD.DAT in the [FERRET.DAT] directory contains a list of poor

passwords. Appendix K lists the passwords in it. You can add additional passwords to this list using any text editor. FERRET supports up to 5,000 entries in this file.

FERRET reads the file using the logical FERRET_PASSWORD. You can change the location of the file by re-defining the logical.

Displaying flag information

This chapter shows you how to generate reports on flags such as AUTOLOGIN and DISMAIL.

Displaying all flags
Use the /REPORT=FLAGS command to generate the flags report. Since this report is pre-specified, you don't have to list the fields which appear on the report. The flags report shows you every flag for the accounts which match the criteria you've specified. The flags are shown in an abbreviated format so that all of them will fit on a single line. Use this report to get an overview of the flags each account has.

You can specify /OUTPUT, /SORT and /TITLE with this report.

Displaying one or more specific flags using /LIST/FORMAT=ROW
Use the /REPORT/LIST qualifiers in conjunction with the selection criteria /FLAGS to generate a detailed report of one or more flags. The detailed flags report shows you the flags held by the accounts which match the other criteria you've specified. The flags are shown in expanded format so the report may wrap if the account has more than a few of them.

You can specify /OUTPUT, /SORT and /TITLE with this report. You must specify /FORMAT=ROW to generate a row-formatted report.

Specifying selection criteria
On either of the reports, you can select one or more accounts to appear on the report by specifying selection criteria. If you don't specify any selection criteria, all accounts will appear on the report. For more information on selection criteria, refer to the chapter "Specifying selection criteria".

Use the qualifier /LEGEND to print a legend page showing the meanings of the abbreviations used on the report.

Use the qualifier /ALL to show all accounts even if they don't have any flags. This is useful when you want to generate a reports showing accounts with negated flags (ie list accounts which don't have TMPMBX).

Displaying privilege information

This chapter shows you how to generate reports on privileges such as SYSPRV and BYPASS or any other OpenVMS privilege.

Displaying all privileges
Use the /REPORT=PRIVILEGES command to generate the privileges report. Since this report is pre-specified, you don't have to list the fields which appear on the report. The privileges report shows you every privilege for the accounts which match the criteria you've specified. The privileges are shown in an abbreviated format so that all of them will fit on a single line. Use this report to get an overview of the privileges each account has. If the account has a privileges through either the default **or** authorized mechanisms, this report shows the user as having it.

Use /REPORT=DEFPRIVILEGES to show only default privileges.
Use /REPORT=AUTHPRIVILEGES to show only authorized privileges.

You can specify /OUTPUT, /SORT and /TITLE with this report.

Displaying one or more specific privileges using /LIST/FORMAT=ROW
Use the /REPORT/LIST qualifiers in conjunction with the selection criteria /PRIVILEGES to generate a detailed report of one or more privileges. The detailed privileges report shows you the privileges held by the accounts which match the other criteria you've specified. The privileges are shown in expanded format so the report may wrap if the account has more than a few of them.

You can specify /OUTPUT, /SORT and /TITLE with this report. You must specify /FORMAT=ROW to generate a row-formatted report.

Specifying selection criteria
On either of the reports, you can select one or more accounts to appear on the report by specifying selection criteria. If you don't specify any selection criteria, all accounts will appear on the report. For more information on selection criteria, refer to the chapter "Specifying selection criteria".

Displaying access information

This chapter shows you how to generate reports on access times.

Only BATCH, DIALUP, LOCAL, NETWORK or REMOTE are shown on the report because ACCESS and INTERACTIVE refer to combinations of the above five categories.

ACCESS is a combination of BATCH, DIALUP, LOCAL, NETWORK and REMOTE access times. That is, it is a combination of all five categories.

INTERACTIVE is a combination of DIALUP, LOCAL and REMOTE access times.

Displaying all access times
Use the /REPORT=ACCESS command to generate the access time report. Since this report is pre-specified, you don't have to list the fields which appear on the report. The access time report shows you every access time for the accounts which match the criteria you've specified. The access times are shown in a graphic format so that all of them will fit on as few lines as possible. Use this report to get an overview of the access times each account has.

You can specify /OUTPUT, /SORT and /TITLE with this report.

Displaying one or more specific access times using /LIST/FORMAT=ROW
Use the /REPORT/LIST qualifiers in conjunction with the selection criteria /ACCESS, /BATCH, /DIALUP, /INTERACTIVE, /LOCAL, /NETWORK or /REMOTE to generate a detailed report of one or more access times. The detailed access time report shows you only the access times you list for the accounts which match the other criteria you've specified.

You can specify /OUTPUT, /SORT, /TITLE and /TRUNCATE with this report. You must specify /FORMAT=ROW to generate a row-formatted report.

Specifying selection criteria
On either of the reports, you can select one or more accounts to appear on the report by specifying selection criteria. If you don't specify any selection criteria, all accounts will appear on the report. For more information on selection criteria, refer to the chapter "Specifying selection criteria".

Generating customized reports

This chapter shows you how to generate your own site-specific reports using the /REPORT command.

Enter the command:

```
$ FERRET/REPORT/LIST
```

to generate a customized report. You can specify /FORMAT, /OUTPUT, /SORT, /TITLE, /TRUNCATE, /TYPE and /WIDTH if you wish.

NOTE: FERRET uses the routine LIB$LP_LINES to determine the number of lines per report page for printed reports. To change the number of lines define the logical SYS$LP_LINES.

Specifying report items
You can specify which items you want on the report in two ways:

```
/LIST
/SPECIFICATION
```

Use the /LIST qualifier to indicate what items you want to see on the report. For example, the qualifier:

```
/LIST=(USER,UIC,CLI,PRIMEDAYS)
```

indicates that you want the four items to appear in the order you listed them on the report. You can specify one or more items using the list command. Appendix G contains a complete list of the UAF items you can select.

Use the /SPECIFICATION qualifier to indicate a file which contains a list of items you want to see on the report with a report title. If you generate reports with the same items repeatedly, put them in a specification file to save keying in the list repeatedly. The section "Creating a specification file" explains how to store report specifications.

If the /LIST or /SPECIFICATION file contains the USER item, disusered accounts will be flagged with an "*" at the start of the user name.

Specifying a report format
There are two report formats:

```
COLUMN (default)
ROW
```

On column reports (/FORMAT=COLUMN), each line represents an account and each item

occupies a column on that line. Use COLUMN reports to compare the values in different accounts by presenting as much information as possible on each line. When you specify a COLUMN report, you can specify the /TRUNCATE qualifier to specify the maximum number of columns there are on each line of the report. Because of the large amount of space required, column-based reports do not show access times, privileges, flags and primedays.

On row reports (/FORMAT=ROW), each item occupies a line by itself. Use ROW reports to obtain the maximum amount of information about each item. If you specify any of the following fields:

FLAGS
PRIVILEGES
DEFPRIVILEGES
AUTHPRIVILEGES
ACCESS
BATCH
DIALUP
INTERACTIVE
LOCAL
REMOTE
PRIMEDAYS

you **must** specify /FORMAT=ROW.

Specifying selection criteria
You can select one or more accounts to appear on the report by specifying selection criteria. If you don't specify any selection criteria, all accounts will appear on the report. For more information on selection criteria, refer to the chapter "Specifying selection criteria".

Specifying report sequence
Use the /SORT qualifier to specify the sequence for the report. The default sequence is USER.

Directing output
You can view the output at your terminal (the default) or direct it to a file which can later be printed. Use the /OUTPUT qualifier to direct report output.

Specifying item width
Some of the items such as DIRECTORY can be very long. Specify /WIDTH to limit these items to a reasonable length so you can put more items on a single line. Appendix H contains a list of the maximum and default lengths of UAF items.

Specifying a report title
Use the /TITLE qualifier to specify a title for your report. If the title includes spaces or special characters, you must enclose it in quotation marks (""). The title can contain up to 64 characters. If you specify /TITLE without title text, FERRET uses the text "FERRET REPORT".

Creating a specification file
If you generate a report with the same set of fields regularly, create a specification file to avoid having to enter a long /LIST=(item,...,item) repeatedly.

By default, the specification file is located in FERRET_DAT: and has the file extension ".SPC"

A specification file is a text file which you create using an editor. You can create any number of specification files. Use the file name to indicate the type of report generated by the specification file.

Each specification file contains a report title (optional) and one or more item names. Each element (title or item) must be on a separate line. New with Version 5 of Ferret is the option to follow any item by a comma and a specify the width for that item in the report. This value will override the default width value for that item (listed in appendix F).

The title must be the first line in the text file. If it includes special characters, you must enclose it in quotation marks (""). FERRET reads the first line and checks to see if it is a valid item name. If it **is** a valid item name, FERRET uses the text from the /TITLE qualifier. If the first line **isn't** a valid item name, FERRET assumes the line is a report title and uses it rather than the text from the /TITLE qualifier. Ferret Version 5 now supports entering NOHEAD for the title; the report will be generated as a flat file with no title, headings or page breaks. These flat files are ideal for importing into other software.

If any other line in the file isn't a valid item name, FERRET generates an error message.

There are several examples of specification files in the [FERRET.DAT] directory.

Modifying fields in one or more accounts

This chapter shows you how to change a field in one or more accounts using the /MODIFY command.

Note

Although FERRET reports can be run at any time, the FERRET MODIFY function locks records in your UAF to prevent other changes from being made simultaneously. This may prevent users from logging in while the MODIFY function is running. We recommend that you change large numbers of accounts during non-prime time.

While every effort has been made to ensure that FERRET works correctly, your UAF is a critical system file. Please ensure you have a recent backup of it before modifying accounts using FERRET.

Specifying the item to modify
Use /MODIFY=item to specify which item you want to change. Appendix G contains a complete list of UAF items.

Specifying the type of modification
You can force an item to have a specific value using the /SET qualifier.

You can ensure that an item is within a range using the /MINIMUM and /MAXIMUM qualifiers.

You can increase or decrease an item's value using the /INCREMENT and /DECREMENT qualifiers.

Specifying selection criteria
You can select one or more accounts to modify by specifying selection criteria. If you don't specify any selection criteria, all accounts will be modified. For more information on selection criteria, refer to the chapter "Specifying selection criteria".

Controlling the modifications
By default, FERRET will update all accounts which match your criteria automatically. You can confirm each account update using the /CONFIRM qualifier. FERRET will display the user name of each record. You can enter:

YES	perform the operation
NO	do not perform the operation but continue processing
EXIT	return to the DCL prompt

Directing output
The modify function logs each change as it makes it. You can direct the output using the /OUTPUT qualifier.

Finding differences between two UAF's

This chapter shows you how to find the differences between two user authorization files using the /REPORT=DIFFERENCES command.

Contents of the differences report
When you run a differences report, FERRET shows:

new accounts (accounts in the current file but not the previous)

accounts which have been deleted (accounts in the previous file but not the current)

accounts which have been modified

The differences report is a ROW formatted report since it contains a variable number of fields.

Enter the command:

$ FERRET/REPORT=DIFFERENCES/UAF_FILE=file-spec

where file-spec is the name of a UAF file to compare against your current UAF file. You must specify /UAF_FILE. You can also specify /TYPE, /SORT and /TITLE if you wish. You cannot specify /LIST or /SPECIFICATION.

You can compare your current UAF with:

an earlier version
a UAF on another node

Comparing your UAF with an earlier version
Comparing your current UAF with an earlier version allows you to account for all modifications to the file and generate a hardcopy log of the changes you've made.

Comparing UAF's on different nodes
Comparing with a file on another node allows you to keep the accounts in both files compatible.

Controlling the reported modifications
By default, FERRET reports **every** change to **every** field. Since many fields change frequently, you can use the /IGNORE qualifier to ignore changes to fields which don't interest you.

Copying records and identifiers from one UAF to another

This chapter shows you how to copy one or more accounts from one user authorization file to another using the /COPY command and how to use the new rights copy utility to copy identifiers and rights as well.

To copy records enter the command:

```
$ FERRET/COPY/UAF_FILE=file-spec
```

where file-spec is the name of a UAF file which will receive the copied records. You must specify /UAF_FILE. Use the /ADD_IDENTIFIER with /COPY if you want to copy all the identifiers an account has as well as the record; the default action is to not copy identifiers. Add_identifier only works if the UAF files share a common rightslist.dat file; if they don't refer to the next section on copying rights identifiers from one UAF to another for information on the new rights copying utility added to Ferret V4.1.

Specifying selection criteria
You can select one or more accounts to copy by specifying selection criteria. If you don't specify any selection criteria, all accounts will be copied. For more information on selection criteria, refer to the chapter "Specifying selection criteria".

Controlling the copying
By default, FERRET will copy all accounts which match your criteria automatically. You can confirm each account copy using the /CONFIRM qualifier. FERRET will display the user name of each record. You can enter:

YES	perform the operation
NO	do not perform the operation but continue processing
EXIT	return to the DCL prompt

Directing output
The copy function logs each change as it makes it. You can direct the output using the /OUTPUT qualifier.

Creating a new UAF file
If the UAF_FILE doesn't exist, FERRET will ask you whether you want to create a new one. The resulting file will contain only the records transferred during the copy.

Copying identifiers
Ferret V4.1 contains a new identifiers copy utility that, when used in conjunction with the Ferret copy functionality, can be used to copy identifiers from one node to another as well as assign those identifiers, automatically, on the new node to the users that held them on the original node.

Since Ferret can only successfully copy identifier information from one UAF to another if they share the same rights file this new utility allows copies to be performed between nodes that do not

share this information.

To use this new rights copy utility follow these steps (for this procedure to work Ferret must be licensed and installed on both the old and new nodes):

1. An output file must be created using the /rights qualifier and /output. All valid Ferret selection criteria can be used to control which SYSUAF accounts have their identifier information copied into this file.

2. The resulting output file can then be copied to the new node

3. The Ferret /copy command is then used to copy the UAF records from the old node to the new node. The rights utility can be used just to copy identifier information without this step if the UAF accounts already exist in both file.

4. Invoke Ferret with the /rights qualifier and the /input qualifier to create the rights identifiers contained in the /output file and assign them to the users which held them on the old node.

For example, assuming we have five accounts for a particular application which uses rights identifiers to control which functions in the application particular users are allowed to perform: 1 operator with all rights, 1 account that has the right to update the database and 3 accounts that are allowed to query the database and run reports the entire process might look like this:

Use Ferret to generate a report showing privilege and identifier information for the accounts to be copied (in this case they all have an account of "HR DB").

```
$ FERRET /REPORT /LIST=(ACCOUNT,USERNAME,UIC,IDENTIFIER,PRIVILEGE) -
_$ /FORMAT=ROW /TYPE=ALPHA /SORT=USERNAME /DESCENDING /OUTPUT=HRDB.LIS -
_$ /ACCOUNT="HR DB"
$ TYPE HRDB.LIS
 DATE:  7-FEB-2000                  FERRET REPORT                    PAGE:   1
 NODE:    ROC
 FILE: SYSUAF
     Field Name        Field Value
 ------------------------------------------------------------------------------
             ACCOUNT : HR DB
            USERNAME :  DBUPDATE
                 UIC : [      HR,    DBUPDATE]
        IDENTIFIERS  : DBOPERATOR                      %X800F4240
                     : DBUSER                          %X800F4242
                     : DBREPORT                        %X800F4243
          PRIVILEGES :  TMPMBX    NETMBX    GRPPRV
*******************************************************************************
             ACCOUNT : HR DB
            USERNAME :  DBOPER
                 UIC : [      HR,      DBOPER]
        IDENTIFIERS  : DBOPERATOR                      %X800F4240
                     : DBMAINT                         %X800F4241
                     : DBUSER                          %X800F4242
                     : DBREPORT                        %X800F4243
          PRIVILEGES :  CMKRNL    TMPMBX    OPER      NETMBX    SYSPRV
*******************************************************************************
             ACCOUNT : HR DB
            USERNAME :  DBCLIENT3
                 UIC : [      HR,   DBCLIENT3]
        IDENTIFIERS  : DBUSER                          %X800F4242
                     : DBREPORT                        %X800F4243
```

```
          PRIVILEGES :  TMPMBX    NETMBX
*******************************************************************************
             ACCOUNT : HR DB
            USERNAME :  DBCLIENT2
                 UIC : [      HR,   DBCLIENT2]
        IDENTIFIERS  : DBUSER                          %X800F4242
                     : DBREPORT                        %X800F4243
          PRIVILEGES :  TMPMBX    NETMBX
*******************************************************************************
             ACCOUNT : HR DB
            USERNAME :  DBCLIENT1
                 UIC : [      HR,   DBCLIENT1]
        IDENTIFIERS  : DBUSER                          %X800F4242
                     : DBREPORT                        %X800F4243
          PRIVILEGES :  TMPMBX    NETMBX
*******************************************************************************
```

Generate the ferret rights output file for all users in account “HR DB”.

```
$ FERRET/RIGHTS/OUTPUT=HRDBIDENT.OUT/ACCOUNT="HR DB"
$ TYPE HRDBIDENT.OUT
DBCLIENT1,18219011,DBUSER,-2146483646,0,0
DBCLIENT1,18219011,DBREPORT,-2146483645,0,0
DBCLIENT2,18219012,DBUSER,-2146483646,0,0
DBCLIENT2,18219012,DBREPORT,-2146483645,0,0
DBCLIENT3,18219013,DBUSER,-2146483646,0,0
DBCLIENT3,18219013,DBREPORT,-2146483645,0,0
DBOPER,18219010,DBOPERATOR,-2146483648,0,0
DBOPER,18219010,DBMAINT,-2146483647,0,0
DBOPER,18219010,DBUSER,-2146483646,0,0
DBOPER,18219010,DBREPORT,-2146483645,0,0
DBUPDATE,18219009,DBOPERATOR,-2146483648,0,0
DBUPDATE,18219009,DBUSER,-2146483646,0,0
DBUPDATE,18219009,DBREPORT,-2146483645,0,0
```

Set host to the new node and login as system.

```
$ SET HOST SWIFT

 Welcome to OpenVMS (TM) Alpha OS

Username: SYSTEM
Password:
   Welcome to OpenVMS (TM) Alpha Operating System, Version V7.2 on node SWIFT
```

Ferret allows a parameter for the UAF to copy records from on the command line. To specify this a logical name is defined that includes the decnet remote login information.

```
$ DEFINE REMOTE_UAF -
  "ROC""SYSTEM password""::FALCON$DKA100:[SYS0.SYSCOMMON.SYSEXE]SYSUAF.DAT"
$ SHOW LOGICAL REMOTE*

(LNM$PROCESS_TABLE)

  "REMOTE_UAF" = "ROC"SYSTEM password"::FALCON$DKA100:[SYS0.SYSCOMMON.SYSEXE]SYSUAF.DAT"
```

To test the logical name and make sure it is defined correctly a report is generated using the remote_uaf.

```
$ FERRET/REPORT/LIST=USER/ACCOUNT="HR DB" REMOTE_UAF
 DATE:  3-JAN-2000                  FERRET REPORT                    PAGE:   1
 NODE:  SWIFT
 FILE: REMOTE_UAF
 USERNAME
 --------------------------------------------------------------------------------
  DBCLIENT1
```

```
  DBCLIENT2
  DBCLIENT3
  DBOPER
  DBUPDATE
```

The same report is generated locally and, as expected, no matching records are found.

```
$ FERRET/REPORT/LIST=USER/ACCOUNT="HR DB"
 DATE:  3-JAN-2000                  FERRET REPORT                    PAGE:   1
 NODE:  SWIFT
 FILE: SYSUAF
 USERNAME
 ------------------------------------------------------------------------------
%FERRET-W-NORECMATCH, No records matched the selection criteria
```

The records are copied with the /add_identifier qualifier so that ferret will try to add the UIC identifiers for each username as they are added.

```
$ FERRET /COPY /UAF_FILE=SYS$SYSTEM:SYSUAF.DAT/ACCOUNT="HR DB"/ADD_IDENTIFIER REMOTE_UAF
Copied user DBCLIENT1 from FALCON"SYSTEM to SYS$SYSTEM:SYSUAF.DAT
Copied user DBCLIENT2 from FALCON"SYSTEM to SYS$SYSTEM:SYSUAF.DAT
Copied user DBCLIENT3 from FALCON"SYSTEM to SYS$SYSTEM:SYSUAF.DAT
Copied user DBOPER from FALCON"SYSTEM to SYS$SYSTEM:SYSUAF.DAT
Copied user DBUPDATE from FALCON"SYSTEM to SYS$SYSTEM:SYSUAF.DAT
```

The rights utility is invoked with the earlier output file specified as input.

```
$ FERRET /RIGHTS /INPUT=ROC"SYSTEM password"::HRDBIDENT.OUT
```

The original report is generated on this new node to verify the accounts exist, they have the proper privileges and the identifiers have been added as expected.

```
$ FERRET /REPORT /LIST=(ACCOUNT, USERNAME, UIC, IDENTIFIER, PRIVI) /FORMAT=ROW
/ACCOUNT="HR DB"
 DATE:  3-JAN-2000                  FERRET REPORT                    PAGE:   1
 NODE:  SWIFT
 FILE: SYSUAF
     Field Name        Field Value
 ------------------------------------------------------------------------------
             ACCOUNT : HR DB
            USERNAME :  DBCLIENT1
                 UIC : [     426,   DBCLIENT1]
        IDENTIFIERS  : DBUSER                          %X800F4242
                     : DBREPORT                        %X800F4243
          PRIVILEGES :  TMPMBX    NETMBX
*******************************************************************************
             ACCOUNT : HR DB
            USERNAME :  DBCLIENT2
                 UIC : [     426,   DBCLIENT2]
        IDENTIFIERS  : DBUSER                          %X800F4242
                     : DBREPORT                        %X800F4243
          PRIVILEGES :  TMPMBX    NETMBX
*******************************************************************************
             ACCOUNT : HR DB
            USERNAME :  DBCLIENT3
                 UIC : [     426,   DBCLIENT3]
        IDENTIFIERS  : DBUSER                          %X800F4242
                     : DBREPORT                        %X800F4243
          PRIVILEGES :  TMPMBX    NETMBX
*******************************************************************************
             ACCOUNT : HR DB
            USERNAME :  DBOPER
                 UIC : [     426,      DBOPER]
        IDENTIFIERS  : DBOPERATOR                      %X800F4240
                     : DBMAINT                         %X800F4241
                     : DBUSER                          %X800F4242
                     : DBREPORT                        %X800F4243
```

```
          PRIVILEGES :  CMKRNL    TMPMBX    OPER      NETMBX    SYSPRV
*******************************************************************************
             ACCOUNT : HR DB
            USERNAME :  DBUPDATE
                 UIC : [     426,    DBUPDATE]
         IDENTIFIERS  : DBOPERATOR                       %X800F4240
                      : DBUSER                           %X800F4242
                      : DBREPORT                         %X800F4243
           PRIVILEGES :  TMPMBX    NETMBX    GRPPRV
*******************************************************************************
```

Specifying selection criteria

This chapter shows you how to select accounts in your UAF. You can select one or more accounts to appear on reports, etc. by specifying selection criteria.

Where you can use selection criteria
You can specify selection criteria with the /REPORT, /COPY and /MODIFY commands.

Many sets of selection criteria
You can select records based on any item in the UAF. For example, the following command:

```
$ FERRET/REPORT=FLAGS/ACCOUNT=ACC*/BIOLM=5:6/DEVICE=DB*
```

selects accounts based on account name, buffered I/O limit and default device.
Refer to the chapter "FERRET commands" for detailed information on each qualifier.

Specifying multiple criteria
When you specify more than one set of selection criteria, they must all be true for the account to be selected.

Specifying exception criteria
You can specify exception criteria. "-" specifies that all records are selected **except** those matching the criteria. This operator applies to the entire list, not just to the first element. For,

```
/ACCOUNT=(-,FRED,JOAN)
```

the "-" is equivalent to the statement:

```
IF NOT(ACCOUNT=FRED OR ACCOUNT=JOAN)
```

That is, it selects every account **except** FRED and JOAN.

Specifying text strings
Many selection criteria such as /ACCOUNT, /USER, etc. require text strings. You can select:

a single value	/ACCOUNT=ENGR
a list of values	/ACCOUNT=(ENGR,ACCT,SALES)
all accounts except a single value	/ACCOUNT=-ENGR
all accounts except a list of values	/ACCOUNT=(-,ENGR,ACCT,SALES)

NOTE The negation operator applies to the **entire** list, not just the first element.

Specifying wildcards
With the qualifiers /ACCOUNT, /CLI, /CLITABLES, /DATA, /OWNER, /UIC and /USER, you can specify the wildcard characters "*" and "%". For example, the following qualifier:

```
/OWNER=ENG*
```

selects all accounts whose OWNER field starts with the characters "ENG".

Specifying numeric values
Many selection criteria require numeric values. You can select:

a specific value	/BIOLM=35
all values up to and including a value	/BIOLM=:35
a specific value and all higher values	/BIOLM=35:
a range of values	/BIOLM=30:35

NOTE: Use n:m to select an inclusive range (i>=n AND i<=m).

Specifying dates
Several of the selection criteria such as /EXPIRATION, /P_PWDDATE, etc. require dates or deltas. Using dates, you can select:

a specific date	/EXPIRATION=09-JAN-1994
all values up to and including a value	/EXPIRATION=:09-JAN-1994
a specific value and all higher values	/EXPIRATION=09-JAN-1994:
a range of values	/EXPIRATION=01-JAN-1993:09-JAN-1994

Specifying privileges
The selection criteria /DEFPRIVILEGES and /PRIVILEGES require you specify privilege(s). Appendix I contains a complete list of OpenVMS privileges. You can select:

a single privilege	/PRIVILEGES=SYSPRV
the absence of a privilege	/PRIVILEGES=NOSYSPRV
any privilege other than TMPMBX or NETMBX	/PRIVILEGES=ELEVATED
a list of privileges	/PRIVILEGES=(SYSPRV,BYPASS)
all accounts without a single privilege	/PRIVILEGES=-SYSPRV
all accounts without a list of privileges	/PRIVILEGES=(-,SYSPRV,BYPASS)

If you want to select accounts based on the absence of a privilege, put "NO" in front of the privilege. By editing the file FERRET_ELEVATED.DAT you can control which privileges are considered elevated.

NOTE: The negation operator "-" applies to the **entire** list, not just the first element.

Specifying flags
The selection criteria /FLAGS requires flag(s) as values. Appendix J contains a complete list of flags. You can select:

a single flag	/FLAGS=DISMAIL
a list of flags	/FLAGS=(AUTOLOGIN,DISMAIL)
all accounts except a single flag	/FLAGS=-AUTOLOGIN
all accounts except a list of flags	/FLAGS=(-,AUTOLOGIN,DISMAIL)

Specifying access times
The selection criteria /ACCESS, /BATCH, /DIALUP, /INTERACTIVE, /LOCAL, /NETWORK and /REMOTE require access times. You can select:

a specific hour	/ACCESS=(PRIMARY,8)
a range of time	/ACCESS=(PRIMARY,8:5)

If **any** portion of the user record matches the criteria, a match is considered to be true. When the selection criteria is negated, if any portion matches the criteria, the selection is **not** made.

For example, if an account has the following access:

```
       012345678901234567890123
LOCAL  --------#########-------
```

The selection criteria /LOCAL=(PRIMARY,8:17) will select this record because it has local access during some portion of the specified time.

The selection criteria /LOCAL=(-,PRIMARY,8:17) will **not** select this record because it has local access during some portion of the specified time and the selection criteria specify **no** access during the entire period.

ACCESS is a combination of BATCH, DIALUP, LOCAL, NETWORK and REMOTE access times. That is, it is a combination of all five categories. If any of the access periods match, ACCESS will match as well.

INTERACTIVE is a combination of DIALUP, LOCAL and REMOTE access times. If any of the three access periods match, INTERACTIVE will match as well.

Specifying Identifiers
FERRET requires that identifiers be specified as text strings. The /IDENTIFIER qualifier will accept a list of values including wildcarded values. If you negate the qualifier by including a "-" in the list it will be applied to the entire list.

A single identifier	/IDENTIFIER=APPL1
A list of identifiers	/IDENTIFIER=(APPL1, APPL2, APPL3[,...])
Accounts without an identifier(s)	/IDENTIFIER=(-,APPL1[,APPL2,...])

Performing security audits automatically

This chapter shows you how to use FERRET to automate a series of daily and monthly checks on your user authorization file.

Performing daily security audits
Use the DCL procedure DAILY_AUDIT.COM to perform a daily security audit on your UAF. The sample daily audit procedure we've supplied:

runs an audit report
compares the current UAF to yesterday's UAF
makes a daily copy of the current UAF
purges old daily UAF copies

This procedure is self-submitting. Once you start it, it runs every day automatically. You can add additional reports to the sample procedure we've supplied.

This report uses a small default bad password list for checking. Sites with high security considerations should consider editing this command procedure and switching to the more complete bad password list included with Version 5. This list is compiled from an internet source that lists passwords found in multiple hacker dictionaries, increasing the likelihood that an account with one of these passwords could be compromised.

Use the DCL procedure WEEKLY_AUDIT.COM to perform a weekly security audit on your UAF using the much larger and more comprehensive bad_passwd_dictionary.dat included with Ferret V5. Since this check is quite resource intensive we do not recommend running more than weekly except at sites with high security considerations.

It is possible to use both the procedures since the daily audit procedure also generates some additional reports; including a report highlighting chnages in the UAF file since the previous day.

Performing monthly security audits
Use the DCL procedure MONTHLY_AUDIT.COM to perform a monthly security audit on your UAF. The sample monthly audit procedure we've supplied:

compares the current UAF to last month's UAF
runs an audit report using the new Ferret V5 larger bad_passwd_dictionary
disables accounts which have been inactive for 60 days
saves the UAF file for next month's comparison
Optimizes the UAF using the OpenVMS utility CONVERT

This procedure is self-submitting. Once you start it, it runs every month automatically. You can add additional reports to the sample procedure we've supplied.

To start any of these procedures, run them interactively:

```
$ @FERRET_COM:DAILY_AUDIT

$ @FERRET_COM:MONTHLY_AUDIT
```

You will be prompted for a batch queue. The procedures will be automatically submitted to batch. The procedures automatically make any necessary copies of the UAF file so that the batch jobs will be able to generate the differences report.

FERRET and the user authorization file (SYSUAF.DAT)

This chapter discusses the SYSUAF.DAT and its relationship with FERRET.

The User Authorization File (SYSUAF.DAT) is an OpenVMS system file containing important information on every user who is authorized to gain access to the system. Each SYSUAF.DAT record contains the username, password, UIC, privileges and additional information.

It is normally maintained by the OpenVMS utility AUTHORIZE.

It can be read in either user name or UIC sequence.

Typically, there is one record in the UAF for each user that can access the system. There is a record with the user name "DEFAULT" which contains default values used during the creation of new accounts. There are special accounts such as SYSTEST, SYSTEST_CLIG and FIELD for use by Digital personnel.

FERRET can list every item in the UAF except passwords and modify every item except the following:

the primary and secondary password encryption algorithms
the SALT value
the user name

SYSUAF.DAT access
For reporting including auditing and difference checking, FERRET needs read-only access to the file. For modifications and copying, it needs write access. FERRET opens the file shared. Only the current record (not the entire file) is locked during updates.

For more complete information about the User Authorization file refer to the OpenVMS AUTHORIZE manual.

Files you need to use FERRET

This chapter shows you how FERRET and OpenVMS files are used and the amount of disk space they require.

FERRET directory structure
The FERRET directory contains all executables, objects, documentation and command procedures. Here is its structure:

[FERRET	
.CDU]	Command Definition
.COM]	DCL Command Procedures
.DAT]	Data Files
.DEF]	Include Files, SOURCE licenses only
.DOC]	Documentation and HELP text
.EXE]	Executables
.LIS]	Compile Listing Files, SOURCE licenses only
.MAP]	Compile Map Files, SOURCE licenses only
.MSG]	Error Message text and object
.OBJ]	Object Library
.SRC]	FORTRAN Source, SOURCE licenses only

It requires 3500 blocks. If you have source, that directory requires an additional 3000 blocks.

SYSUAF.DAT

FERRET reads information from and writes information to the OpenVMS System User Authorization File. Refer to the chapter "FERRET and the OpenVMS user authorization file (SYSUAF.DAT)" for more information.

Logicals you need to use FERRET

This chapter shows you the logicals that FERRET uses and how to define them.

To use FERRET, you must define several logicals. Here is a description of each logical that may be defined on your system.

FERRET_CDU - This logical points to the [FERRET.CDU] directory. It is used to access the FERRET command definition table. FERRET_CDU is optional.

FERRET_COM - This logical points to the [FERRET.COM] directory. It is used to access FERRET DCL command procedures. FERRET_COM is optional.

FERRET_DAT - This logical points to the [FERRET.DAT] directory. It is used to access the data files and command procedures for mailing. It must be defined in the system logical table. FERRET_DAT is required.

FERRET_DOC - This logical points to the [FERRET.DOC] directory. It is used to access the screen interface help files. It must be defined in the system logical table. FERRET_DOC is required.

FERRET_EXE - This logical points to the [FERRET.EXE.VAX] or the [FERRET.EXE.AXP] directory. It is used to access the FERRET executables. It must be defined in the system logical table. FERRET_EXE is required.

FERRET_PASSWORD - This logical points to the FERRET_PASSWORD.DAT file in [FERRET.DAT] directory. It is used to access the list of poor passwords. It must be defined in the system logical table. FERRET_PASSWORD is required.

FERRET$NOHEADER - This logical suppresses headers on FERRET reports. It must be defined in the system logical table. FERRET$HEADER is optional. Alternatively any specification file can include NOHEAD for the first line to suppress headers and page breaks; this allows for creating flat files only when required and leaves FERRETs default headings, etc. unchanged in other reports.

SYS$LP_LINES - This logical controls how many lines FERRET reports on a single page. The default value, if this logical is not defined, is 60.

SYSUAF - This logical points to the UAF file. The default definition is "SYS$SYSTEM:SYSUAF.DAT". Note that this is a logical defined by OpenVMS rather than a FERRET logical.

FERRET_ELEVATED - This logical can be used to redirect FERRET to a different file and/or location for the list of privileges that should considered elevated.

You can define the basic logicals that FERRET requires by typing:

```
$ @SYS$MANAGER:FERRET_SYSTEM_LOGICALS.COM
```

Any additional logicals should be defined in the FERRET_SITE_LOGICALS.COM procedure. This command procedure is new with V4 and allows you to place site specific logicals in a file that will not be replaced during future upgrades. It is executed by the FERRET_STARTUP.COM procedure.

Privileges you need to use FERRET

This chapter shows you the privileges you need to do various FERRET operations.

FERRET requires the following privileges to run:

- SYSPRV
- TMPMBX
- NETMBX

You can acquire all necessary privileges by typing:

```
$ @FERRET_COM:SET_PRV.COM
```

FERRET Commands

This chapter shows you the purpose of each FERRET command and lists the qualifiers that are valid to use with it. Then it lists all the qualifiers in alphabetical order and describes each qualifier in detail.

It provides a complete command reference "manual" for a FERRET user.

Command syntax
FERRET commands look and act like DCL commands. The commands conform to normal OpenVMS DCL command syntax.

FERRET commands have the format:

```
$ FERRET[/qualifier...] parameter
```

FERRET is the name of the command, /qualifier is the name of a command qualifier and parameter is the name of the user authorization file to be used as input. Lowercase and upper-case characters in command and qualifier names are equivalent. As in DCL, '/', serves as a delimiter and command lines can be continued on to another line by terminating the line with a hyphen, pressing <RETURN> and typing the rest of the command on the next line.

Abbreviating commands
As with DCL, many FERRET commands can be truncated to a unique string, for example, "OUTPUT" can be truncated to "OUT". This provides compact command entry for experienced users. In command procedures, it is best to avoid abbreviating command names and qualifiers. Please refer to the OpenVMS DCL manual for more details.

The maximum length of a DCL command is 256 characters. This may be a problem when you are entering lists of fields or several sets of selection criteria.

Editing command lines
As with DCL, FERRET commands and qualifiers can be edited using terminal keys. Command-line editing is most useful for modifying long command lines.

FERRET command line overview

You can produce reports using the /REPORT qualifier, do global updates based on selection criteria, check your user authorization file for potential problems, compare two user authorization files for differences and copy user records from one user authorization file to another using the /COPY command. Here are examples of FERRET commands:

```
$ FERRET/REPORT/LIST=(UIC,USER,WSDEFAULT,WSQUOTA,WSEXTENT)/SORT=UIC


$ FERRET/REPORT=AUDIT/OUTPUT


$ FERRET/REPORT=DIFFERENCE/UAF_FILE=SYSUAF.OLD


$ FERRET/COPY/UAF_FILE=FALCON::SYSUAF.DAT/UIC=[77,*]


$ FERRET/MODIFY=ASTLM/ASTLM=5:7/INCREMENT=3/ACCOUNT="ACC*"
```

The first command creates a report showing memory quotas by UIC. By default, the file being scanned is SYSUAF.DAT and the output is directed to the screen.

The second command audits the SYSUAF.DAT file. The report will be stored in the file FERRET.LIS.

The third command generates a list of differences between the file SYSUAF.OLD and SYSUAF.DAT.

The fourth command copies records with the UIC [77,*] to the specified user authorization file.

The fifth command adds 3 to the ASTLM for all records whose ASTLM is between 5 and 7 inclusive and whose ACCOUNT name starts with "ACC".

This chapter describes the purpose of each FERRET command and lists the qualifiers that are valid to use with it. Then it lists all the qualifiers in alphabetical order and describes each qualifier in detail.

HELP
The HELP command provides access to FERRET's on-line HELP text.

FERRET's HELP text can be installed into the system help library or into a user help library.

To access FERRET's help, you enter:

```
$ HELP FERRET
```

Qualifiers
This section describes the purpose of each FERRET qualifier. Then it lists all the qualifiers in alphabetical order and describes each qualifier in detail.

Qualifier syntax
FERRET qualifiers look and act like DCL qualifiers. They conform to normal OpenVMS DCL command qualifier syntax.

A qualifier consists of a keyword, or a keyword followed by a value. The keyword starts with a slash. All qualifiers apply to the entire command. FERRET qualifiers have one of the following formats:

```
FERRET/qualifier

FERRET/qualifier=x
```

Depending on the qualifier, "x" can be an alphanumeric value, a numeric value, a file name, a device, a directory, a date or a delta time).

Most of the qualifiers have defaults.

FERRET qualifier list

This page contains a complete list of all FERRET qualifiers. Subsequent pages contain detailed descriptions of each qualifier.

/ACCESS	Specify selection criteria
/ACCOUNT	Specify selection criteria
/ADD_IDENTIFIER	Specify that identifiers are to be copied
/ALL	Control selection in flags, privileges report
/ASTLM	Specify selection criteria
/BATCH	Specify selection criteria
/BIOLM	Specify selection criteria
/BYTLM	Specify selection criteria
/CLI	Specify selection criteria
/CLITABLES	Specify selection criteria
/CONFIRM	Confirm account copy or modification
/COPY	Copy records from one SYSUAF to another
/CPUTIME	Specify selection criteria
/DATA	Specify selection criteria
/DECREMENT	Decrease the value of a numeric field
/DEFPRIVILEGES	Specify selection criteria
/DEVICE	Specify selection criteria
/DIALUP	Specify selection criteria
/DIOLM	Specify selection criteria
/DIRECTORY	Specify selection criteria
/ENQLM	Specify selection criteria
/EXCLUDE	Control which items /REPORT=AUDIT checks
/EXPIRATION	Specify selection criteria
/FILLM	Specify selection criteria
/FLAGS	Specify selection criteria
/FORMAT	Specify report format
/I_LASTLOGIN	Specify selection criteria
/IDENTIFIER	Specify selection criteria
/IGNORE	Specify a list of field changes to ignore
/INCREMENT	Increase the value of a numeric field
/INTERACTIVE	Specify selection criteria
/JTQUOTA	Specify selection criteria
/LEGEND	Print list of abbreviation meanings
/LGICMD	Specify selection criteria
/LIST	Specify a list of report fields
/LOCAL	Specify selection criteria
/LOGFAILS	Specify selection criteria
/MAXACCTJOBS	Specify selection criteria
/MAXDETACH	Specify selection criteria
/MAXIMUM	Specify a maximum for a numeric field
/MAXJOBS	Specify selection criteria
/MINIMUM	Specify a minimum for a numeric field

/MODIFY	Cause the specified field to be modified
/N_LASTLOGIN	Specify selection criteria
/NETWORK	Specify selection criteria
/OUTPUT	Specify the destination of output
/OWNER	Specify selection criteria
/P_ENCRYPT	Specify selection criteria
/P_PASSWORD	Specify selection criteria
/P_PWDDATE	Specify selection criteria
/PASSWORD_FILE	Specify a file listing bad passwords that audit should check for
/PBYTLM	Specify selection criteria
/PGFLQUOTA	Specify selection criteria
/PRCLM	Specify selection criteria
/PRIMEDAYS	Specify selection criteria
/PRIORITY	Specify selection criteria
/PRIVILEGES	Specify selection criteria
/PWDEXPIRED	Specify selection criteria
/PWDLIFETIME	Specify selection criteria
/PWDMINIMUM	Specify selection criteria
/QUEPRI	Specify selection criteria
/REMOTE	Specify selection criteria
/REPORT	Specify a report to be generated
/S_ENCRYPT	Specify selection criteria
/S_PASSWORD	Specify selection criteria
/S_PWDDATE	Specify selection criteria
/SALT	Specify selection criteria
/SET	Specify a new value for a field
/SHRFILLM	Specify selection criteria
/SORT	Specify the sequence of a report
/SPECIFICATION	Specify a file containing report fields
/STATISTICS	Specify file statistics during operations
/TITLE	Specify the title for a report
/TQELM	Specify selection criteria
/TRUNCATE	Specify whether fields are to be truncated
/TYPE	Specify UIC format
/UAF_FILE	Specify a SYSUAF.DAT (/MODIFY, /COPY, and /REPORT=DIFFERENCES)
/UIC	Specify selection criteria
/USER	Specify selection criteria
/VERSION	Display FERRET version
/WIDTH	Specify report width
/WSDEFAULT	Specify selection criteria
/WSEXTENT	Specify selection criteria
/WSQUOTA	Specify selection criteria

/ACCESS

Use this qualifier to control whether only those records including the specified access time are selected. If you omit the qualifier, access time is not used to select records. ACCESS time is a combination of BATCH, DIALUP, LOCAL, NETWORK and REMOTE. If any of these include a portion of the specified time, the record is selected. See the section "Specifying access times" in the chapter "Specifying selection criteria" for more details.

FORMAT

/ACCESS=([-,]PRIMARY,[n:m],[n][,...]
SECONDARY,[n:m],[n],[,...])

KEYWORDS

"-"

Specifies that all records are selected except those matching any specified access time. This operator applies to the entire list, not just to the first element.

PRIMARY

Specifies the primary access times.

SECONDARY

Specifies the secondary access times.

access-time[,...]

Specifies the access time used to select records. The access time matches the access time specified in the user authorization file.

When you specify this qualifier, specify at least one access time. Specify hours as integers from 0 to 23 inclusive. Hours may be specified as single hours (n), or as ranges of hours (n:m). Note that the syntax shown here is different from that used by AUTHORIZE. 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. If you specify more than one access time, separate them with commas, and enclose the list in parentheses.

EXAMPLES

$ FERRET/REPORT/LIST=(USER,ASTLM)/ACCESS=(PRIMARY,8:17)

Generate a report for all accounts whose primary access time includes all or part of the period 8 a.m. to 5 p.m. in one or more of the access types.

$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,ACCESS)/ACCESS=(-,SECONDARY,23)/FORMAT=ROW

Generate a report in UIC sequence for all accounts except those with a secondary access time of 11 p.m.

/ACCOUNT

Use this qualifier to control whether only those records matching the specified account name are selected. If you omit the qualifier, account name is not used to select records.

FORMAT

/ACCOUNT=([-,]account-name[,...])

KEYWORDS

"-"

Specifies that all records are selected except those matching any specified account name. This operator applies to the entire list, not just to the first element.

account name[,...]

Specifies the account name used to select records. The account name is 1 through 8 alphanumeric characters. The account name matches the account name specified in the user authorization file.

When you specify this qualifier, specify at least one account name. You can specify up to 64 account names. If you specify an account name more than once, FERRET counts and uses only the first reference. If you specify more than one account name, separate them with commas, and enclose the list in parentheses. You can use the wildcard characters "*" and "%" in account names. When you specify a list, the account will be selected if it matches one or more of the elements in the list.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,ASTLM)/ACCOUNT=ENG
```

Generate a report for the ENG account.

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI)/ACCOUNT=(-,ACC*)
```

Generate a report in UIC sequence for all accounts except those starting with "ACC".

/ADD_IDENTIFER

Use this qualifier to control whether identifiers are copied when accounts are copied using /COPY. If you omit the qualifier, identifiers are not be copied.

FORMAT

/ADD_IDENTIFIER
/NOADD_IDENTIFER (default)

KEYWORDS

None

EXAMPLES

```
$ FERRET/COPY/UAF_FILE=SYS$MANAGER:SYSUAF.77/UIC=[77,*]/ADD_IDENTIFIER
```

Copy all [77,*] records from the default SYSUAF.DAT to SYSUAF.77.

/ALL

Use this qualifier in conjunction with the /FLAGS, /DEFPRIVILEGES and /PRIVILEGES qualifiers to control whether all accounts (even those without any flags or privileges) are include in the report. If you negate the qualifier, only accounts with at least one flag (or privilege) are included. The default is /ALL which includes all accounts including those with no flags or privileges at all.

FORMAT

/ALL
/NOALL

KEYWORDS

None

EXAMPLES

```
$ FERRET/REPORT=FLAGS/NOALL/FLAGS=-Disctly
```

Generate a flags report for accounts which do not have the Disctly flag set. Because /NOALL is specified, only accounts with at least one flag will be included on the report.

/ASTLM

Use this qualifier to control whether only those records matching the specified AST limit are selected. If you omit the qualifier, the AST limit is not used to select records.

FORMAT

/ASTLM=[-] [n] [n:m] [n:] [:m]

KEYWORDS

"-"

Specifies that all records are selected except those matching the specified AST limit.

[n] [n:m] [n:] [:m]

Specifies the AST limit used to select records. The AST limit specifies the maximum number of AST's the user can have queued at one time. Specify the AST limit as an integer with a minimum value of 2. An AST limit of 0 indicates unlimited AST's are allowed. The AST limit matches the AST limit specified in the user authorization file.

Specify n:m to select an inclusive range of AST limits using the relationship (i>=n AND i<=m). Specify n to select a specific AST limit. Specify n: to select an AST limit and all higher values. Specify :m to select an AST limit and all lower values.

This is not a list; you must specify one and only one of the selections.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,ASTLM)/ASTLM=5:
```

Generate a report for all accounts with AST limits of 5 or more

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,ASTLM)/ASTLM=-7
```

Generate a report in UIC sequence for all accounts except those with AST limits of 7.

/BATCH

Use this qualifier to control whether only those records matching the specified access time for batch jobs are selected. If you omit the qualifier, access time for batch jobs is not used to select records. See the section "Specifying access times" in the chapter "Specifying selection criteria" for more details.

FORMAT

/BATCH=([-,]PRIMARY,[n:m],[n] [,...]
SECONDARY,[n:m],[n],[,...])

KEYWORDS

"-"

Specifies that all records are selected except those matching any specified access time for batch jobs. This operator applies to the entire list, not just to the first element.

PRIMARY

Specifies the primary access times.

SECONDARY

Specifies the secondary access times.

access-time[,...]

Specifies the access time used to select records. The access time matches the access time specified for batch jobs in the user authorization file.

When you specify this qualifier, specify at least one access time. Specify hours as integers from 0 to 23 inclusive. Hours may be specified as single hours (n), or as ranges of hours (n:m). If the ending hour of a range is earlier than the starting hour, the range extends from the starting hour through midnight to the ending hour. The first set of hours after the keyword PRIMARY specifies hours on primary days; the second set of hours after the keyword SECONDARY specifies hours on secondary days. Note that hours are *inclusive*; that is, if you grant access during a given hour, access extends to the end of that hour. If you specify more than one access time, separate them with commas, and enclose the list in parentheses.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,ASTLM,BATCH)/BATCH=(PRIMARY,8:17)/FORMAT=ROW
```

Generate a report for all accounts whose primary access time for batch jobs includes all or part of the period 8 a.m. to 5 p.m.

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,BATCH)/BATCH=(-,SECONDARY,23)/FORMAT=ROW
```

Generate a report in UIC sequence for all accounts except those with a secondary access time for batch jobs of 11 p.m.

/BIOLM

Use this qualifier to control whether only those records matching the specified BIO limit are selected. If you omit the qualifier, the buffered IO limit is not used to select records.

FORMAT

/BIOLM=[-] [n] [n:m] [n:] [:m]

KEYWORDS

"-"

Specifies that all records are selected except those matching the specified BIO limit.

[n] [n:m] [n:] [:m]

Specifies the BIO limit used to select records. The BIO limit specifies the maximum number of BIO's such as terminal IO the user can have queued at one time. Specify the BIO limit as an integer. The BIO limit matches the BIO limit specified in the user authorization file.

Specify n:m to select an inclusive range of BIO limits using the relationship (i>=n AND i<=m). Specify n to select a specific BIO limit. Specify n: to select a BIO limit and all higher values. Specify :m to select a BIO limit and all lower values.

This is not a list; you must specify one and only one of the selections.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,BIOLM)/BIOLM=5:
```

Generate a report for all accounts with BIO limits of 5 or more

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,BIOLM)/BIOLM=-7
```

Generate a report in UIC sequence for all accounts except those with BIO limits of 7.

/BYTLM

Use this qualifier to control whether only those records matching the specified buffered IO byte limit are selected. If you omit the qualifier, the byte limit is not used to select records.

FORMAT

/BYTLM=[-] [n] [n:m] [n:] [:m]

KEYWORDS

"-"

Specifies that all records are selected except those matching the specified buffered IO byte limit.

[n] [n:m] [n:] [:m]

Specifies the buffered IO byte limit used to select records. The byte limit specifies the maximum number of bytes of nonpaged system dynamic memory that the user can have queued at one time. Specify the byte limit as an integer. The byte limit matches the byte limit specified in the user authorization file.

Specify n:m to select an inclusive range of byte limits using the relationship (i>=n AND i<=m). Specify n to select a specific byte limit. Specify n: to select a byte limit and all higher values. Specify :m to select a byte limit and all lower values.

This is not a list; you must specify one and only one of the selections.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,BYTLM)/BYTLM=1024:
```

Generate a report for all accounts with byte limits of 1024 or more

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,BYTLM)/BYTLM=-:2048
```

Generate a report in UIC sequence for all accounts except those with byte limits of 2048 or less.

/CLI

Use this qualifier to control whether only those records matching the specified command line interpreter (CLI) are selected. If you omit the qualifier, CLI name is not used to select records.

FORMAT

/CLI=([-,]cli-name[,...])

KEYWORDS

"-"

Specifies that all records are selected except those matching any specified CLI name. This operator applies to the entire list, not just to the first element.

CLI name[,...]

Specifies the CLI name used to select records. The CLI name is 1 through 12 alphanumeric characters. Normally, it is either DCL or MCR. The CLI name matches the CLI name specified in the user authorization file.

When you specify this qualifier, specify at least one CLI name. You can specify up to 64 CLI names. If you specify a CLI name more than once, FERRET counts and uses only the first reference. If you specify more than one CLI name, separate them with commas, and enclose the list in parentheses. You can use the wildcard characters "*" and "%" in CLI names. When you specify a list, the account will be selected if it matches one or more of the elements in the list.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,CLI)/CLI=MCR
```

Generate a report for all accounts with MCR as their CLI name.

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI)/CLI=(-,DCL,MCR)
```

Generate a report in UIC sequence for all accounts except those with DCL or MCR as their CLI names.

/CLITABLES

Use this qualifier to control whether only those records matching the specified command line interpreter (CLI) tables are selected. If you omit the qualifier, CLITABLES name is not used to select records.

FORMAT

/CLITABLES=([-,]clitable-name[,...])

KEYWORDS

"-"

Specifies that all records are selected except those matching any specified CLITABLE name. This operator applies to the entire list, not just to the first element.

CLI table name[,...]

Specifies the CLI table name used to select records. The CLI table name is 1 through 31 alphanumeric characters. The CLI table name matches the CLI table name specified in the user authorization file.

When you specify this qualifier, specify at least one CLI table name. You can specify up to 64 CLI names. If you specify a CLI name more than once, FERRET counts and uses only the first reference. If you specify more than one CLI table name, separate them with commas, and enclose the list in parentheses. You can use the wildcard characters "*" and "%" in CLI names. When you specify a list, the account will be selected if it matches one or more of the elements in the list.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,CLI,CLITABLES)/CLITABLES=CAD.EXE
```

Generate a report for all accounts with CAD.EXE as their CLI table name.

```
$ FERRET/REPORT/LIST=(USER,CLITABLES)/CLITABLES=(-,DCLTABLES)
```

Generate a report for all accounts except those with DCLTABLES as their CLI table names.

/CONFIRM

Use this qualifier with /COPY or /MODIFY to control whether records matching the selection criteria are affected. FERRET will display the user name of each record. You can enter:

YES	perform the operation
NO	do not perform the operation but continue processing
CTRL/Z	return to the DCL prompt

If you omit the qualifier, all selected records are copied or modified.

FORMAT

/CONFIRM

KEYWORDS

None

EXAMPLES

```
$ FERRET/COPY/UAF_FILE=TMP.DAT/CONFIRM/UIC=[1,*]
```

Copy all accounts with the UIC group 1 requesting confirmation before each copy.

```
$ FERRET/MODIFY=ASTLM/SET=35/CONFIRM/ACCOUNT=ACC*
```

Set ASTLM to 35 in all accounts starting with "ACC" requesting confirmation before each update.

/COPY

Use this qualifier to copy selected records from one user authorization file to another You must specify the UAF_FILE qualifier when you specify the /COPY qualifier. You can only specify one of the following qualifiers in a single FERRET command:

/COPY
/MODIFY
/REPORT

If the file specified by /UAF_FILE doesn't exist, FERRET asks you whether you want to create it. This is the same procedure as AUTHORIZE uses.

FORMAT

/COPY

KEYWORDS

None

EXAMPLES

```
$ FERRET/COPY/UAF_FILE=SYS$MANAGER:SYSUAF.77/UIC=[77,*]
```

Copy all [77,*] records from the default SYSUAF.DAT to SYSUAF.77.

```
$ FERRET/COPY/UAF_FILE=VAX1::SYS$MANAGER:SYSUAF.OLD/USER=ACC*
```

Copy all the accounts with usernames starting with ACC from the default SYSUAF to the specified file.

/CPUTIME

Use this qualifier to control whether only those records matching the specified CPU time limit, in seconds, are selected. If you omit the qualifier, the CPU time limit is not used to select records.

FORMAT

/CPUTIME=[-] [n] [n:m] [n:] [:m]

KEYWORDS

"-"

Specifies that all records are selected except those matching the specified CPU time limit.

[n] [n:m] [n:] [:m]

Specifies the CPU time limit used to select records. The CPU time limit specifies the maximum number of CPU seconds that the user can take per session. Specify the CPU time limit as **an integer number of seconds**. The CPU time limit matches the CPU time limit specified in the user authorization file.

Specify n:m to select an inclusive range of CPU time limits using the relationship (i>=n AND i<=m). Specify n to select a specific CPU time limit. Specify n: to select a CPU time limit and all higher values. Specify :m to select a CPU time limit and all lower values.

This is not a list; you must specify one and only one of the selections.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,CPUTIME)/CPUTIME=115:
```

Generate a report for all accounts with CPU time limits of 115 or more

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,CPUTIME)/CPUTIME=-0
```

Generate a report in UIC sequence for all accounts except those with infinite CPU time limits

/DATA

Use this qualifier to control whether only those records matching the specified user data area are selected. If you omit the qualifier, the user data area is not used to select records.

FORMAT

/DATA=([-,]text-string[,...])

KEYWORDS

"-"

Specifies that all records are selected except those matching any specified user data area.

text-string[,...]

Specifies the user data area used to select records. The user data area is 1 through 255 bytes. You can only select using alphanumeric characters; you cannot select using binary formats such as integer or byte. The user data area matches the user data area specified in the user authorization file. FERRET allows you to list and modify the user data area; AUTHORIZE does not.

When you specify this qualifier, specify at least one text string. You can specify up to 64 text strings. If you specify a text string more than once, FERRET counts and uses only the first reference. If you specify more than one value, separate them with commas, and enclose the list in parentheses. You can use the wildcard characters "*" and "%" in user data area values. When you specify a list, the account will be selected if it matches one or more of the elements in the list. If you include strings with embedded blanks, enclose them in quotes.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,ASTLM)/DATA="ENG DEPARTMENT"
```

Generate a report for accounts with the characters "ENG DEPARTMENT" in the user data area.

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI)/DATA=(-,ACC*)
```

Generate a report in UIC sequence for all accounts except those with "ACC" in the user data area.

/DECREMENT

Use this qualifier to decrease the field specified by /MODIFY by a specified amount. When you specify /MODIFY, you must specify one and only one of the following groups of qualifiers:

{/INCREMENT | /DECREMENT}

{/MAXIMUM | /MINIMUM}

{/SET}

If you specify /DECREMENT, you cannot specify /INCREMENT in the same command.

If you specify /DECREMENT or /INCREMENT, you cannot specify /SET in the same command.

FORMAT

/DECREMENT=n

KEYWORDS

n

Specifies the amount by which the field specified by /MODIFY is to be decreased. Specify the decrement as an integer. If the field is smaller than the decrement, FERRET sets the field to its lowest valid value, usually zero.

This qualifier can only be used with integer fields. It cannot be used with OpenVMS date-time fields.

EXAMPLES

```
$ FERRET/MODIFY=BYTLM/DECREMENT=256/ACCOUNT=RDB*
```

Reduce the BYTLM field by 256 in all accounts which start with RDB

```
$ FERRET/MODIFY=ASTLM/DECREMENT=5
```

Reduce the ASTLM field by 5 in all accounts

/DEFPRIVILEGES

Use this qualifier to control whether only those records matching the specified default privileges are selected. If you omit the qualifier, default privileges are not used to select records.

FORMAT

/DEFPRIVILEGES=([-,] [NO]privilege[,...])

KEYWORDS

"-"

Specifies that all records are selected except those matching any specified default privilege. This operator applies to the entire list, not just to the first element. Accounts with no DEFPRIVILEGES will be included (see /ALL).

privilege[,...]

Specifies the default privileges used to select records. A list of valid privileges is contained in Appendix I. Specify the absence of a privilege by placing "NO" in front of the privilege name. The default privileges match the default privileges specified in the user authorization file.

When you specify this qualifier, specify at least one privilege. You can specify up to 35 privileges. If you specify a privilege more than once, FERRET counts and uses only the first reference. If you specify more than one privilege, separate them with commas, and enclose the list in parentheses. When you specify a list, the account will be selected if it matches one or more of the elements in the list.

EXAMPLES

```
$ FERRET/REPORT/LIST=USER/DEFPRIVILEGES=(CMKRNL,SYSPRV)
```

Generate a report of all accounts which have the CMKRNL or SYSPRV as a default privilege.

```
$ FERRET/REPORT/LIST=(USER,UIC,DEFPRIVILEGES)/DEFPRIVILEGES=(-,TMPMBX)/FORMAT=ROW
```

Generate a report for all accounts which don't have the TMPMBX privilege. Specify a ROW formatted report to list all privileges. Use /NOALL to exclude users with no default privileges.

/DESCENDING

Use this qualifier when generating list reports to have the reported sorted in descending order on whatever /sort key has been chosen instead of ascending. If this qualifier is not specified the report will be sorted in ascending order.

FORMAT

/DESCENDING

KEYWORDS

This qualifier has no keywords and is not negatable.

EXAMPLES

$ ferret /report /specification=memlq /sort=pgflquota /descending

Generate the preformatted memory quota report sorted in descending order by pgflquota.

$ ferret/report/specification=login/sort=i_lastlogin/descending

Generate the login report sorted by the last interactive login in descending order. This report would show all users from those that have logged in most recently to those that have never logged in.

/DEVICE

Use this qualifier to control whether only those records matching the specified default device at login are selected. If you omit the qualifier, device is not used to select records.

FORMAT

/DEVICE=([-,]device-name[,...])

KEYWORDS

"-"

Specifies that all records are selected except those matching any specified default device name. This operator applies to the entire list, not just to the first element.

device name[,...]

Specifies the default device name used to select records. The device name is 1 through 31 alphanumeric characters. The device name matches the device name specified in the user authorization file.

When you specify this qualifier, specify at least one device name. You can specify up to 64 device names. If you specify a device name more than once, FERRET counts and uses only the first reference. If you specify more than one device name, separate them with commas, and enclose the list in parentheses. When you specify a list, the account will be selected if it matches any of the elements in the list. Device names may be wildcarded.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,SHRFILLM)/DEVICE=DUA0:
```

Generate a report for all accounts with the default device DUA0:.

```
$ FERRET/REPORT/LIST=(USER,UIC,DEVICE)/DEVICE=-DUB2:
```

Generate a report for all accounts except those with the default device DUB2:

/DIALUP

Use this qualifier to control whether only those records including the specified access time for dialup jobs are selected. If you omit the qualifier, access time for dialup jobs is not used to select records. See the section "Specifying access times" in the chapter "Specifying selection criteria" for more details.

FORMAT

/DIALUP=([-,]PRIMARY,[n:m],[n] [,...]
SECONDARY,[n:m],[n],[,...])

KEYWORDS

"-"

Specifies that all records are selected except those matching any specified access time for dialup jobs. This operator applies to the entire list, not just to the first element.

PRIMARY

Specifies the primary access times.

SECONDARY

Specifies the secondary access times.

access-time[,...]

Specifies the access time for dialup jobs used to select records. The access time matches the access time for dialup jobs specified in the user authorization file.

When you specify this qualifier, specify at least one access time. Specify hours as integers from 0 to 23 inclusive. Hours may be specified as single hours (n), or as ranges of hours (n:m). If the ending hour of a range is earlier than the starting hour, the range extends from the starting hour through midnight to the ending hour. The first set of hours after the keyword PRIMARY specifies hours on primary days; the second set of hours after the keyword SECONDARY specifies hours on secondary days. Note that hours are *inclusive*; that is, if you grant access during a given hour, access extends to the end of that hour. If you specify more than one access time, separate them with commas, and enclose the list in parentheses.

EXAMPLES

$ FERRET/REPORT/LIST=(USER,ASTLM)/DIALUP=(PRIMARY,8:17)

Generate a report for all accounts whose primary access time for dialup jobs includes all or part of the period 8 a.m. to 5 p.m.

$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,DIALUP)/DIALUP=(-,SECONDARY,23)/FORMAT=ROW

Generate a report in UIC sequence for all accounts except those with a secondary access time for dialup jobs of 11 p.m.

/DIOLM

Use this qualifier to control whether only those records matching the specified direct IO limit are selected. If you omit the qualifier, the direct IO limit is not used to select records.

FORMAT

/DIOLM=[-] [n] [n:m] [n:] [:m]

KEYWORDS

"-"

Specifies that all records are selected except those matching the specified DIO limit.

[n] [n:m] [n:] [:m]

Specifies the DIO limit used to select records. The DIO limit specifies the maximum number of DIO's such as disk IO the user can have queued at one time. Specify the DIO limit as an integer. The DIO limit matches the DIO limit specified in the user authorization file.

Specify n:m to select an inclusive range of DIO limits using the relationship (I>=n AND I<=m). Specify n to select a specific DIO limit. Specify n: to select a DIO limit and all higher values. Specify :m to select a DIO limit and all lower values.

This is not a list; you must specify one and only one of the selections.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,DIOLM)/DIOLM=5:
```

Generate a report for all accounts with DIO limits of 5 or more

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,DIOLM)/DIOLM=-:7
```

Generate a report in UIC sequence for all accounts except those with DIO limits of 7 or less.

/DIRECTORY

Use this qualifier to control whether only those records matching the specified default directory at login are selected. If you omit the qualifier, directory is not used to select records.

FORMAT

/DIRECTORY=([-,]directory-name[,...])

KEYWORDS

"-"

Specifies that all records are selected except those matching any specified default directory name. This operator applies to the entire list, not just to the first element.

directory name[,...]

Specifies the default directory name used to select records. The directory name is 1 through 63 alphanumeric characters. The directory name matches the directory name specified in the user authorization file.

When you specify this qualifier, specify at least one directory name. You can specify up to 64 directory names. If you specify a directory name more than once, FERRET counts and uses only the first reference. If you specify more than one directory name, separate them with commas, and enclose the list in parentheses. When you specify a list, the account will be selected if it matches one or more of the elements in the list. You can use the wildcard characters "*" and "%" in directory names.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,SHRFILLM)/DIRECTORY=[ENGDIR]
```

Generate a report for all accounts with the default directory [ENGDIR].

```
$ FERRET/REPORT/LIST=(USER,DIRECTORY)/DIRECTORY=(-,[ACT])
```

Generate a report for all accounts except those with the default directory [ACT]

/ENQLM

Use this qualifier to control whether only those records matching the specified lock queue limit are selected. If you omit the qualifier, the lock queue limit is not used to select records.

FORMAT

/ENQLM=[-] [n] [n:m] [n:] [:m]

KEYWORDS

"-"

Specifies that all records are selected except those matching the specified lock queue limit.

[n] [n:m] [n:] [:m]

Specifies the lock queue limit used to select records. The lock queue limit specifies the maximum number of lock queue's the user can have queued at one time. Specify the lock queue limit as an integer with a minimum value of 2. The lock queue limit matches the lock queue limit specified in the user authorization file.

Specify n:m to select an inclusive range of lock queue limits using the relationship (I>=n AND I<=m). Specify n to select a specific lock queue limit. Specify n: to select a lock queue limit and all higher values. Specify :m to select a lock queue limit and all lower values.

This is not a list; you must specify one and only one of the selections.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,ENQLM)/ENQLM=5:
```

Generate a report for all accounts with lock queue limits of 5 or more

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,ENQLM)/ENQLM=-:7
```

Generate a report in UIC sequence for all accounts except those with lock queue limits of 7 or less.

/EXCLUDE

Use this qualifier to control which checks FERRET makes when you are generating an audit report. If you omit the qualifier FERRET will make all of its audit checks on the UAF.

FORMAT

/EXCLUDE=(keyword,...)

KEYWORDS

keyword[,...]

Specifies the checks that FERRET will omit from the audit report. Choose one or more of the following keywords:

DISUSER	Do not report accounts that are marked DISUSER
	Do not report accounts that are not marked DISUSER but that Digital recommends should be
EXPIRED	Do not report accounts that have expired
FILE	Do not check UAF file ownership
	Do not check UAF file protections
LOGFAIL	Do not report accounts that have had an excessive number of login failures
LOGIN	Do not report accounts that have never logged in
	Do not report accounts that have no recent logins
PASSWORD	Do not report interactive accounts that are marked preexpired
	Do not report accounts with passwords shorter than the minimum length set in the UAF for that account
	Do not report SYSTEM if its password is less than 8 characters
	Do not check passwords to see if they are easily guessed or are included in the FERRET_PASSWORD.DAT file of passwords that should not be used
	Do not report accounts that do not have passwords
	Do not report accounts that have not changed their password for a long time
PRIORITY	Do not report accounts that have an elevated base priority
UIC	Do not report accounts that have duplicate UICs
	Do not report accounts that have no UIC

EXAMPLES

```
$ FERRET/REPORT=AUDIT/EXCLUDE=(PRIORITY,FILE,LOGFAIL)
```

Generate an audit report performing all the checks except the ones for elevated priority, excessive logfail counts and the checks on the UAF file protection and owner.

/EXPIRATION

Use this qualifier to control whether only those records matching the specified expiration date are selected. If you omit the qualifier, expiration date is not used to select records.

FORMAT

/EXPIRATION=[-] [n] [n:m] [n:] [:m]

KEYWORDS

"-"

Specifies that all records are selected except those matching the specified expiration. This operator applies to the entire list, not just to the first element.

[n] [n:m] [n:] [:m]

Specifies the expiration date used to select records. The expiration date is the date after which the account has expired and cannot be logged into. Specify the expiration date as a date or a delta time. You cannot include a time-of-day (11:38) as part of the date or delta time. The expiration date matches the expiration date specified in the user authorization file.

Specify n:m to select an inclusive range of expiration dates using the relationship (I>=n AND I<=m). Specify n to select a specific expiration date. Specify n: to select a expiration date and all higher values. Specify :m to select a expiration date and all lower values. You cannot specify a range of delta times.

When you specify a delta time, it applies to the future.

This is not a list; you must specify one and only one of the selections.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,EXPIRATION)/EXPIRATION=25-FEB-1994
```

Generate a list of all accounts which expire on February 25, 1994

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI)/EXPIRATION=0
```

Generate a report in UIC sequence for all accounts which don't have an expiration date.

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI)EXPIRATION=7
```

Generate a report in UIC sequence for all accounts which expire within a week.

/FILLM

Use this qualifier to control whether only those records matching the specified file limit are selected. If you omit the qualifier, the file limit is not used to select records.

FORMAT

/FILLM=[-] [n] [n:m] [n:] [:m]

KEYWORDS

"-"

Specifies that all records are selected except those matching the specified file limit.

[n] [n:m] [n:] [:m]

Specifies the file limit used to select records. The file limit specifies the maximum number of files the user may have open at one time. Specify the file limit as an integer. The file limit matches the file limit specified in the user authorization file.

Specify n:m to select an inclusive range of file limits using the relationship (I>=n AND I<=m). Specify n to select a specific file limit. Specify n: to select a file limit and all higher values. Specify :m to select a file limit and all lower values.

This is not a list; you must specify one and only one of the selections.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,FILLM,SHRFILLM)/FILLM=5:
```

Generate a report for all accounts with file limits of 5 or more

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,FILLM)/FILLM=-:7
```

Generate a report in UIC sequence for all accounts except those with file limits of 7 or less.

/FLAGS

Use this qualifier to control whether only those records matching the specified flags are selected. If you omit the qualifier, flags are not used to select records.

FORMAT

/FLAGS=([-,] [NO]flag[,...])

KEYWORDS

"-"

Specifies that all records are selected except those matching any specified flags. This operator applies to the entire list, not just to the first element. Accounts with no flags will be included (see /ALL).

flags[,...]

Specifies the flags used to select records. A list of valid flags is contained in Appendix J. Specify the absence of a flag by placing "NO" in front of the flag name. The flags match the flags specified in the user authorization file.

When you specify this qualifier, specify at least one flag. You can specify up to 18 flags. If you specify a flag more than once, FERRET counts and uses only the first reference. If you specify more than one flag, separate them with commas, and enclose the list in parentheses. When you specify a list, the account will be selected if it matches one or more of the elements in the list.

Use /NOALL if you want to exclude accounts with no flags from a negated list.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,FLAGS)/FLAGS=(AUDIT,DISUSER)/FORMAT=ROW
```

Generate a report of all accounts which have the AUDIT or DISUSER flags.

```
$ FERRET/REPORT/LIST=(USER,UIC)/FLAGS=(-,DISMAIL)
```

Generate a report for all accounts which don't have the DISMAIL flag.

/FORMAT

Use this qualifier to specify the format of the report specified by /REPORT.

FORMAT

/FORMAT=[ROW] [COLUMN]

KEYWORDS

ROW

Specifies that the report is to be produced with one field per line.

COLUMN

Specifies that the report is to be produced with one record per line.

The qualifier /TRUNCATE specifies the maximum width of a column report. The default value is 132. If the report line is longer than the maximum width, it will wrap or be truncated depending on the printer characteristics.

If you specify ROW, you cannot specify COLUMN or /TRUNCATE.

If you specify COLUMN,
you cannot specify ROW
you may specify /TRUNCATE

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,UIC)/FORMAT=ROW
```

Generate a row report using the default SYSUAF.DAT. The report goes to FERRET.LIS.

```
$ FERRET/REPORT/SPEC=RPT/FORMAT=COLUMN/TRUNCATE=80
```

Generate a column report with a maximum width of 80. The report line will be truncated if it is longer than 80 characters.

/I_LASTLOGIN

Use this qualifier to control whether only those records matching the specified last interactive login date are selected. If you omit the qualifier, interactive login is not used to select records.

The qualifiers I_LASTLOGIN and N_LASTLOGIN are related.

FORMAT

/I_LASTLOGIN=[-] [n] [n:m] [n:] [:m]

KEYWORDS

"-"

Specifies that all records are selected except those matching the specified interactive login date.

[n] [n:m] [n:] [:m]

Specifies the last interactive login date used to select records. The last interactive login date specifies the last time a non-batch login completed successfully for this account. Specify the last interactive login as a date or a delta value. You cannot include a time-of-day (11:38) as part of the date or delta time. The last interactive login date matches the last interactive login date recorded in the user authorization file.

Specify n:m to select an inclusive range of last interactive login dates using the relationship (I>=n AND I<=m). Specify n to select a specific last login date. Specify n: to select a particular last interactive login and all higher values. Specify :m to select a particular last interactive login and all lower values. You cannot specify a range of delta times.

A delta time selects all accounts which have logged in during the last n days. When you specify a delta time, it applies to the past.

This is not a list; you must specify one and only one of the selections.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,I_LASTLOGIN)/I_LASTLOGIN=5
```

Generate a report for all accounts with last interactive login within the last 5 days

```
$ FERRET/REPORT/LIST=(USER,I_LASTLOGIN)/I_LASTLOGIN=-30
```

Generate a report for all accounts which haven't logged in within the last 30 days

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,I_LASTLOGIN)/I_LASTLOGIN=0
```

Generate a report in UIC sequence for all accounts which have never logged in.

/IDENTIFIER

Use this qualifier to control whether only those records that have the specified identifier included in their rights are selected. If you omit the qualifier, identifier is not used to select records.

FORMAT

/IDENTIFIER=([-,]identifier[,...])

KEYWORDS

"-"

Specifies that all records except those holding this identifier(s) are included.

identifier[,...]

Specifies the identifier used to select records. Identifiers are usually single word text strings. The identifier matches a defined rights identifier in the rightslist.dat file that has been granted to one or more users.

When you specify this qualifier, specify at least one identifier. You can specify up to 64 identifiers. If you specify an identifier more than once, FERRET counts and uses only the first reference. If you specify more than one identifier, separate them with commas, and enclose the list in parentheses. You can use the wildcard characters "*" and "%" in identifier names. When you specify a list, the account will be selected if it matches one or more of the elements in the list.

EXAMPLES

```
$ FERRET/REPORT=IDENTIFIER/IDENTIFIER=(APPL1,APPL2,SYSMGR*)
```

Generate an identifier report showing all the users that have been granted the APPL1 or APPL2 identifiers or any identifier starting with SYSMGR.

```
$ FERRET/REPORT/LIST=(USER,ACCOUNT,IDENTIFIER)/FORMAT=ROW/IDENTIFIER=(-,APPL1)
```

Generate a report for all users except those who have been granted the APPL1 rights identifier. NOTE: When using identifier as a /LIST keyword the report must be in row format.

/IGNORE

Use this qualifier to specify a list of items to be ignored during a differences report. You can only specify the IGNORE command when you specify the /REPORT=DIFFERENCES command.

FORMAT

/REPORT=DIFFERENCES/IGNORE=([-,]item-name[,...])

KEYWORDS

"-"

Specifies that all fields are ignored except those matching any specified item name. This operator applies to the entire list, not just to the first element.

item-name[,...]

Specifies the item name to be ignored. A list of valid items is contained in Appendix G. The item name matches the item name specified in the user authorization file.

If you specify /IGNORE without any arguments, the following list of items is ignored:

I_LASTLOGIN
N_LASTLOGIN
P_PASSWORD
S_PASSWORD
P_PWDDATE
S_PWDDATE
LOGFAILS

You can specify up to 57 item names. If you specify an item name more than once, FERRET counts and uses only the first reference. If you specify more than one item name, separate them with commas, and enclose the list in parentheses.

EXAMPLES

```
$ FERRET/REPORT=DIFFERENCES/IGNORE=(I_LASTLOGIN,P_PWDDATE)
```

Generate a differences report ignoring the last interactive login and the primary password change date.

/INCREMENT

Use this qualifier to increase the field specified by /MODIFY by a specified amount. When you specify /MODIFY, you must specify one and only one of the following groups of qualifiers:

{/INCREMENT | /DECREMENT}

{/MAXIMUM | /MINIMUM}

{/SET}

If you specify /INCREMENT, you cannot specify /DECREMENT in the same command.

If you specify /DECREMENT or /INCREMENT, you cannot specify /SET in the same command.

FORMAT

/INCREMENT=n

KEYWORDS

n

Specifies the amount by which the field specified by /MODIFY is to be increased. Specify the increment as an integer. If the field is to small to hold the resulting value, FERRET sets the field to its highest valid value.

This qualifier can only be used with integer fields. It cannot be used with OpenVMS date-time fields.

EXAMPLES

```
$ FERRET/MODIFY=BYTLM/INCREMENT=256/ACCOUNT=RDB*
```

Increase the BYTLM field by 256 in all accounts which start with RDB

```
$ FERRET/MODIFY=ASTLM/INCREMENT=5
```

Increase the ASTLM field by 5 in all accounts

/INTERACTIVE

Use this qualifier to control whether only those records includes the specified access time for interactive jobs are selected. If you omit the qualifier, access time for interactive jobs is not used to select records. INTERACTIVE includes DIALUP, REMOTE and REMOTE. See the section "Specifying access times" in the chapter "Specifying selection criteria" for more details.

FORMAT

/INTERACTIVE=([-,]PRIMARY,[n:m],[n] [,...]
SECONDARY,[n:m],[n],[,...])

KEYWORDS

"-"

Specifies that all records are selected except those matching any specified access time for interactive jobs. This operator applies to the entire list, not just to the first element.

PRIMARY

Specifies the primary access times.

SECONDARY

Specifies the secondary access times.

access-time[,...]

Specifies the access time for interactive jobs used to select records. The access time matches the access time for interactive jobs specified in the user authorization file.

When you specify this qualifier, specify at least one access time. Specify hours as integers from 0 to 23 inclusive. Hours may be specified as single hours (n), or as ranges of hours (n:m). If the ending hour of a range is earlier than the starting hour, the range extends from the starting hour through midnight to the ending hour. The first set of hours after the keyword PRIMARY specifies hours on primary days; the second set of hours after the keyword SECONDARY specifies hours on secondary days. Note that hours are *inclusive*; that is, if you grant access during a given hour, access extends to the end of that hour. If you specify more than one access time, separate them with commas, and enclose the list in parentheses.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,ASTLM)/INTERACTIVE=(PRIMARY,8:17)
```

Generate a report for all accounts whose primary access time for interactive jobs includes all or part of the period 8 a.m. to 5 p.m. for DIALUP, REMOTE or LOCAL access.

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,INTERACTIVE)/INTERACTIVE=(-,SECONDARY,23)/FORMAT=ROW
```

Generate a report in UIC sequence for all accounts except those with a secondary access time for interactive jobs of 11 p.m.

/JTQUOTA

Use this qualifier to control whether only those records matching the specified job-wide logical name table byte quota are selected. If you omit the qualifier, the byte quota is not used to select records.

FORMAT

/JTQUOTA=[-] [n] [n:m] [n:] [:m]

KEYWORDS

"-"

Specifies that all records are selected except those matching the specified job-wide byte quota.

[n] [n:m] [n:] [:m]

Specifies the byte quota used to select records. The byte quota specifies the maximum number of bytes in the job-wide logical name table. Specify the byte quota as an integer. The byte quota matches the byte quota specified in the user authorization file.

Specify n:m to select an inclusive range of byte quotas using the relationship (I>=n AND I<=m). Specify n to select a specific byte quota. Specify n: to select a byte quota and all higher values. Specify :m to select a byte quota and all lower values.

This is not a list; you must specify one and only one of the selections.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,JTQUOTA)/JTQUOTA=1024:
```

Generate a report for all accounts with byte quotas of 1024 or more

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,JTQUOTA)JTQUOTA=-:2048
```

Generate a report in UIC sequence for all accounts except those with byte quotas of 2048 or less.

/LEGEND

Use this qualifier with /FLAGS, /DEFPRIVILEGES and /PRIVILEGES to display a list of abbreviations with their associated meanings. If you omit the qualifier, the legend page is not generated.

FORMAT

/LEGEND

EXAMPLES

```
$ FERRET/REPORT=FLAGS/LEGEND
```

Generate a report for all accounts show flag abbreviations.

/LGICMD

Use this qualifier to control whether only those records matching the specified default login command file are selected. If you omit the qualifier, default login is not used to select records.

FORMAT

/LGICMD=([-,]login-command-file[,...])

KEYWORDS

"-"

Specifies that all records are selected except those matching any specified default login command files. This operator applies to the entire list, not just to the first element.

login-command-file[,...]

Specifies the default login command file used to select records. If you omit device or directory, they default to the device and directory in the account record. The login command file matches the default login command file specified in the user authorization file.

When you specify this qualifier, specify at least one login command file. You can specify up to 64 login command files. If you specify a login command file more than once, FERRET counts and uses only the first reference. If you specify more than one file, separate them with commas, and enclose the list in parentheses. When you specify a list, the account will be selected if it matches one or more of the elements in the list. You can use the wildcard characters "*" and "%" in login command procedure names.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,UIC)/LGICMD=CAD.COM
```

Generate a report for all accounts with the default login command file of CAD.COM.

```
$ FERRET/REPORT/LIST=(USER,UIC,LGICMD)/LGICMD=(-,LOGIN.COM)
```

Generate a report for all accounts except those with the default of LOGIN.COM

/LIST

Use this qualifier to specify a list of items in a user authorization file. You can only specify the LIST command when you specify the /REPORT command. When you specify a date field, both the date and time are printed. However, when you use a date field as selection criteria, only the date can be entered. You cannot include a time-of-day (11:38) as part of the date or delta time when using selection criteria

IF you specify a pre-defined report using /REPORT, you cannot use the LIST or SPECIFICATION qualifiers.

If you use the LIST qualifier, you cannot use the SPECIFICATION qualifier and vice-versa.

FORMAT

/REPORT/LIST=(item-name[,...])

KEYWORDS

item-name[,...]

Specifies the item name to appear on the report. A list of valid items is contained in Appendix E. You cannot list passwords. The item name matches the item name specified in the user authorization file.

When you specify this qualifier, specify at least one item name. You can specify up to 55 item names. You cannot specify P_PASSWORD and S_PASSWORD as items. If you specify an item name more than once, FERRET counts and uses only the first reference. If you specify more than one item name, separate them with commas, and enclose the list in parentheses.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,CPUTIME)/CPUTIME=5
```

Generate a report for all accounts with CPU time limits of 5 seconds.

/LOCAL

Use this qualifier to control whether only those records including the specified access time for local jobs are selected. If you omit the qualifier, access time for local jobs is not used to select records. See the section "Specifying access times" in the chapter "Specifying selection criteria" for more details.

FORMAT

/LOCAL=([-,]PRIMARY,[n:m],[n] [,...]
SECONDARY,[n:m],[n],[,...])

KEYWORDS

"-"

Specifies that all records are selected except those matching any specified access time for local jobs. This operator applies to the entire list, not just to the first element.

PRIMARY

Specifies the primary access times.

SECONDARY

Specifies the secondary access times.

access-time[,...]

Specifies the access time for local jobs used to select records. The access time matches the access time for local jobs specified in the user authorization file.

When you specify this qualifier, specify at least one access time. Specify hours as integers from 0 to 23 inclusive. Hours may be specified as single hours (n), or as ranges of hours (n:m). If the ending hour of a range is earlier than the starting hour, the range extends from the starting hour through midnight to the ending hour. The first set of hours after the keyword PRIMARY specifies hours on primary days; the second set of hours after the keyword SECONDARY specifies hours on secondary days. Note that hours are *inclusive*; that is, if you grant access during a given hour, access extends to the end of that hour. If you specify more than one access time, separate them with commas, and enclose the list in parentheses.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,ASTLM)/LOCAL=(PRIMARY,8:17)
```

Generate a report for all accounts whose primary access time for local jobs includes all or part of the period 8 a.m. to 5 p.m.

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,LOCAL)/LOCAL=(-,SECONDARY,23)/FORMAT=ROW
```

Generate a report in UIC sequence for all accounts except those with a secondary access time for local jobs of 11 p.m.

/LOGFAILS

Use this qualifier to control whether only those records matching the specified number of login failures are selected. If you omit the qualifier, login failure is not used to select records.

FORMAT

/LOGFAILS=[-] [n] [n:m] [n:] [:m]

KEYWORDS

"-"

Specifies that all records are selected except those matching the specified login failure.

[n] [n:m] [n:] [:m]

Specifies the login failures used to select records. The login failures specifies the number of times the user tried to login and failed. Specify the login failures as an integer. The login failures matches the login failures recorded in the user authorization file. Note that the login failure count is set to zero when a successful login occurs.

Specify n:m to select an inclusive range of login failures using the relationship (I>=n AND I<=m). Specify n to select a specific login failures. Specify n: to select login failures and all higher values. Specify :m to select login failures and all lower values.

This is not a list; you must specify one and only one of the selections.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,LOGFAILS)/LOGFAILS=5:
```

Generate a report for all accounts with login failures of 5 or more

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,LOGFAILS)/LOGFAILS=-0
```

Generate a report in UIC sequence for all accounts with non-zero login failures.

/MAXACCTJOBS

Use this qualifier to control whether only those records matching the specified maximum number of batch, interactive and detached processes are selected. If you omit the qualifier, maximum jobs is not used to select records.

FORMAT

/MAXACCTJOBS=[-] [n] [n:m] [n:] [:m]

KEYWORDS

"-"

Specifies that all records are selected except those matching the specified maximum jobs.

[n] [n:m] [n:] [:m]

Specifies the maximum jobs used to select records. The maximum jobs specifies the maximum number of batch, interactive and detached processes which the user can have active at one time. Specify the maximum jobs as an integer. The maximum jobs matches the maximum jobs specified in the user authorization file.

Specify n:m to select an inclusive range of maximum jobs using the relationship (I>=n AND I<=m). Specify n to select a specific maximum jobs. Specify n: to select maximum jobs and all higher values. Specify :m to select maximum jobs and all lower values.

This is not a list; you must specify one and only one of the selections.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,MAXACCTJOBS)/MAXACCTJOBS=5:
```

Generate a report for all accounts with maximum jobs of 5 or more

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,MAXACCTJOBS)/MAXACCTJOBS=-:7
```

Generate a report in UIC sequence for all accounts except those with maximum jobs of 7 or less.

/MAXDETACH

Use this qualifier to control whether only those records matching the specified maximum number of detached processes are selected. If you omit the qualifier, maximum detached jobs is not used to select records.

FORMAT

/MAXDETACH=[-] [n] [n:m] [n:] [:m]

KEYWORDS

"-"

Specifies that all records are selected except those matching the specified maximum jobs.

[n] [n:m] [n:] [:m]

Specifies the maximum jobs used to select records. The maximum jobs specifies the maximum number of detached processes which the user can have active at one time. Specify the maximum jobs as an integer. The maximum jobs matches the maximum jobs specified in the user authorization file.

Specify n:m to select an inclusive range of maximum jobs using the relationship (I>=n AND I<=m). Specify n to select a specific maximum jobs. Specify n: to select maximum jobs and all higher values. Specify :m to select maximum jobs and all lower values.

This is not a list; you must specify one and only one of the selections.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,MAXDETACH)/MAXDETACH=5:
```

Generate a report for all accounts with maximum detached jobs of 5 or more

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,MAXDETACH)/MAXDETACH=-:7
```

Generate a report in UIC sequence for all accounts except those with maximum detached jobs of 7 or less.

/MAXIMUM

Use this qualifier to replace the field specified by /MODIFY by a specified maximum amount. If the field is larger than the value specified by /MAXIMUM, it is replaced by the /MAXIMUM value. Otherwise, it is left unchanged. When you specify /MODIFY, you must specify one and only one of the following groups of qualifiers:

{/INCREMENT | /DECREMENT}

{/MAXIMUM | /MINIMUM}

{/SET}

You can specify /MAXIMUM and /MINIMUM in the same command.

FORMAT

/MAXIMUM=n

KEYWORDS

n

Specifies the maximum value for the field specified by /MODIFY. Specify the maximum as an integer. If the field is less than or equal to the maximum, it is left unchanged. Otherwise, it is replaced by the /MAXIMUM value.

EXAMPLES

```
$ FERRET/MODIFY=WSDEFAULT/MAXIMUM=2500/ACCOUNT=RDB*
```

Limit WSDEFAULT to a maximum of 2500 in all accounts which start with RDB

```
$ FERRET/MODIFY=MAXACCTJOBS/MAXIMUM=16
```

Limit the MAXACCTJOBS field to a maximum of 16 in all accounts

/MAXJOBS

Use this qualifier to control whether only those records matching the specified maximum number of batch, interactive and detached processes are selected. If you omit the qualifier, maximum jobs is not used to select records.

FORMAT

/MAXJOBS=[-] [n] [n:m] [n:] [:m]

KEYWORDS

"-"

Specifies that all records are selected except those matching the specified maximum jobs.

[n] [n:m] [n:] [:m]

Specifies the maximum jobs used to select records. The maximum jobs specifies the maximum number of batch, interactive and detached processes which the user can have active at one time. Specify the maximum jobs as an integer. The maximum jobs matches the maximum jobs specified in the user authorization file.

Specify n:m to select an inclusive range of maximum jobs using the relationship (I>=n AND I<=m). Specify n to select a specific maximum jobs. Specify n: to select maximum jobs and all higher values. Specify :m to select maximum jobs and all lower values.

This is not a list; you must specify one and only one of the selections.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,MAXJOBS)/MAXJOBS=5:
```

Generate a report for all accounts with maximum jobs of 5 or more

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,MAXJOBS)/MAXJOBS=-:7
```

Generate a report in UIC sequence for all accounts except those with maximum jobs of 7 or less.

/MINIMUM

Use this qualifier to replace the field specified by /MODIFY by a specified minimum amount. If the field is smaller than the value specified by /MINIMUM, it is replaced by the /MINIMUM value. Otherwise, it left unchanged. When you specify /MODIFY, you must specify one and only one of the following groups of qualifiers:

{/INCREMENT | /DECREMENT}

{/MAXIMUM | /MINIMUM}

{/SET}

You can specify /MAXIMUM and /MINIMUM in the same command.

FORMAT

/MINIMUM=n

KEYWORDS

n

Specifies the minimum value for the field specified by /MODIFY. Specify the minimum as an integer. If the field is greater than or equal to the minimum, it is left unchanged. Otherwise, it is replaced by the /MINIMUM value.

EXAMPLES

```
$ FERRET/MODIFY=WSDEFAULT/MINIMUM=250/ACCOUNT=RDB*
```

Ensure the WSDEFAULT field is at least 250 in all accounts which start with RDB

```
$ FERRET/MODIFY=ASTLM/MINIMUM=3
```

Ensure the ASTLM field is at least 3 in all accounts

/MODIFY

Use this qualifier to change a specified field in all selected records. You can only specify a single field. When you specify /MODIFY, you must specify one and only one of the following groups of qualifiers:

{/INCREMENT | /DECREMENT}

{/MAXIMUM | /MINIMUM}

{/SET}

You can only specify one of the following qualifiers in a single FERRET command:

/COPY
/MODIFY
/REPORT

FORMAT

/MODIFY=item-name

KEYWORDS

item name
Specifies the user authorization item to be modified. A list of valid items is contained in Appendix G. Note that there are some fields you cannot modify.

EXAMPLES

```
$ FERRET/MODIFY=BYTLM/DECREMENT=256/ACCOUNT=RDB*
```

Reduce the BYTLM field by 256 in all accounts which start with RDB

```
$ FERRET/MODIFY=ASTLM/INCREMENT=5
```

Increase the ASTLM field by 5 in all accounts

/N_LASTLOGIN

Use this qualifier to control whether only those records matching the specified last non-interactive login dates are selected. If you omit the qualifier, non-interactive login date is not used to select records.

The qualifiers I_LASTLOGIN and N_LASTLOGIN are related.

FORMAT

/N_LASTLOGIN=[-] [n] [n:m] [n:] [:m]

KEYWORDS

"-"

Specifies that all records are selected except those matching the specified non-interactive login date.

[n] [n:m] [n:] [:m]

Specifies the last non-interactive login date used to select records. The last non-interactive login specifies the last time a batch login completed successfully for this account. Specify the last non-interactive login as a date or a delta value. You cannot include a time-of-day (11:38) as part of the date or delta time. The last non-interactive login matches the last non-interactive login recorded in the user authorization file.

Specify n:m to select an inclusive range of last non-interactive logins using the relationship (I>=n AND I<=m). Specify n to select a specific last login date. Specify n: to select a particular last non-interactive login and all higher values. Specify :m to select a particular last non-interactive login and all lower values. You cannot specify a range with delta times.

A delta time selects all accounts which have logged in during the last n days. When you specify a delta time, it applies to the past.

This is not a list; you must specify one and only one of the selections.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,N_LASTLOGIN)/N_LASTLOGIN=5
```

Generate a report for all accounts with last non-interactive login within the last 5 days

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,N_LASTLOGIN)/N_LASTLOGIN=-45
```

Generate a report in UIC sequence for all accounts which haven't logged in using BATCH within the last 45 days.

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,N_LASTLOGIN)/N_LASTLOGIN=0
```

Generate a report in UIC sequence for all accounts which haven't ever logged in using BATCH.

/NETWORK

Use this qualifier to control whether only those records including the specified access time for network jobs are selected. If you omit the qualifier, access time for network jobs is not used to select records. See the section "Specifying access times" in the chapter "Specifying selection criteria" for more details.

FORMAT

/NETWORK=([-,]PRIMARY,[n:m],[n] [,...]
SECONDARY,[n:m],[n],[,...])

KEYWORDS

"-"

Specifies that all records are selected except those matching any specified access time for network jobs. This operator applies to the entire list, not just to the first element.

PRIMARY

Specifies the primary access times.

SECONDARY

Specifies the secondary access times.

access-time[,...]

Specifies the access time for network jobs used to select records. The access time matches the access time for network jobs specified in the user authorization file.

When you specify this qualifier, specify at least one access time. Specify hours as integers from 0 to 23 inclusive. Hours may be specified as single hours (n), or as ranges of hours (n:m). If the ending hour of a range is earlier than the starting hour, the range extends from the starting hour through midnight to the ending hour. The first set of hours after the keyword PRIMARY specifies hours on primary days; the second set of hours after the keyword SECONDARY specifies hours on secondary days. Note that hours are *inclusive*; that is, if you grant access during a given hour, access extends to the end of that hour. If you specify more than one access time, separate them with commas, and enclose the list in parentheses.

EXAMPLES

$ FERRET/REPORT/LIST=(USER,ASTLM)/NETWORK=(PRIMARY,8:17)

Generate a report for all accounts whose primary access time for network jobs includes all or part of the period 8 a.m. to 5 p.m.

$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,NETWORK)/NETWORK=(-,SECONDARY,23)/FORMAT=ROW

Generate a report in UIC sequence for all accounts except those with a secondary access time for network jobs of 11 p.m.

/OUTPUT

Use this qualifier to direct FERRET output. If you omit the qualifier, selected records are output to SYS$OUTPUT.

FORMAT

/OUTPUT=[file-spec]

KEYWORDS

file-spec

Specifies the name of the file that is to contain the selected records. If you omit the file name, the file name "FERRET.LIS" is used. If you omit a node, FERRET will default to your current node. If you omit a device, FERRET will default to your current device. If you omit a directory, FERRET will default to your current directory. If you omit a file extension, FERRET will default to ".LIS".

EXAMPLES

```
$ FERRET/REPORT=DIFFERENCES/UAF_FILE=SYSUAF.OLD/OUTPUT=R
```

Compare the default SYSUAF.DAT with SYSUAF.OLD and report differences. The report goes to R.LIS.

```
$ FERRET/REPORT/LIST=(USER,BYTLM)/OUTPUT=SYS$MANAGER:
```

Generate a report and direct the output to SYS$MANAGER:FERRET.LIS

/OWNER

Use this qualifier to control whether only those records matching the specified owner name are selected. If you omit the qualifier, owner name is not used to select records.

FORMAT

/OWNER=([-,]owner-name[,...])

KEYWORDS

"-"

Specifies that all records are selected except those matching any specified owner name. This operator applies to the entire list, not just to the first element.

owner-name[,...]

Specifies the owner name used to select records. The owner name is 1 through 31 alphanumeric characters. The owner name matches the owner name specified in the user authorization file. If the owner name includes blanks, it must be enclosed in quotes.

When you specify this qualifier, specify at least one owner name. You can specify up to 64 owner names. If you specify an owner name more than once, FERRET counts and uses only the first reference. If you specify more than one owner name, separate them with commas, and enclose the list in parentheses. You can use the wildcard characters "*" and "%" in owner names. When you specify a list, the account will be selected if it matches one or more of the elements in the list.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,ASTLM)/OWNER=ENG
```

Generate a report for the ENG owner name.

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI)/OWNER=(-,ACC*)
```

Generate a report in UIC sequence for all accounts except those with owners starting with "ACC".

/P_ENCRYPT

Use this qualifier to control whether only those records matching the specified primary password encryption algorithm are selected. If you omit the qualifier, primary encryption algorithm is not used to select records.

The qualifiers P_ENCRYPT and S_ENCRYPT are related.

FORMAT

/P_ENCRYPT=(-,algorithm[,...])

KEYWORDS

"-"

Specifies that all records are selected except those matching any specified encryption algorithm.

"AD_II" "PURDY" "PURDY_V" "PURDY_S"
Specifies the encryption algorithm used to select records. The encryption algorithm specifies the method used to encrypt the password and username. The encryption algorithm matches the encryption algorithm specified in the user authorization file. FERRET allows you to list but not modify the algorithm; AUTHORIZE does not allow you to do either.

When you specify this qualifier, specify at least one algorithm. You can specify up to four algorithms. If you specify an algorithm more than once, FERRET counts and uses only the first reference. If you specify more than one algorithm, separate them with commas, and enclose the list in parentheses. When you specify a list, the account will be selected if it matches one or more of the elements in the list.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,SALT,P_ENCRYPT)/P_ENCRYPT=PURDY_S
```

Generate a report for all accounts using the PURDY_S encryption algorithm

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,P_ENCRYPT)/P_ENCRYPT=-AD_II
```

Generate a report in UIC sequence for all accounts except those using the AD_II encryption routine

/P_PASSWORD

Use this qualifier to control whether only those records matching the specified primary password are selected. If you omit the qualifier, primary password is not used to select records.

The qualifiers P_PASSWORD and S_PASSWORD are related.

FORMAT

/P_PASSWORD=([-,]text-string[,...])

KEYWORDS

"-"

Specifies that all records are selected except those matching any specified primary password.

text-string

Specifies the primary password used to select records. The primary password is 1 through 31 alphanumeric characters. The primary password matches the primary password specified in the user authorization file. FERRET uses the encryption algorithm (and SALT if necessary) specified in the user authorization file to calculate the hashed value of the text string so it can be compared with the hashed primary password in the user authorization file.

When you specify this qualifier, specify at least one primary password. You can specify up to 64 primary passwords. If you specify a primary password more than once, FERRET counts and uses only the first reference. If you specify more than one primary password, separate them with commas, and enclose the list in parentheses. When you specify a list, the account will be selected if it matches one or more of the elements in the list.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,P_PASSWORD)/P_PASSWORD=SECRET
```

Generate a report for all accounts with a primary password of SECRET

```
$ FERRET/REPORT/LIST=(USER,P_PASSWORD)/P_PASSWORD=-BUTLER
```

Generate a report for all accounts except those whose primary password is BUTLER.

/P_PWDDATE

Use this qualifier to control whether only those records matching the specified primary password change date are selected. If you omit the qualifier, primary password change date is not used to select records.

The qualifiers P_PWDDATE and S_PWDDATE are related.

FORMAT

/P_PWDDATE=[-] [n] [n:m] [n:] [:m]

KEYWORDS

"-"

Specifies that all records are selected except those matching the specified primary password change date. This operator applies to the entire list, not just to the first element.

[n] [n:m] [n:] [:m]

Specifies the primary password change date used to select records. The primary password change date specifies the date the user changed the account primary password. Specify the primary password change date as a date or a delta value. You cannot include a time-of-day (11:38) as part of the date or delta time. The primary password change date matches the primary password change date specified in the user authorization file.

Specify n:m to select an inclusive range of primary password change dates using the relationship (I>=n AND I<=m). Specify n to select a specific primary password change dates. Specify n: to select primary password change dates and all higher values. Specify :m to select primary password change dates and all lower values. You cannot specify a range with delta times.

When you specify a delta time, it applies to the past. This is not a list; you must specify one and only one of the selections.

Primary password date is normally set by OpenVMS when a user changes their password. For security purposes you may not modify this field in the UAF using Ferret except to set the date to pre-expired; forcing the user to set a new password the next time they login.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,P_PWDDATE)/P_PWDDATE=-5
```

Generate a report for all accounts who changed their primary password 5 or more days ago

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,P_PWDDATE)/P_PWDDATE=0
```

Generate a report in UIC sequence for all accounts whose primary password expires today.

```
$ FERRET/MODIFY=P_PWDDATE /SET=PRE-EXPIRED /ACCOUNT=ADMIN
```

Set all ADMIN accounts so that they must change their password the next time they login.

/Password_file

Use this qualifier to specify a file of bad passwords that the audit report should check for. If this qualifier is not specified the audit report uses the file Ferret_dat:ferret_password.dat.

FORMAT

/PASSWORD_FILE=*filename*

KEYWORDS

None

EXAMPLE

$ Ferret /report=audit /password_file=bad_password_dictionary.dat

Generate an audit report checking for bad passwords using the new, more comprehensive list, included with Version 5 of Ferret.

/PBYTLM

Use this qualifier to control whether only those records matching the specified paged buffer IO count limit are selected. If you omit the qualifier, the paged buffer IO count limit is not used to select records.

FORMAT

/PBYTLM=[-] [n] [n:m] [n:] [:m]

KEYWORDS

"-"

Specifies that all records are selected except those matching the specified paged buffer IO count limit.

[n] [n:m] [n:] [:m]

Specifies the paged buffer IO count limit used to select records. Specify the paged buffer IO count limit as an integer. The paged buffer IO count limit matches the paged buffer IO count limit specified in the user authorization file. FERRET allows you to list and modify the paged byte count limit; AUTHORIZE does not.

Specify n:m to select an inclusive range of paged buffer IO count limits using the relationship (I>=n AND I<=m). Specify n to select a specific paged buffer IO count limit. Specify n: to select a paged buffer IO count limit and all higher values. Specify :m to select a paged buffer IO count limit and all lower values.

This is not a list; you must specify one and only one of the selections.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,PBYTLM)/PBYTLM=12:
```

Generate a report for all accounts with paged buffer IO count limit of 12 or more

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,PBYTLM)/PBYTLM=-:20
```

Generate a report in UIC sequence for all accounts except those with paged buffer IO count limit of 20 or less.

/PGFLQUOTA

Use this qualifier to control whether only those records matching the specified page file quota are selected. If you omit the qualifier, page file quota is not used to select records.

FORMAT

/PGFLQUOTA=[-] [n] [n:m] [n:] [:m]

KEYWORDS

"-"

Specifies that all records are selected except those matching the specified page file quota.

[n] [n:m] [n:] [:m]

Specifies the page file quota used to select records. The page file quota specifies the maximum number of pages the user can use in the page file at one time. Specify the page file quota as an integer. The page file quota matches the page file quota specified in the user authorization file.

Specify n:m to select an inclusive range of page file quotas using the relationship (I>=n AND I<=m). Specify n to select a specific page file quota. Specify n: to select a page file quota and all higher values. Specify :m to select a page file quota and all lower values.

This is not a list; you must specify one and only one of the selections.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,PGFLQUOTA)/PGFLQUOTA=5000:
```

Generate a report for all accounts with page file quotas of 5,000 or more

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,PGFLQUOTA)/PGFLQUOTA=-:10000
```

Generate a report in UIC sequence for all accounts except those with page file quotas of 10,000 or less.

/PRCLM

Use this qualifier to control whether only those records matching the specified maximum number of subprocesses are selected. If you omit the qualifier, process limit is not used to select records.

FORMAT

/PRCLM=[-] [n] [n:m] [n:] [:m]

KEYWORDS

"-"

Specifies that all records are selected except those matching the specified maximum number of subprocesses.

[n] [n:m] [n:] [:m]

Specifies the process limit used to select records. The process limit specifies the maximum number of batch, interactive and detached processes which the user can have active at one time. Specify the process limit as an integer. The process limit matches the process limit specified in the user authorization file.

Specify n:m to select an inclusive range of process limit using the relationship (I>=n AND I<=m). Specify n to select a specific process limit. Specify n: to select process limit and all higher values. Specify :m to select process limit and all lower values.

This is not a list; you must specify one and only one of the selections.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,PRCLM)/PRCLM=5:
```

Generate a report for all accounts with process limit of 5 or more

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,PRCLM)/PRCLM=-:7
```

Generate a report in UIC sequence for all accounts except those with process limit of 7 or less.

/PRIMEDAYS

Use this qualifier to control whether only those records matching the specified prime days are selected. If you omit the qualifier, prime days is not used to select records.

FORMAT

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

KEYWORDS

"-"

Specifies that all records are selected except those matching any specified prime days. This operator applies to the entire list, not just to the first element.

prime-day[,...]

Specifies the prime days used to select records. The table below contains a list of valid entries. Specify that a day is not prime by placing "NO" in front of the day name. The prime days matches the prime days specified in the user authorization file.

When you specify this qualifier, specify at least one prime day. You can specify up to 7 prime days. If you specify a prime day more than once, FERRET counts and uses only the first reference. If you specify more than one prime days, separate them with commas, and enclose the list in parentheses. When you specify a list, the account will be selected if it matches one or more of the elements in the list.

MONDAY
TUESDAY
WEDNESDAY
THURSDAY
FRIDAY
SATURDAY
SUNDAY

You can truncate these entries to three characters if you wish.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,ASTLM)/PRIMEDAYS=(MON,TUE,WED)
```

Generate a report for accounts whose prime days are as specified

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI)/PRIMEDAYS=(-,FRI)
```

Generate a report in UIC sequence for all accounts except those with prime days on Friday.

/PRIORITY

Use this qualifier to control whether only those records matching the specified priority are selected. If you omit the qualifier, priority is not used to select records.

FORMAT

/PRIORITY=[-] [n] [n:m] [n:] [:m]

KEYWORDS

"-"

Specifies that all records are selected except those matching the specified priority.

[n] [n:m] [n:] [:m]

Specifies the priority used to select records. The priority specifies which process will receive resources if more than one is ready to run. Specify the priority as an integer in the range 0 through 31. The priority matches the priority specified in the user authorization file.

Specify n:m to select an inclusive range of priorities using the relationship (I>=n AND I<=m). Specify n to select a specific priority. Specify n: to select a priority and all higher values. Specify :m to select a priority and all lower values.

This is not a list; you must specify one and only one of the selections.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,PRIORITY)/PRIORITY=5:
```

Generate a report for all accounts with priorities of 5 or more. These accounts have higher than default priority.

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,PRIORITY)/PRIORITY=:3
```

Generate a report in UIC sequence for all accounts except those with priorities of 3 or less. These accounts have lower than default priority.

/PRIVILEGES

Use this qualifier to control whether only those records matching the specified privileges are selected. Accounts will be matched if they have the specified privileges by default or are authorized to have them. If you omit this qualifier, privileges are not used to select records.

FORMAT

/PRIVILEGES=([-,][NO]privilege[,...])

KEYWORDS

"-"

Specifies that all records are selected except those matching any specified privilege. This operator applies to the entire list, not just to the first element.

privilege[,...]

Specifies the privileges used to select records. A list of valid privileges is contained in Appendix I. Specify the absence of a privilege by placing "NO" in front of the privilege name. These privileges match the privileges specified in the user authorization file. In addition, you can specify the keywords ELEVATED and NOELEVATED. ELEVATED means the account has more than TMPMBX and NETMBX. NOELEVATED means the account has only TMPMBX and NETMBX. ELEVATED can be defined to be a different set of privileges by editing the FERRET_ELEVATED.DAT file.

When you specify this qualifier, specify at least one privilege. You can specify up to 35 privileges. If you specify a privilege more than once, FERRET counts and uses only the first reference. If you specify more than one privilege, separate them with commas, and enclose the list in parentheses. When you specify a list, the account will be selected if it matches one or more of the elements in the list.

EXAMPLES

```
$ FERRET/REPORT/LIST=USER/PRIVILEGES=(CMKRNL,SYSPRV)
```

Generate a report of all accounts which have the CMKRNL or SYSPRV privilege.

```
$ FERRET/REPORT/LIST=(USER,UIC)/PRIVILEGES=(-,TMPMBX)
```

Generate a report for all accounts which don't have the TMPMBX privilege.

/PWDEXPIRED

Use this qualifier to control whether only those records matching the specified password expired status are selected. If you omit the qualifier, password expired status is not used to select records.

FORMAT

/PWDEXPIRED
/NOPWDEXPIRED

KEYWORDS

None

EXAMPLES

```
$ FERRET/REPORT/LIST=USER/PWDEXPIRED
```

Generate a report of accounts whose password will expire on first login.

```
$ FERRET/REPORT/LIST=USER/NOPWDEXPIRED/UIC=[77,*]
```

Generate a report of accounts in UIC [77,*] whose password will not expire on first login.

/PWDLIFETIME

Use this qualifier to control whether only those records matching the specified password lifetime are selected. If you omit the qualifier or specify NOPWDLIFETIME, password lifetime is not used to select records.

FORMAT

/PWDLIFETIME=[-] [n] [n:m] [n:] [:m]
/NOPWDLIFETIME (Default)

KEYWORDS

"-"

Specifies that all records are selected except those matching the specified password lifetime.

[n] [n:m] [n:] [:m]

Specifies the password lifetime used to select records. The password lifetime specifies the maximum duration a user can use the same password. Specify the password lifetime as a number of days. You cannot include a time-of-day (11:38) as part of the delta time. The password lifetime matches the password lifetime specified in the user authorization file.

Specify n:m to select an inclusive range of password lifetimes using the relationship (I>=n AND I<=m). Specify n to select a specific password lifetime. Specify n: to select a password lifetime and all higher values. Specify :m to select a password lifetime and all lower values.

This is not a list; you must specify one and only one of the selections.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,PWDLIFETIME)/PWDLIFETIME=90:
```

Generate a report for all accounts with password lifetimes of 90 or more days

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,PWDLIFETIME)/PWDLIFETIME=-:30
```

Generate a report in UIC sequence for all accounts except those with password lifetimes of 30 or less.

/PWDMINIMUM

Use this qualifier to control whether only those records matching the specified password minimum length are selected. If you omit the qualifier, password minimum is not used to select records.

FORMAT

/PWDMINIMUM=[-] [n] [n:m] [n:] [:m]

KEYWORDS

"-"

Specifies that all records are selected except those matching the specified password minimum length.

[n] [n:m] [n:] [:m]

Specifies the password minimum length used to select records. The password minimum specifies the minimum number of characters the user can use for their password. Specify the password minimum as an integer. The password minimum matches the password minimum specified in the user authorization file.

Specify n:m to select an inclusive range of password minimums using the relationship (I>=n AND I<=m). Specify n to select a specific password minimum. Specify n: to select a password minimum and all higher values. Specify :m to select a password minimum and all lower values.

This is not a list; you must specify one and only one of the selections.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,PWDMINIMUM)/PWDMINIMUM=5:
```

Generate a report for all accounts with password minimums of 5 or more

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,PWDMINIMUM)/PWDMINIMUM=-:7
```

Generate a report in UIC sequence for all accounts except those with password minimums of 7 or less.

/QUEPRI

Use this qualifier to control whether only those records matching the specified queue priority are selected. If you omit the qualifier, queue priority is not used to select records.

NOTE: FERRET supports QUEPRI as a selection criteria and can modify QUEPRI as well, however, this field is not used in recent versions of OpenVMS.

FORMAT

/QUEPRI=[-] [n] [n:m] [n:] [:m]

KEYWORDS

"-"

Specifies that all records are selected except those matching the specified queue priority.

[n] [n:m] [n:] [:m]

Specifies the queue priority used to select records. The queue priority specifies the maximum queue priority the user can use to submit batch jobs. Specify the queue priority as an integer. The queue priority matches the queue priority specified in the user authorization file. FERRET allows you to list and modify the queue priority; AUTHORIZE does not.

Specify n:m to select an inclusive range of queue priorities using the relationship (I>=n AND I<=m). Specify n to select a specific queue priority. Specify n: to select a queue priority and all higher values. Specify :m to select a queue priority and all lower values.

This is not a list; you must specify one and only one of the selections.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,QUEPRI)/QUEPRI=101:
```

Generate a report for all accounts with queue priorities of 101 or more. This will find accounts that submit batch jobs at higher than default queue priority.

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,QUEPRI)/QUEPRI=-:99
```

Generate a report in UIC sequence for all accounts except those with queue priorities of 99 or less. This will find accounts that submit batch jobs at lower than default queue priority.

/REMOTE

Use this qualifier to control whether only those records including the specified access time for remote jobs are selected. If you omit the qualifier, access time for remote jobs is not used to select records. See the section "Specifying access times" in the chapter "Specifying selection criteria" for more details.

FORMAT

/REMOTE=([-,]PRIMARY,[n:m],[n][,...]
SECONDARY,[n:m],[n],[,...])

KEYWORDS

"-"

Specifies that all records are selected except those matching any specified access time for remote jobs. This operator applies to the entire list, not just to the first element.

PRIMARY

Specifies the primary access times.

SECONDARY

Specifies the secondary access times.

access-time[,...]

Specifies the access time for remote jobs used to select records. The access time for remote jobs matches the access time specified in the user authorization file.

When you specify this qualifier, specify at least one access time. Specify hours as integers from 0 to 23 inclusive. Hours may be specified as single hours (n), or as ranges of hours (n:m). If the ending hour of a range is earlier than the starting hour, the range extends from the starting hour through midnight to the ending hour. The first set of hours after the keyword PRIMARY specifies hours on primary days; the second set of hours after the keyword SECONDARY specifies hours on secondary days. Note that hours are *inclusive*; that is, if you grant access during a given hour, access extends to the end of that hour. If you specify more than one access time, separate them with commas, and enclose the list in parentheses.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,PWDMINIMUM)/REMOTE=(PRIMARY,8:17)
```

Generate a report for all accounts whose primary access time for remote jobs includes all or part of the period 8 a.m. to 5 p.m.

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,REMOTE)/REMOTE=(-,SECONDARY,23)/FORMAT=ROW
```

Generate a report in UIC sequence for all accounts except those with a secondary access time for remote jobs of 11 p.m.

/REPORT

Use this qualifier to generate a list of items in a user authorization file. You can only specify one of the following qualifiers in a single FERRET command:

/COPY
/MODIFY
/REPORT

You can specify /SORT, /TITLE, /LIST, /SPECIFICATION qualifiers with the /REPORT qualifier.

If you specify a pre-defined report using /REPORT, you cannot use the /LIST or /SPECIFICATION qualifiers.

If you use the /LIST qualifier, you cannot use the /SPECIFICATION qualifier and vice-versa.

NOTE: The /REPORT command puts an "*" in the first column of any line which contains an account which has been DISUSERED.

FORMAT

/REPORT = [AUDIT] [DIFFERENCES] [FLAGS] [PRIVILEGES] [ACCESS] [IDENTIFIER]

KEYWORDS

"AUDIT" (Default)
Specifies that the user authorization file should be checked and the pre-formatted audit report should be generated.

"DIFFERENCES"
Specifies that the user authorization file should be compared to another file and pre-formatted differences report should be generated.

"FLAG"
Specifies that the pre-formatted flags report should be generated.

“IDENTIFIER”
Specifies that the pre-formatted identifier report should be generated.

“PRIVILEGES” or “BOTHPRIVILEGES”
Specifies that the pre-formatted privileges report should be generated to show all privileges available to the users.

"DEFPRIVILEGES"
Specifies that the pre-formatted privileges report should be generated to show default privileges available to the users.

"AUTHPRIVILEGES"
Specifies that the pre-formatted privileges report should be generated to show authorized privileges available to the users.

"ACCESS"
Specifies that the pre-formatted access report should be generated.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,ASTLM)/ASTLM=5/USER=A*
```

Generate a report for all accounts with an AST limit of 5 seconds and a username starting with "A".

```
$ FERRET/REPORT=DIFFERENCES/CPUTIME=115/SORT=UIC
```

Generate a differences report sorted by UIC for all accounts with CPU time limits of 115 seconds

```
$ FERRET/REPORT=AUDIT/OUTPUT/TITLE=February Audit"
```

Audit the default SYSUAF.DAT. The report has the title "February Audit" and goes to FERRET.LIS.

```
$ FERRET/REPORT/SPEC=RPT SYS$MANAGER:SYSUAF.OLD
```

Generates a report of the fields in the file RPT.SPC. The report goes to SYS$OUTPUT.

/RIGHTS

The /rights qualifier, new to Ferret V4.1, is used in conjunction with the /input and /output qualifiers to generate a text file containing information about rights identifiers held by selected users and facilitate copying these identifiers to another node.

This qualifier must be used with either:

/output	to create an export file of rights identifier information
/input	to read an export file of rights identifier information and add and assign identifiers according to the information it contains

For a detailed description of how to use this qualifier with a complete example refer to the section “Copying Rights Identifiers from one UAF to another” on page 33 of this manual.

/S_ENCRYPT

Use this qualifier to control whether only those records matching the specified secondary password encryption algorithm are selected. If you omit the qualifier, secondary encryption algorithm is not used to select records.

The qualifiers P_ENCRYPT and S_ENCRYPT are related.

FORMAT

/S_ENCRYPT=(-,algorithm[,...])

KEYWORDS

"-"

Specifies that all records are selected except those matching any specified encryption algorithm.

"AD_II" "PURDY" "PURDY_V" "PURDY_S"

Specifies the encryption algorithm used to select records. The encryption algorithm specifies the method used to encrypt the password and username. The encryption algorithm matches the encryption algorithm specified in the user authorization file. FERRET allows you to list but not modify the algorithm; AUTHORIZE does not allow you to do either.

When you specify this qualifier, specify at least one algorithm. You can specify up to four algorithms. If you specify an algorithm more than once, FERRET counts and uses only the first reference. If you specify more than one algorithm, separate them with commas, and enclose the list in parentheses. When you specify a list, the account will be selected if it matches one or more of the elements in the list.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,SALT,S_ENCRYPT)/S_ENCRYPT=PURDY_S
```

Generate a report for all accounts using the PURDY_S encryption algorithm to encrypt their secondary passwords.

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,S_ENCRYPT)/S_ENCRYPT=-AD_II
```

Generate a report in UIC sequence for all accounts except those using the AD_II encryption algorithm to encrypt their secondary passwords.

/S_PASSWORD

Use this qualifier to control whether only those records matching the specified hashed secondary password are selected. If you omit the qualifier, secondary password is not used to select records.

The qualifiers P_PASSWORD and S_PASSWORD are related.

FORMAT

/S_PASSWORD=([-,]text-string[,...])

KEYWORDS

"-"

Specifies that all records are selected except those matching any specified hashed secondary password.

text-string

Specifies the secondary password used to select records. The secondary password is 1 through 31 alphanumeric characters. The secondary password matches the secondary password specified in the user authorization file. FERRET uses the encryption algorithm (and SALT if necessary) specified in the user authorization file to calculate the hashed value of the text string so it can be compared with the hashed secondary password in the user authorization file.

When you specify this qualifier, specify at least one secondary password. You can specify up to 64 secondary passwords. If you specify a secondary password more than once, FERRET counts and uses only the first reference. If you specify more than one secondary password, separate them with commas, and enclose the list in parentheses. When you specify a list, the account will be selected if it matches one or more of the elements in the list.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,S_PASSWORD)/S_PASSWORD=SECRET
```

Generate a report for all accounts with a secondary password of SECRET

```
$ FERRET/REPORT/LIST=(USER,S_PASSWORD)/S_PASSWORD=-BUTLER
```

Generate a report for all accounts except those whose secondary password is BUTLER.

/S_PWDDATE

Use this qualifier to control whether only those records matching the specified secondary password change date are selected. If you omit the qualifier, secondary password change date is not used to select records.

The qualifiers P_PWDDATE and S_PWDDATE are related.

FORMAT

/S_PWDDATE=[-] [n] [n:m] [n:] [:m]

KEYWORDS

"-"

Specifies that all records are selected except those matching the specified secondary password change date.

[n] [n:m] [n:] [:m]

Specifies the secondary password change date used to select records. The secondary password change date specifies the date the user changed the account secondary password. Specify the secondary password change date as a date or a delta value. You cannot include a time-of-day (11:38) as part of the date or delta time. The secondary password change date matches the secondary password change date specified in the user authorization file.

Specify n:m to select an inclusive range of secondary password change dates using the relationship (I>=n AND I<=m). Specify n to select a specific secondary password change dates. Specify n: to select secondary password change dates and all higher values. Specify :m to select secondary password change dates and all lower values.

When you specify a delta time, it applies to the past. This is not a list; you must specify one and only one of the selections.

Secondary password date is normally set by OpenVMS when a user changes their secondary password. For security purposes you may not modify this field in the UAF using Ferret except to set the date to pre-expired; forcing the user to set a new password the next time they login.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,S_PWDDATE)/S_PWDDATE=-5
```

Generate a report for all accounts who changed their secondary password 5 or more days ago

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,S_PWDDATE)/S_PWDDATE=0
```

Generate a report in UIC sequence for all accounts whose secondary password expires today.

```
$ FERRET/MODIFY=S_PWDDATE /SET=PRE-EXPIRED /ACCOUNT=ADMIN
```

Set all ADMIN accounts so that they must change their secondary password the next time

they login.

/SALT

Use this qualifier to control whether only those records matching the specified random password salt are selected. If you omit the qualifier, random password salt is not used to select records. The salt value is a random number generated by OpenVMS during password encryption. Although negative salt values are possible, you cannot search for them using this qualifier.

FORMAT

/SALT=[-] [n] [n:m] [n:] [:m]

KEYWORDS

"-"

Specifies that all records are selected except those matching the specified random password salt.

[n] [n:m] [n:] [:m]

Specifies the random password salt used to select records. The random password salt is a random number generated by OpenVMS. Specify the random password salt as an integer. The random password salt matches the random password salt specified in the user authorization file. FERRET allows you to list but not modify the SALT; AUTHORIZE does not allow you to do either.

Specify n:m to select an inclusive range of random password salts using the relationship (I>=n AND I<=m). Specify n to select a specific random password salt. Specify n: to select a random password salt and all higher values. Specify :m to select a random password salt and all lower values.

This is not a list; you must specify one and only one of the selections.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,SALT,TQELM)/SALT=33215:
```

Generate a report for all accounts with random password salts of 33215 or more

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,SALT)/SALT=-:5092
```

Generate a report in UIC sequence for all accounts except those with random password salts of 5092 or less.

/SET

Use this qualifier to specify the value of the field specified by /MODIFY. When you specify /MODIFY, you must specify one and only one of the following groups of qualifiers:

{/INCREMENT | /DECREMENT}

{/MAXIMUM | /MINIMUM}

{/SET}

FORMAT

/SET=n

KEYWORDS

n

Specifies the value for the field specified by /MODIFY. If it is numeric, the value must be positive. The value you specify must be valid for the OpenVMS AUTHORIZE field you are trying to update. For example, you cannot specify a value of 100 for the priority field which has a maximum value of 31.

EXAMPLES

```
$ FERRET/MODIFY=BYTLM/SET=256/ACCOUNT=RDB*
```

Set the BYTLM field to 256 in all accounts which start with RDB

```
$ FERRET/MODIFY=ASTLM/SET=5
```

Set the ASTLM field to 5 in all accounts

/SHRFILLM

Use this qualifier to control whether only those records matching the specified shared file limit are selected. If you omit the qualifier, shared file limit is not used to select records.

FORMAT

/SHRFILLM=[-] [n] [n:m] [n:] [:m]

KEYWORDS

"-"

Specifies that all records are selected except those matching the specified shared file limit.

[n] [n:m] [n:] [:m]

Specifies the shared file limit used to select records. The SHRFILLM limit specifies the maximum number of shared files the user may have open at one time. Specify the SHRFILLM limit as an integer. The SHRFILLM limit matches the SHRFILLM limit specified in the user authorization file.

Specify n:m to select an inclusive range of SHRFILLM limits using the relationship (I>=n AND I<=m). Specify n to select a specific SHRFILLM limit. Specify n: to select a SHRFILLM limit and all higher values. Specify :m to select a SHRFILLM limit and all lower values.

This is not a list; you must specify one and only one of the selections.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,SHRFILLM,TQELM)/SHRFILLM=5:
```

Generate a report for all accounts with SHRFILLM limits of 5 or more

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,SHRFILLM)/SHRFILLM=-:7
```

Generate a report in UIC sequence for all accounts except those with SHRFILLM limits of 7 or less.

/SORT

Use this qualifier to specify the sequence of reports specified with the /REPORT qualifier. Reports are always generated sorted in ascending order unless the /DESCENDING qualifier is used.

FORMAT

/REPORT /SORT=SEQUENCE_TYPE [/DESCENDING]

KEYWORDS

SEQUENCE_TYPE

The following table gives a complete list of the valid sequence types supported by Ferret V5.0. **USER**, to generate the report is username sequence, is the default type for all list reports if /sort is not specified.

EXAMPLES

$ FERRET /REPORT /LIST=(USER,UIC) /SORT=UIC

Generate a report of all accounts in UIC sequence.

$FERRET /REPORT /LIST=(ACCOUNT, USERNAME, OWNER, PGFLQUOTA) /SORT=ACCOUNT /DESCENDING

Generates a report of all users in the UAF file sorted by account in descending order.

Sequence Types Supported by Ferret V5.0		
Account	Astlm	Biolm
Bytlm	Cli	Clitables
Cputime	Device	Diolm
Directory	Enqlm	Expiration
Fillm	I_Lastlogin	Jtquota
Lgicmd	Logfails	Maxacctjobs
Maxdetach	Maxjobs	N_Lastlogin
Owner	P_Pwddate	Pbytlm
Pgflquota	Prclm	Priority
Pwdlifetime	Pwdminimum	Quepri
S_Pwddate	Salt	Shrfillm
Tqelm	Username	UIC
WSDefault	WSExtent	WSQuota

/SPECIFICATION

Use this qualifier to specify a file containing a list of items in a user authorization file.

You can specify /SORT, /TITLE, /LIST, /SPECIFICATION qualifiers with the /REPORT qualifier.

IF you specify a pre-defined report using /REPORT, you cannot use the /LIST or /SPECIFICATION qualifiers. See Chapter "Generating customized reports" for more information.

If you use the /LIST qualifier, you cannot use the /SPECIFICATION qualifier and vice-versa.

There were some enhancements made to specification files with V5 of Ferret. Refer to the section on specification files earlier in this manual for more details.

FORMAT

/REPORT/SPECIFICATION=file-spec

KEYWORDS

file-spec

Specifies the name of the file from which the item list and title are read. You must specify the file name. If you omit a node, FERRET will default to your current node. If you omit a device, FERRET will default to your current device. If you omit a directory, FERRET will default to your current directory. If you omit a file extension, FERRET will default to ".SPC". If FERRET doesn't find the file using the information and defaults you supply, it will try using the file specification "FERRET_DAT:filename.SPC". If it doesn't find the file there, it will report an error.

EXAMPLES

```
$ FERRET/REPORT/SPECIFICATION=FERRET_DAT:QUOTAS_AND_LIMITS
```

Generate a report for all accounts using the list of fields in the specified file.

/STATISTICS

Use this qualifier to display file statistics such as records read during FERRET operations.

For the pre-formatted access, audit, flags, privilege reports as well as the report generator, /STATISTICS shows the records read and the records selected.

For the differences report, /STATISTICS shows the records read from the main file, the records read from the comparison file and the number of records found to be different.

For the copy function, /STATISTICS shows the records read, the records copied and the records not copied.

For the modify function, /STATISTICS shows the records read, the records modified and the records not modified.

FORMAT

/STATISTICS
/NOSTATISTICS (default)

KEYWORDS

None

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,ASTLM,BYTLM)/STATISTICS
```

Generates a report showing file statistics

/TITLE

Use this qualifier to specify the title to be printed in the centre of the first line of the report.

FORMAT

/TITLE=title

KEYWORDS

title

Specifies the title to be printed on the report. If the title includes spaces or special characters, you must enclose it in quotation marks (""). The title can contain up to 64 characters. If you specify /TITLE without title text, FERRET uses the text "FERRET REPORT".

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,ASTLM,BYTLM)/TITLE="Limits Report"
```

Generates a report with the title "Limits Report"

/TQELM

Use this qualifier to control whether only those records matching the specified timer queue limit are selected. If you omit the qualifier, the timer queue entry limit is not used to select records.

FORMAT

/TQELM=[-] [n] [n:m] [n:] [:m]

KEYWORDS

"-"

Specifies that all records are selected except those matching the specified timer queue entries limit.

[n] [n:m] [n:] [:m]

Specifies the time queue entries limit used to select records. The TQE limit specifies the maximum number of TQE's the user can have queued at one time. Specify the TQE limit as an integer. The TQE limit matches the TQE limit specified in the user authorization file.

Specify n:m to select an inclusive range of TQE limits using the relationship (I>=n AND I<=m). Specify n to select a specific TQE limit. Specify n: to select a TQE limit and all higher values. Specify :m to select a TQE limit and all lower values.

This is not a list; you must specify one and only one of the selections.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,TQELM)/TQELM=5:
```

Generate a report for all accounts with TQE limits of 5 or more

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI,TQELM)/TQELM=-:7
```

Generate a report in UIC sequence for all accounts except those with TQE limits of 7 or less.

/TRUNCATE

Use this qualifier to specify the width of the report specified by /REPORT. Using this length, the report is truncated to the last whole field.

FORMAT

/TRUNCATE=n

KEYWORDS

n

Specifies the maximum width of a column report. The default value is 132. If the report line is longer than the maximum width, it will wrap or be truncated depending on the printer characteristics.

If you specify /FORMAT=ROW, you cannot specify /FORMAT=COLUMN or /TRUNCATE.

If you specify /FORMAT=COLUMN,
you cannot specify /FORMAT=ROW
you may specify /TRUNCATE

EXAMPLES

```
$ FERRET/REPORT/SPEC=RPT/FORMAT=COLUMN/TRUNCATE=80
```

Generate a column report with a maximum width of 80. The report line will be truncated at a field boundary if it is longer than 80 characters.

/TYPE

Use this qualifier to specify the format of the UIC's on reports.

FORMAT

/TYPE=[NUMERIC] [ALPHANUMERIC]

KEYWORDS

NUMERIC

Specifies that UIC's are to be formatted in the form [n,m] where n and m are octal numbers.

ALPHANUMERIC (Default)

Specifies that UIC's are to be formatted in the form [account,username] where account and username are text strings.

If you specify NUMERIC, you cannot specify ALPHANUMERIC and vice-versa.

EXAMPLES

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI)/TYPE=ALPHANUMERIC
```

Format UIC's using the alphanumeric format.

V5 Enhancement

Since most users that want numeric UICs in their reports will consistently want the report in that format a new item name has been added to Ferret V5. To bypass the type qualifier use the appropriate item below in the /list of parameters or in the specification file:

- specify UIC for ALPHANUMERIC
- specify OCTAL_UIC for NUMERIC

both formats can be included in the same report. For users who run a particular report frequently using OCTAL_UIC instead of UIC in the specification field eliminates the need to always add /type=numeric to the command line.

/UAF_FILE

Use this qualifier to specify a second user authorization file. You can only specify the qualifier when you specify the /REPORT=DIFFERENCES or /COPY qualifiers.

FORMAT

/UAF_FILE=file-spec

KEYWORDS

file-spec

Specifies the name of the file that is to be compared or have records copied to it. You must specify the file name. If you omit a node, FERRET will default to your current node. If you omit a device, FERRET will default to your current device. If you omit a directory, FERRET will default to your current directory. If you omit a file extension, FERRET will default to ".DAT".

EXAMPLES

```
$ FERRET/REPORT=DIFFERENCES/UAF_FILE=SYS$MANAGER:SYSUAF.OLD
```

Compare the default SYSUAF.DAT with SYSUAF.OLD and report differences. The report goes to FERRET.LIS.

```
$ FERRET/COPY/UAF_FILE=VAX1::SYS$MANAGER:SYSUAF.OLD/USER=ACC*
```

Copy all the accounts with usernames starting with ACC from the default SYSUAF to the specified file

/UIC

Use this qualifier to control whether only those records matching the specified UIC are selected. If you omit the qualifier, UIC is not used to select records. New to Version 5 of Ferret is the ability to specify a range of UICs.

FORMAT

/UIC=([-,]UIC[,...])

KEYWORDS

"-"

Specifies that all records are selected except those matching any specified UIC.

UIC[,...]

Specifies the UIC used to select records. The UIC value, specified in octal, is a group and member number separated by a comma and enclosed in brackets. The UIC value matches the UIC specified in the user authorization file. Alternatively you may specify a range of UIC groups, members or both by providing a starting value and an ending value separated by a colon ":". In order for the DCL parser to correctly identify a UIC it must be enclosed in double quotes or the comma will be interpreted as a list separator.

When you specify this qualifier, specify at least one UIC. You can specify up to 64 UIC's. If you specify a UIC more than once, FERRET counts and uses only the first reference. If you specify more than one UIC, separate them with commas. You can use the wildcard character "*" to select all the members of a UIC group or all the groups that have a specific UIC member. You cannot use the wildcard character when specifying a UIC range. When you specify a list, the account will be selected if it matches one or more of the elements in the list.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,UIC,ASTLM)/UIC=[77,*]
```

Generate a report for accounts whose UIC group is 77. Display the UIC in alphanumeric format (default).

```
$ FERRET /REPORT /LIST=(USER,OCTAL_UIC,OWNER) /UIC="[100:777,1:2]"
```

Generate a report for the first two members of all UIC groups from 100 to 777. Display the UIC in its octal format.

```
$ FERRET/REPORT/LIST=(USER,UIC,CLI)/UIC=(-,[*,1])
```

Generate a report for all users except those whose UIC member is 1 for their group.

/USER

Use this qualifier to control whether only those records matching the specified user name are selected. If you omit the qualifier, user name is not used to select records.

FORMAT

/USER=([-,]user-name[,...])

KEYWORDS

"-"

Specifies that all records are selected except those matching any specified user name. This operator applies to the entire list, not just to the first element.

user name[,...]

Specifies the user name used to select records. The user name is 1 through 12 alphanumeric characters. The user name matches the user name specified in the user authorization file.

When you specify this qualifier, specify at least one user name. You can specify up to 64 user names. If you specify a user name more than once, FERRET counts and uses only the first reference. If you specify more than one user name, separate them with commas, and enclose the list in parentheses. You can use the wildcard characters "*" and "%" in user names. When you specify a list, the account will be selected if it matches one or more of the elements in the list.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,ASTLM)/USER=ENG*
```

Generate a report for accounts whose user names start with ENG.

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,CLI)/USER=(-,ACC*)
```

Generate a report in UIC sequence for all users except those starting with "ACC".

/VERSION

Use this qualifier to check the version of FERRET you are running. The VERSION qualifier must be submitted as a separate command.

FORMAT

/VERSION

KEYWORDS

None

EXAMPLES

$ FERRET/VERSION

Display the current version of FERRET you are running in the message:

%FERRET-I-VERSION, this is FERRET 3.0

/WIDTH

Use this qualifier to specify the widths of long fields so more fields will fit on one line. If you omit the qualifier, the items are printed at their full width. Since flags and privileges can also be long fields, they are shown in abbreviated form when /WIDTH is specified. Finally, UIC's are shown in their numeric format rather than their alphanumeric format regardless of the setting of the TYPE qualifier.

FORMAT

/WIDTH=(field_name=n,...,field_name=n)
/NOWIDTH=(field_name=n,...,field_name=n)

KEYWORDS

field_name=n
Specifies the maximum width for the UAF fields. If you specify /WIDTH, but omit the list, FERRET applies its own set of defaults for each field. Refer to Appendix H for a complete list of the field name and default field lengths for each field in the UAF.

EXAMPLES

```
$ FERRET/WIDTH
```

Truncate long fields to their FERRET default lengths

```
$ FERRET/WIDTH=(DEVICE=10,DIRECTORY=20)
```

Truncate device to 10 characters and directory to 20 characters

/WSDEFAULT

Use this qualifier to control whether only those records matching the specified WSDEFAULT limit are selected. If you omit the qualifier, working set default is not used to select records.

FORMAT

/WSDEFAULT=[-] [n] [n:m] [n:] [:m]

KEYWORDS

"-"

Specifies that all records are selected except those matching the specified WSDEFAULT limit.

[n] [n:m] [n:] [:m]

Specifies the WSDEFAULT limit used to select records. The WSDEFAULT limit specifies the number of memory pages allocated to user at login. Specify the WSDEFAULT limit as an integer. The WSDEFAULT limit matches the WSDEFAULT limit specified in the user authorization file.

Specify n:m to select an inclusive range of WSDEFAULT limits using the relationship (I>=n AND I<=m). Specify n to select a specific WSDEFAULT limit. Specify n: to select a WSDEFAULT limit and all higher values. Specify :m to select a WSDEFAULT limit and all lower values.

This is not a list; you must specify one and only one of the selections.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,WSDEFAULT)/USER=ENG*
```

Generate a WSDEFAULT report for all users having usernames starting with ENG

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,WSDEFAULT)/WSDEFAULT=-:700
```

Generate a report in UIC sequence for all accounts except those with WSDEFAULT limits of 700 or less.

/WSEXTENT

Use this qualifier to control whether only those records matching the specified WSEXTENT limit are selected. If you omit the qualifier, working set extent is not used to select records.

FORMAT

/WSEXTENT=[-] [n] [n:m] [n:] [:m]

KEYWORDS

"-"

Specifies that all records are selected except those matching the specified WSEXTENT limit.

[n] [n:m] [n:] [:m]

Specifies the WSEXTENT limit used to select records. The WSEXTENT limit specifies the maximum number of memory pages a user can be given if memory is limited. Specify the WSEXTENT limit as an integer. The WSEXTENT limit matches the WSEXTENT limit specified in the user authorization file.

Specify n:m to select an inclusive range of WSEXTENT limits using the relationship (I>=n AND I<=m). Specify n to select a specific WSEXTENT limit. Specify n: to select a WSEXTENT limit and all higher values. Specify :m to select a WSEXTENT limit and all lower values.

This is not a list; you must specify one and only one of the selections.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,WSEXTENT)/WSEXTENT=500:
```

Generate a report for all accounts with WSEXTENT limits of 500 or more

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,WSEXTENT)/WSEXTENT=-:700
```

Generate a report in UIC sequence for all accounts except those with WSEXTENT limits of 700 or less.

/WSQUOTA

Use this qualifier to control whether only those records matching the specified WSQUOTA limit are selected. If you omit the qualifier, working set quota is not used to select records.

FORMAT

/WSQUOTA=[-] [n] [n:m] [n:] [:m]

KEYWORDS

"-"

Specifies that all records are selected except those matching the specified WSQUOTA limit.

[n] [n:m] [n:] [:m]

Specifies the WSQUOTA limit used to select records. The WSQUOTA limit specifies the maximum number of memory pages a user can be given if memory is available. Specify the WSQUOTA limit as an integer. The WSQUOTA limit matches the WSQUOTA limit specified in the user authorization file.

Specify n:m to select an inclusive range of WSQUOTA limits using the relationship (I>=n AND I<=m). Specify n to select a specific WSQUOTA limit. Specify n: to select a WSQUOTA limit and all higher values. Specify :m to select a WSQUOTA limit and all lower values.

This is not a list; you must specify one and only one of the selections.

EXAMPLES

```
$ FERRET/REPORT/LIST=(USER,WSQUOTA)/WSQUOTA=500:
```

Generate a report for all accounts with WSQUOTA limits of 500 or more

```
$ FERRET/REPORT/SORT=UIC/LIST=(UIC,WSQUOTA)/WSQUOTA=-:700
```

Generate a report in UIC sequence for all accounts except those with WSQUOTA limits of 700 or less.

Appendix A, Error messages

FERRET uses OpenVMS-style error messages. The chapter lists every FERRET error message in alphabetical order along with an explanation and recommended actions.

The error messages are divided into the categories:

- Informational - %FERRET-I-
- Warning - %FERRET-W-
- Error - %FERRET-E-
- Success - %FERRET-S-

The rest of the appendix lists error messages and recommended action.

ABKEYW, *keyword* is an ambiguous keyword - supply more characters
The keyword you entered could match more than one keyword. Please check for typing errors, check the qualifier documentation and re-enter the command with more characters on the ambiguous keyword.

DECTRUNC, *value* value could not be fully decremented, set to minimum of *value*
The value you tried to decrement with a $ FERRET/MODIFY=x/DECREMENT=n command could not be fully decremented. It was set to the minimum allowed value.

DIFFRIGHTATTR, The attributes for *identifier* is different on this node. Old: *old* New: *new*
This message indicates that while Ferret was trying to add a new identifier it discovered that the identifier already existed with different attributes. Ferret will not make any change in this case.

DIFFRIGHTVAL, The value for *ident* is different on this node. Old: *old* New: *new*
During trying to add an identifier Ferret discovered an identifier already exists with the same name but a different value. Ferret will not make any change in this case.

DIFFUIC, The UIC for user *user* is different on this node. Old: *old* New: *new*
While Ferret was trying to add the UIC identifier for a particular user it discovered that the user has a different UIC identifier on this node. Ferret will not make any change in this case.

DUPIDENT, Username *username* already has the identifer *identiifer*
The specified user already has the specified identifier. Ferret makes no changes in this case.

DUPKEY, Duplicate key encountered, username: *username*
During a copy operation, FERRET found an account which was already in the file. The existing account is left unchanged.

ERRCLOSEFILE, Error closing file *file_name*

An error occurred while closing the specified file. The error message(s) that follow will explain the problem.

ERRINQUAL, Error in processing the qualifier *qualifier*

FERRET encountered an error while processing a command. The error message(s) that follow will explain the problem.

ERROPENFILE, Error opening file *file_name*

An error occurred while opening the specified file. The error message(s) that follow will explain the problem.

ERRREADFILE, Error reading file *file_name*

An error occurred while reading the specified file. The error message(s) that follow will explain the problem.

ERRREWRITFILE, Error rewriting file *file_name*

An error occurred while updating a record in the specified file. The error message(s) that follow will explain the problem.

ERRWRITFILE, Error writing file *file_name*

An error occurred while adding a record to the specified file. The error message(s) that follow will explain the problem.

GRPNOTADD, Could not add the identifier for the group *group*

FERRET could not add the identifier for the specified group during a COPY or MODIFY operation.

IDENTNOTUIC, *string* is not a UIC identifier

The string you specified is not a valid identifier. Please check for typing errors, check the qualifier documentation and re-enter the command.

IDVALUSED, *Identifier* can not be created since the value is already used

The specified identifier cannot be added because that identifier value has already been used.

INCTRUNC, *value* value could not be fully incremented, set to maximum of *value*

The value you tried to increment with a $ FERRET/MODIFY=x/INCREMENT=n command could not be fully incremented. It was set to the maximum allowed value.

INVDATE, *string* is not a valid date for the qualifier *qualifier*

The date you specified using the specified qualifier is invalid. The syntax may be wrong or you may have specified a time as well as a date. Please check for typing mistakes, check the qualifier documentation and re-enter the command with a valid OpenVMS date.

INVHOUR, *string* is not a valid keyword or hour specification for the qualifier *qualifier*
The hour you specified using the specified qualifier is invalid. Please check for typing mistakes, check the qualifier documentation and re-enter the command with a valid OpenVMS date.

INVKEYWORD, *string* is not a valid keyword for the qualifier *qualifier*
You have tried to enter an invalid keyword for the Ferret qualifier. Please checking for spelling and re-enter the command.

INVLISTENTRY, *string* is not a valid entry, check spelling or truncation
You specified a invalid keyword for a list. Please check for typing mistakes, check the qualifier documentation and re-enter the command with the correct keyword.

INVMOD, The value *string* is not a valid parameter for MODIFY
You cannot change the item you specified. Please check for typing errors, check the qualifier documentation and re-enter the command.

INVPDATEMOD, *string* is an invalid password date, can only use PRE-EXPIRE
You tried to enter something other than pre-expire for a password date. Please check the qualifier documentation and re-enter the command.

INVRANGE, Qualifier *qualifier* has an invalid range
You have entered an invalid range of values for qualifier *qualifier*. The first number must be less than the second number.

INVSPECENTRY, Invalid specification entry: *string*
FERRET could not find the specification file you specified. Please check for typing errors, check the qualifier documentation and re-enter the command.

INVUICFORMAT, *string* is not a valid format for a UIC, check brackets
The UIC you specified using the specified qualifier is invalid. The syntax may be wrong, the group or member may be too large or small. Please check for typing mistakes, check the qualifier documentation and re-enter the command with a valid UIC.

ITEMREQ, You must enter a value for the *qualifier* qualifier
You must specify an item when you specify this qualifier. Check for typing errors, check the qualifier documentation and re-enter the command.

LOGNOTDEFINED, *logical_name* logical not defined
One or more of the FERRET logicals are not defined. Please check system logicals and define the logicals.

MEMNOTADD, Could not add the identifier for the member *member*
FERRET could not add the identifier for the specified member during a COPY or MODIFY operation.

NODEC, *item* could not be decremented

The item you specified cannot be decremented since the current value is less than the decrement. Since a value of 0 often allows infinite resource usage, the account is left unchanged. Please check for typing errors, check the qualifier documentation and re-enter the command.

NOIDENTINFO, No rights identifiers to export

Ferret did not find any identifiers to export for the specified selection criteria. Please check your criteria and try again. Be sure to run the export function on the source node and not the destination node.

NOLIST, Lists are not allowed for the qualifier *qualifier*

You cannot specify a list of values for this qualifier. Please check for typing errors, check the qualifier documentation and re-enter the command with a single value.

NOMINUS, Minus sign not valid with qualifier *qualifier* in this command

You have specified a "-" with a Ferret qualifier that does not allow them. Please remove the "-" sign. Check to see if you can negate individual keywords instead; /QUALIFIER=(NOkeyword).

NORANGE, A range of values is not allowed for *qualifier*

You cannot specify a range of values for this qualifier. Please check for typing errors, check the qualifier documentation and re-enter the command with a single value.

NORECMATCH, No records matched the selection criteria

No records in the specified file matched your selection criteria.

NORMAL, Normal successful completion

This is a normal completion message. No action is necessary.

NOSUCHIDENT, *string* is not an identifier

The string you specified is not an identifier. Please check for typing errors and re-enter the command with a correct identifier.

NOTALLOWCOL, *item* is not allowed in column-based reports

Some items (PRIVILEGES, FLAGS, ACCESS, PRIMEDAYS) require too much space to be used effectively on column-based reports. Specify /FORMAT=ROW when you want to display these fields.

NOUSER, Unable to assign rights for user *username* as it does not exist on this node

The user does not exist so a rights identifier cannot be added for it. When using Ferret to copy UAF accounts be sure to copy the accounts before running the identifier copy utility.

NOWILDUIC, Wildcarded UIC's are not allowed for the qualifier *qualifier*

You cannot specify wildcards for this item. Check the qualifier documentation and re-enter the command without wildcards.

PARSERR, Error parse rights information. Trying to parse: *identifier*

Ferret encountered an error trying to parse the rights information. Please verify that the rights utility input file has been copied successfully and has not been changed.

REPORTRUNC, Report truncated to last complete field

The report you requested required more characters than the maximum. FERRET truncated the report to the last complete field. One or more fields have been omitted from the report.

REQSYSPRV, The privilege SYSPRV is required to use FERRET

FERRET requires SYSPRV. Make sure you have the appropriate privilege and try the command again.

TOOMANYCHAR, The item *I* specified with the qualifier *q* is too long, maximum is *n*

The text string you specified for the item is greater than the maximum length. Check the qualifier documentation and re-enter the command with a length less than or equal to the maximum length.

TOOMANYITEM, Too many items specified for *item*, maximum allowed is *n*

You have specified too many of the specified items. Check the qualifier documentation and re-enter the command with fewer items.

VALUEREQ, A value is required for the qualifier *qualifier*

You must specify a value when you specify this qualifier. Check the qualifier documentation and re-enter the command with a value.

VALUETOOHIGH, The item *I* specified with the qualifier *q* is too high, maximum is *n*

The value you specified for the item is greater than the legal maximum. Check the qualifier documentation and re-enter the command with a value equal to or less than the maximum.

VALUETOOLOW, The item *I* specified with the qualifier *q* is too low, minimum is *n*

The value you specified for the item is less than the legal minimum. Check the qualifier documentation and re-enter the command with a value equal to or greater than the minimum.

VERSION, This is FERRET 4.0 from Saiga Systems

This is the FERRET response to the command FERRET/VERSION with some additional support and license information provided for reference purposes.

Appendix B, Moving HELP text

This appendix shows you how to move FERRET HELP screens between your system help library and private, user help library. You would do this if you had previously installed FERRET help into the system help library and did not want public access to the help screens.

Moving HELP from system to a user library
To move the FERRET HELP screens from the system HELP library to a private, user help library:

1. Delete help text from the system help library:

```
$ LIBRARY/DELETE=FERRET SYS$HELP:HELPLIB.HLB
```

2. Define a user help library logical.

2.1 Enter the command "$ SHOW LOGICAL HLP$*" to find a user library logical name that has not previously been assigned (logical names may be HLP$LIBRARY, HLP$LIBRARY_1, HLP$LIBRARY_2, ... ,HLP$LIBRARY_n)

2.2 Assign the help logical as follows:

```
$ DEFINE/SYSTEM HLP$LIBRARY_n FERRET_DOC:FERRET.HLB
```

If you define the logical in the SYSTEM table, everyone will be able to access the HELP. If you define it in your PROCESS table, only you will be able to access the HELP. If you use the SYSTEM table, you should add a line to the FERRET system startup to define it every time the system is booted. If you use the PROCESS table, you should add a line to your LOGIN.COM.

Moving HELP from a user to the system library
To move the FERRET HELP screens from a private, user help library to the system help library:

1. Find the logical pointing to the user help library for FERRET and deassign it.

```
$ SHOW LOGICAL HLP$LIBRARY*
$ DEASSIGN HLP$LIBRARY_n
```

2. Add the FERRET help library to the system help library.

```
$ LIBRARY/REPLACE/HELP SYS$HELP:HELPLIB.HLB -
_$ dev:[FERRET.DOC]FERRET.HLP
```

3. If the HLP$LIBRARY_n logical was not the last logical in the sequence of user help library logicals, you must assign something else to it. HELP stops translating HLP$LIBRARY_n logicals when it encounter the first one which isn't defined.

Appendix C, Moving command definitions

This appendix shows you how to install the FERRET command definition in your system DCLTABLES, remove it from the DCLTABLES or access it from the FERRET directory. You would remove the FERRET command definition if you had previously installed the FERRET command definition in the system command definition library and did not want public access to the command definition.

To install the command definition in the system table:

1. Check which version of the table is installed

```
$ INSTALL
INSTALL> LIST SYS$LIBRARY:DCLTABLES.EXE
INSTALL> EXIT
```

2. Replace the FERRET command definitions in the table:

```
$ SET COMMAND/TABLE=SYS$LIBRARY:DCLTABLES.EXE -
_$ /OUTPUT=SYS$LIBRARY:DCLTABLES.EXE -
_$ /REPLACE FERRET_CDU:FERRET
```

NOTE: Ensure the new DCLTABLES.EXE are in the same directory as the previous tables.

3. Install the new table:

```
$ INSTALL
INSTALL> REPLACE SYS$LIBRARY:DCLTABLES.EXE
INSTALL> EXIT
```

4. Log out and back in to get a copy of the new table.

To remove the command definition from the system table, type:

```
$ SET COMMAND/DELETE=FERRET/TABLE=SYS$LIBRARY:-
_$ DCLTABLES.EXE/OUTPUT=SYS$LIBRARY:DCLTABLES.EXE
```

To access the command definition from the FERRET directory, type:

```
$ @FERRET_COM:INSTALL_CDU.COM
```

Appendix D, Removing FERRET from your system

This appendix shows you how to remove FERRET from your system if you received a demo, decided to return it and want to remove FERRET from your system.

NOTE: There is a command procedure REMOVE_FERRET.COM which you can adapt to perform many of these steps rather than keying the commands individually.

Delete directories
To remove the FERRET directories from your system, type:

```
$ DELETE SYS$SYSDEVICE:[FERRET...]*.*;*/EXCLUDE=(*.DIR)
```

This removes all non-directory files from the directory structure.

To delete the FERRET directory file from your system, set the protection to allow delete and delete the directory files. Type:

```
$ SET FILE/PROTECTION=S:RWED SYS$SYSDEVICE:[FERRET...]*.DIR
$ DELETE SYS$SYSDEVICE:[FERRET...]*.*;*
$ DELETE SYS$SYSDEVICE:[000000]FERRET.DIR;*
```

Remove HELP screens
If help screens were added into the system help library, remove them by typing:

```
$ LIBRARY/DELETE=FERRET SYS$HELP:HELPLIB.HLB
```

If help screens were added into a private, user help library, follow the procedure outlined in Appendix B to remove them.

Remove command definition
If the FERRET command verb was added to the DCLTABLES, remove it by typing:

```
$ SET COMMAND/DELETE=FERRET/TABLE=SYS$LIBRARY:-
_$ DCLTABLES.EXE/OUTPUT=SYS$LIBRARY:DCLTABLES.EXE
```

Note: Remember to remove the command:

```
@FERRET_COM:INSTALL_CDU.COM
```

from your LOGIN.COM and any other command procedures.

Deassign system logical names
Deassign the system logicals required by FERRET:

```
$ DEASSIGN/SYSTEM FERRET_CDU
$ DEASSIGN/SYSTEM FERRET_COM
$ DEASSIGN/SYSTEM FERRET_DAT
$ DEASSIGN/SYSTEM FERRET_DOC
$ DEASSIGN/SYSTEM FERRET_EXE
$ DEASSIGN/SYSTEM FERRET_PASSWORD
```

Remove SYS$MANAGER files and edit your system startup procedure
Do a directory of SYS$MANAGER:*FERRET*.* and delete all the FERRET specific files.

Remove the @FERRET_STARTUP reference in your system startup procedure.

Appendix E, UAF items

This appendix list the names of the items in the UAF record.

ACCESS
ACCOUNT
ASTLM
BATCH
BIOLM
BYTLM
CLI
CLITABLES
CPUTIME
DATA
DEFPRIVILEGES
DEVICE
DIALUP
DIOLM
DIRECTORY
ENQLM
EXPIRATION
FILLM
FLAGS
GENERATE_PASSWORD #
I_LASTLOGIN
INTERACTIVE
JTQUOTA
LGICMD
LOCAL
LOGFAILS
MAXACCTJOBS
MAXDETACH
MAXJOBS
N_LASTLOGIN
NETWORK
OWNER
P_ENCRYPT *
P_PASSWORD #
P_PWDDATE
PBYTLM
PGFLQUOTA
PRCLM
PRIMEDAYS
PRIORITY
PRIVILEGES
PWDEXPIRED #
PWDLIFETIME
PWDMINIMUM
QUEPRI+
REMOTE
S_ENCRYPT *
S_PASSWORD #
S_PWDDATE
SALT *
SHRFILLM
TQELM
UIC
USER *
WSDEFAULT
WSEXTENT
WSQUOTA

means this field cannot be specified in /LIST
* means this field cannot be specified in /MODIFY
+ included in FERRET for compatibility with the UAF file. This parameter is not used in recent versions of OpenVMS.

Appendix F, UAF item lengths

This table shows the maximum length of items as well as the default length they will be truncated to if /TRUNCATE is specified without any arguments.

Field	Maximum	Default	Field	Maximum	Default
ACCOUNT	8	8	N_LASTLOGIN	23	11
ASTLM	5	5	OCTAL_UIC*	65	23
BIOLM	5	5	OWNER	31	16
BYTLM	10	7	P_ENCRYPT	9	9
CLI	12	3	P_PWDDATE	23	11
CLITABLES	31	9	PBYTLM	10	6
CPUTIME	16	10	PGFLQUOTA	10	9
DATA	255	16	PRCLM	5	5
DEVICE	31	14	PRIORITY	8	8
DIOLM	5	5	PWDLIFETIME	16	11
DIRECTORY	63	14	PWDMINIMUM	6	6
ENQLM	5	5	QUEPRI	6	6
EXPIRATION	23	11	S_ENCRYPT	9	9
FILLM	5	5	S_PWDDATE	23	11
I_LASTLOGIN	23	11	SALT	6	6
JTQUOTA	10	7	SHRFILLM	8	8
LGICMD	63	30	TQELM	5	5
LOGFAILS	8	8	UIC	65	23
MAXACCTJOBS	11	11	USERNAME	12	12
MAXDETACH	9	9	WSDEFAULT	10	9
MAXJOBS	7	7	WSEXTENT	10	8
			WSQUOTA	10	7

* The OCTAL_UIC item is new to Version 5 of Ferret. It is meant to provide a more convenient method for including UICs in the numeric, octal format. Using this item in a /LIST or in a specification file instead of just UIC will include the numeric format of the UIC without having to specify the /type qualifier. It is equivalent to /list=uic /type=numeric. Specifying just UIC is equivalent to /list=uic /type=alpha. When creating reports it is possible to include both OCTAL_UIC and UIC in the same report.

Appendix G, OpenVMS privilege

Below are listed the OpenVMS privileges and the abbreviations for them that are used by FERRET.

Name	Abbreviation	Name	Abbreviation
ACNT	AC	OPER	OP
ALLSPOOL	AS	PFNMAP	PF
ALTPRI	AP	PHY_IO	PI
*AUDIT	AU	PRMCEB	PC
BUGCHK	BC	PRMGBL	PG
BYPASS	BP	PRMMBX	PM
CMEXEC	CE	PSWAPM	PS
CMKRNL	CK	READALL	RA
DETACH	DE	SECURITY	SC
DIAGNOSE	DI	SETPRV	SP
DOWNGRADE	DO	SHARE	SH
EXQUOTA	EQ	SHMEM	SM
GROUP	GR	SYSGBL	SG
GRPNAM	GN	SYSLCK	SL
GRPPRV	GP	SYSNAM	SN
*IMPORT	IM	SYSPRV	SV
LOG_IO	LI	TMPMBX	TM
MOUNT	MT	UPGRADE	UP
NETMBX	NM	VOLPRO	VP
		WORLD	WR

* New with OpenVMS Version 6.1

NOTE: Digital recommends that most accounts have only TMPMBX and NETMBX. The keyword ELEVATED refers to any account which has any privilege listed in FERRET_ELEVATED.DAT. By default this list contains all the privielges except TMPMBX and NETMBX. The privileges UPGRADE and DOWNGRADE are defined within OpenVMS but not yet documented.

Appendix H, Flag abbreviations

This appendix lists all the flags associated with an OpenVMS account along with the corresponding FERRET abbreviations.

Flag	Abbreviation
AUDIT	AUDT
AUTOLOGIN	ALOG
CAPTIVE	CPTV
DEFCLI	DCLI
DISCTLY	CTLY
DISFORCE_PWD_CHANGE	DPWD
DISIMAGE	DIMG
DISMAIL	DMAI
DISNEWMAIL	DNEW
DISPWDDIC	DDIC
DISPWDHIS	DHIS
DISRECONNECT	DREC
DISREPORT	DRPT
DISUSER	DUSR
DISWELCOME	DWEL
GENPWD	GENP
LOCKPWD	LCKP
PWD_EXPIRED	EXP
PWD2_EXPIRED	EXP2
RESTRICTED	RES

Appendix I, Poor passwords

This appendix lists the poor passwords supplied in the default bad password file FERRET_DAT:FERRET_PASSWORD.DAT. To use the larger bad password file added to Ferret V5.0 add the following to your audit command:

/BAD_PASSWORD=FERRET_DAT:BAD_PASSWD_DICTIONARY.DAT.

ABRACADABRA
ACCOUNTNG
ALLIN1
ALLINONE
ALPHAAXP
APASSWORD
CUCKOOEGG
CUCKOOSEGG
CYBERPUNK
DECNET
FIELD
GUEST
HOCUSPOCUS
MANAGER
MYPASSWORD
OPENSESAME
OPENVMS
SERVICE
SHAZAAM
SUPERMAN
SUPERUSER
SYSGEN
SYSMAN
SYSMANAGER
SYSMGR
SYSTARTUP
SYSTEM
SYSTEMMANAGER
SYSUAF
TOPSECRET
VAXCLUSTER
VAXMACRO
VAXTPU
XDELTA

Index

QUALIFIER SUMMARY

This page provides a quick reference guide to FERRET commands and qualifiers that can be used at the DCL command level.

/ACCESS	Specify selection criteria
/ACCOUNT	Specify selection criteria
/ADD_IDENTIFIER	Specify that identifiers are to be copied
/ALL	Include all accounts in the flags report
/ASTLM	Specify selection criteria
/BAD_PASSWORDS	Specify the password dictionary file to be used for the Audit
/BATCH	Specify selection criteria
/BIOLM	Specify selection criteria
/BYTLM	Specify selection criteria
/CLI	Specify selection criteria
/CLITABLES	Specify selection criteria
/CONFIRM	Confirm account copy or modification
/COPY	Copy records from one SYSUAF to another
/CPUTIME	Specify selection criteria
/DATA	Specify selection criteria
/DECREMENT	Decrease the value of a numeric field
/DEFPRIVILEGES	Specify selection criteria
/DEVICE	Specify selection criteria
/DIALUP	Specify selection criteria
/DIOLM	Specify selection criteria
/DIRECTORY	Specify selection criteria
/ENQLM	Specify selection criteria
/EXPIRATION	Specify selection criteria
/FILLM	Specify selection criteria
/FLAGS	Specify selection criteria
/FORMAT	Specify report format
/I_LASTLOGIN	Specify selection criteria
/IGNORE	Specify a list of field changes to ignore
/INCREMENT	Increase the value of a numeric field
/INTERACTIVE	Specify selection criteria
/JTQUOTA	Specify selection criteria
/LEGEND	Print list of abbreviation meanings
/LGICMD	Specify selection criteria
/LIST	Specify a list of report fields
/LOCAL	Specify selection criteria
/LOGFAILS	Specify selection criteria
/MAXACCTJOBS	Specify selection criteria
/MAXDETACH	Specify selection criteria
/MAXIMUM	Specify a maximum for a numeric field

/MAXJOBS	Specify selection criteria
/MINIMUM	Specify a minimum for a numeric field
/MODIFY	Cause the specified field to be modified
/N_LASTLOGIN	Specify selection criteria
/NETWORK	Specify selection criteria
/OUTPUT	Specify the destination of output
/OWNER	Specify selection criteria
/P_ENCRYPT	Specify selection criteria
/P_PASSWORD	Specify selection criteria
/P_PWDDATE	Specify selection criteria
/PBYTLM	Specify selection criteria
/PGFLQUOTA	Specify selection criteria
/PRCLM	Specify selection criteria
/PRIMEDAYS	Specify selection criteria
/PRIORITY	Specify selection criteria
/PRIVILEGES	Specify selection criteria
/PWDEXPIRED	Specify selection criteria
/PWDLIFETIME	Specify selection criteria
/PWDMINIMUM	Specify selection criteria
/QUEPRI	Specify selection criteria
/REMOTE	Specify selection criteria
/REPORT	Specify a report to be generated
/S_ENCRYPT	Specify selection criteria
/S_PASSWORD	Specify selection criteria
/S_PWDDATE	Specify selection criteria
/SALT	Specify selection criteria
/SET	Specify a new value for a field
/SHRFILLM	Specify selection criteria
/SORT	Specify the sequence of a report
/SPECIFICATION	Specify a file containing report fields
/STATISTICS	Specify file statistics during operations
/TITLE	Specify the title for a report
/TQELM	Specify selection criteria
/TRUNCATE	Specify whether fields are to be truncated
/TYPE	Specify UIC format
/UAF_FILE	Specify a SYSUAF.DAT (/MODIFY, /COPY)
/UIC	Specify selection criteria
/USER	Specify selection criteria
/VERSION	Display FERRET version
/WIDTH	Specify report width
/WSDEFAULT	Specify selection criteria
/WSEXTENT	Specify selection criteria
/WSQUOTA	Specify selection criteria