SENTRY

The Integrated Security System

Release 4

User Guide

Fitzgerald & Long

12341 E. Cornell Avenue, #18
Aurora, Colorado 80014-3323 USA
Phone: (303) 755-1102
FAX: (303) 755-1703

NOTICE

The information contained in this guide is subject to change without notice.

Fitzgerald & Long, Inc. shall not be liable for technical or editorial omissions made herein; nor for incidental or consequential damages resulting from the furnishing, performance, or use of this material.

Table Of Contents

USING THIS GUIDE

The SENTRY User's Guide is comprehensive in its descriptions of all of SENTRY's menus, data entry screens and reports. The Guide follows the same structure as the SENTRY menu system.

There are four major sections in SENTRY. These are:

1. Database Creation and Validation
2. Database Maintenance
3. Reports
4. Utilities

Additionally, there is an introductory section and a number of appendices. The introduction includes an overview of the User's Guide, a description of conventions used throughout the SENTRY screens, installation instructions and suggestions on getting started.

Note that each menu selection has a number to its left indicating the selection number from the Main Menu. For example, the **Database Maintenance Menu** is preceded by the number "**2**", indicating that it is the second selection from the Main Menu. The **User Maintenance** program documentation has the section number 2.2 in it's title. This references the second program, **User Maintenance**, in the second section, **Database Maintenance**.

The Guide uses several notation conventions for the sake of easy reading and conciseness. These include:

<RETURN> This figure indicates that the return key, sometimes called NEW LINE or ENTER, should be pressed. This is one key stroke.

<ESC> This figure is used to indicate the escape key. Most keyboards have a key labeled "ESC". The use of the escape key is ALWAYS followed by <RETURN>. SENTRY uses this key to allow an abort or escape from any program. All data remains as it were prior to the aborted session. Please note that this function may be assigned to another key if desired. See Appendix 2 for details on creating new key bindings.

" " (quotes) The SENTRY User's Guide frequently uses double quotation marks to set off the characters you should enter. NEVER type the quotes!

TCL **T**erminal **C**ontrol **L**anguage. SENTRY will function equally well on any of the UNIX-based database environments, including uniVerse, UniData and PI/open. Since each environment uses its own naming conventions we have used the generic term "**TCL**" to indicate the command prompt for whichever environment you are using. For UniData and

PI/open the command prompt is indicated by a colon "**:**" while for uniVerse the prompt is a greater-than sign "**>**".

USING THE SCREENS

SENTRY data entry screens feature some very helpful functions. These include "repaint", "backup", "escape" (exit without update), "execute" and "help". The following paragraphs describe each function.

Repaint ^^ <RETURN> Enter a caret twice, followed by <RETURN>. The caret key is generally located on the same key as the "6" (SHIFT 6). This is a total of three key strokes. The screen will be repainted and the cursor will be repositioned to its original position. This is very convenient when a system message causes a data entry screen to scroll.

Backup ^ <RETURN> Press the caret key followed by return (2 key strokes). This will cause the cursor to backup one prompt in the data entry screen.

Escape <ESC> <RETURN> Press the escape key followed by the return key (2 key strokes). This feature allows you to exit any data entry program at any prompt. No data will be changed.

Use this key to exit data entry screens when you have made changes and wish to cancel your changes. To save changes you must enter "**F**" to file those changes.

XEQ You may use TCL (Terminal Control Language) commands at any input prompt. Enter "**XEQ**" followed by your command. For example:

```
XEQ LIST SENTRY.USERS WITH <
DEPARTMENT = "MIS" USER.NAME
```

HELP Enter the word HELP at any input prompt in SENTRY. A HELP screen will be displayed containing a brief explanation of the expected input and syntax where appropriate. Press <RETURN> to exit the HELP screen.

Please note that these functions may be assigned to alternate keys if desired. See Appendix 2 for details regarding creation of new key bindings

Data Entry Conventions

Underscore/underline

When awaiting data, the cursor is positioned at the beginning of the field. The field is delineated by underscores. A sentence describing the field is displayed at the bottom of the screen. No data appearing on the underscore is an indication that the field in the database is currently null.

Field numbers

Each data entry screen and menu uses sequential numbers which appear at the left of the field descriptions. To address a particular field, enter the number associated with that field.

Change a field

Having addressed the desired field via the field number, an underscore will appear to the right of the current data and the cursor will be positioned on the leftmost character of the data field. Type over the existing data to change it. DO NOT space over existing data to delete characters which your new entry does not cover. Simply <RETURN> when you have entered the new data. The field will be repainted to display your entry.

Deleting a field

When you wish to delete the data in a field and make the field null, address the field using the appropriate line number, then enter a space followed by <RETURN>. A blank (null) field will be displayed.

INSTALLING SENTRY

Installing the SENTRY software is very simple! Just follow these easy steps. If you encounter problems at any point, please call us for additional assistance.

Before you begin, check your system to see if there is a possible conflict with the accounts we will be loading. Do you have an account or user name called "sentry" or "sentry.practice"? If you have an account or user ID which uses either of these names, DO NOT INSTALL SENTRY. Please call us for alternate installation instructions. If you are in doubt as to the naming conventions on your computer, DO NOT INSTALL SENTRY. Be safe, call us for assistance and instruction on installation. We want to help.

SENTRY will require approximately 5 to 10 MB of disk space in one filesystem on your computer. This is an estimate. The actual size will vary depending on the number of files on your system and the cross referencing for those files. Please discuss your disk space concerns with us. Check to see that this space is available before beginning installation. You will NOT need to stop or start the system during installation and your users may continue to use the computer while you are installing SENTRY.

1. Login to your system as the super-user (usually the user "root"). Change directories ("cd") to the directory where you wish to place the SENTRY account. We suggest placing SENTRY in a top-level directory (for example, the "/u1" or "/usr" directory). SENTRY may be placed on any local file system.

2. List the contents of the directory using "**ls**" or "**ls -C**". Make sure that this is the directory where you wish to place SENTRY. Use "**pwd**" to verify your directory.

3. If SENTRY has been previously installed on your system, there may be an existing directory named "sentry". Change the name of this existing directory to "sentry.old" by entering the command:

mv sentry sentry.old

Enter "**ls -C**" to verify that the name is changed.

4. Restore the contents of the tape using cpio. You will need to know the device file used to interface with your tape drive. Ours, for example, is "/dev/rmt/0m". Enter this command:

cpio -icvBdum < /dev/xxx *(replace xxx with your device file name)*

The tape contains two accounts: sentry and sentry.practice. You must restore sentry; sentry.practice is optional. It contains several demonstration items and files.

5. When the restore is complete, cd to the sentry directory and list the contents ("ls" or "ls -C").

6. Notice a file named "install". This is a script which will perform the steps necessary to install the SENTRY software. Execute the script by entering:

./install

7. Next type the command to enter your database environment (uv, udt, piopen). You should now see the TCL prompt ">" or ":".

If you see the UNIX message "…:not found" when you enter the command, it means that your PATH variable is not setup to contain the path to the command directory of your database. Each database environment has a directory named "**bin**" which contains its executable programs. The UNIX PATH variable must contain the path to this directory in order for you to use the environment's commands. Depending upon the database system you have and where it is installed the path will look like one of these:

uniVerse	**/…/uv/bin**	"**…**" implies that the actual path varies
UniData	**/…/udt/bin**	according to where your database
PI/open	**/…/isys/bin**	account was installed.

The PATH variable may be set permanently by modifying the ".profile" file in your home directory to include the appropriate path in the PATH assignment. The problem may be resolved temporarily (until you logout) by entering these Bourne shell commands at the UNIX prompt:

```
PATH=$PATH:/…/…/bin
export PATH
```

Note that "**/…/…/bin**" must be replaced with the actual appropriate pathname!

8. Set the proper terminal type for the terminal you are using with the **SET.TERM.TYPE** command, (e.g. SET.TERM.TYPE tvi925).

9. Now enter the command "**SENTRY**". You will see a copyright screen which identifies your company and computer system. If there are discrepancies in the data on this screen, please contact us. SENTRY is licensed only for use at the company and on the system described on the copyright screen.

10. Enter a carriage return. You will now see the SENTRY Menu on your screen (Figure 1).

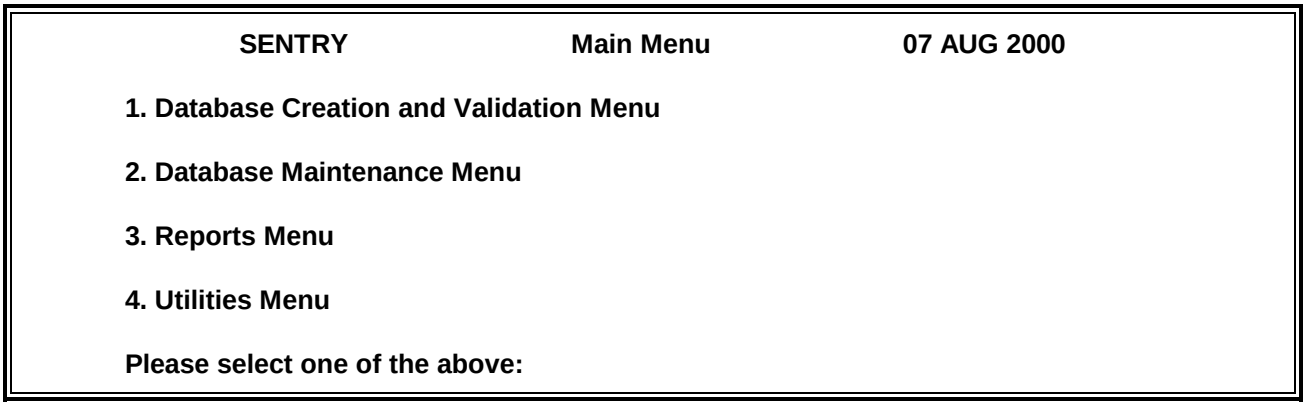

Figure 1 - *Main Menu*

11. At this point you are ready to begin loading your data into the SENTRY database. This procedure is described in the following section "Getting Started".

GETTING STARTED

This section describes how to invoke the SENTRY Main Menu. It also describes the copyright and the validation screen which will be displayed as you enter SENTRY. Additionally, the first three steps for loading the SENTRY database are presented.

< < S E N T R Y - Serial Number 00.08.70100 > >

This version of SENTRY has been prepared expressly for

Fitzgerald & Long, Inc.
12341 East Cornell Avenue
Aurora, Colorado

and may be used there only on the following computer system:

Hewlett-Packard 9000-E25, PI/Open Serial # 999999

Any other use is in violation of the license and is forbidden.

< < < < Release 4.1 - Copyright 1988 - 2000 > > > >

Fitzgerald & Long, Inc.
12341 East Cornell, # 18
Aurora, Colorado 80014 USA

Telephone: (303) 755-1102

Figure 2 - *This is an example of the SENTRY copyright screen.*

Having restored SENTRY from tape and installed the software, you are ready to proceed with this section. SENTRY is installed as a directory named **sentry**; this directory is also setup as a standard database account. To access SENTRY you must be "in" the **sentry** account – that is, **sentry** must be your present working directory. To reach **sentry** from the UNIX prompt, use the UNIX "**cd**" command followed by the command to invoke your database environment (e.g. **"uv", "udt"** or **"piopen"**). To reach **sentry** from TCL in another account use the TCL "**LOGTO**" command.

Since SENTRY is a security product, it won't allow just any user to use it to modify your system! Only users whose UNIX UID is 0 (zero) will be permitted to enter SENTRY. Users with the UID of 0 are referred to as "super users" because they have the power to do nearly anything on the system. The standard user **"root"** is an example of a "super user". The passwords to super user logins should be carefully protected!

Our recommendation is that you create a userid called **sentry** with the UID of 0 (zero). This user will have "sentry" as its "home" directory and will invoke the database on login. Suggestion: use SENTRY to create this user while "getting started" with SENTRY.

At TCL, enter:

SENTRY

The SENTRY copyright screen (Figure 2) will be displayed. This screen reminds you that SENTRY is protected by copyright law and is licensed for use to the company and computer system named on the screen. Under no circumstances may you use the SENTRY software for any other company and/or computer system than the one for which this copy of SENTRY was prepared, without the written permission of Fitzgerald & Long, Inc.

The copyright screen awaits a <RETURN>.

Validating System Administrator authority.....

You must be super-user to use SENTRY!

Press <RETURN> to continue :

Figure 3 - *This screen is displayed immediately after the copyright screen in the previous figure. You will see the second line "You must be super user to use SENTRY" only if your user ID has a UID other than 0 (zero).*

NOTE: If another user is logged in as the System Administrator and attempts to use SENTRY, the following message will be displayed.

SENTRY is currently being run by user n.

This is a safety precaution. SENTRY is a very powerful tool and should only be used by the System Administrator or his designee. SENTRY is designed to be a single user utility. Therefore, only one user at a time is allowed into SENTRY.

The third SENTRY screen (Figure 3) informs you that SENTRY is validating that your user ID has a UID of 0 (zero). If it does NOT, you will see the message:

"You must be a super-user to use SENTRY!"

The validation screen may flash by so quickly that you cannot read it because the test for UID = 0 is so quick. Unless the validation fails, SENTRY will display the Main Menu.

The SENTRY Main Menu

There are four selections on the SENTRY Main Menu. These are:

1. Database Creation and Validation Menu
2. Database Maintenance Menu
3. Reports Menu
4. Utilities Menu

Choose selection one, **Database Creation and Validation Menu**. This selection presents another menu which has three more choices. Each selection in each menu is documented thoroughly in the User Guide. Simply look for the User Guide section that corresponds to the number of the menu selection. For example, to get to the second selection of the Database Creation and Validation Menu you first entered "**1**" from the Main Menu and then entered "**2**" from the next menu. In the User Guide you will find documentation about this selection in section 1.2.

Read the appropriate section of the User Guide for each of the three selections in the Database Creation and Validation Menu and then execute each one in turn. They perform the following tasks to setup your SENTRY database:

1. **Upload User and Group Profiles from UNIX** - this program will read your UNIX passwd and group files and create database records in SENTRY for all the users and groups which have been setup on your system. The process will take just a few seconds.

2. **Create Database from File System** - this program scans the locals disks on your system and builds cross reference information in SENTRY about the directories and files it finds. The cross reference uses a sophisticated database structure known as a "balanced B-tree" - this will allow SENTRY to locate objects on your disk nearly instantaneously! Because this is a complex task it will take longer, perhaps as long as an hour or more. The appropriate section of the User Guide describes a technique for running this program as a "phantom" or "background" task to avoid tying up your terminal.

3. **Validate the User Profile Database** - this program validates the logical integrity of the data you have uploaded into SENTRY. It will print a report of any problems and inconsistencies it finds. If you

wish to send the report to a specific printer, form or destination use the SETPTR command to set your printer parameters before executing this selection.
After performing these steps your SENTRY database reflects the actual state of your system. You may now use the Database Maintenance Menu to fix the inconsistencies reported by the validation program or to modify users, groups and file permissions. You may also begin to protect database commands. The Reports Menu will print a variety of useful reports which will allow you to view the data you have collected. The Utilities Menu contains a number of tools which will occasionally be useful.

Complete documentation for each menu and selection in SENTRY is contained in the next sections of this User Guide.

INTRODUCING THE MAIN MENU

SENTRY'S Main Menu follows the copyright screen and the System Administrator validation screen. It is the entry point into the four submenus. The four submenus are presented as selections 1 through 4 (Figure 4).

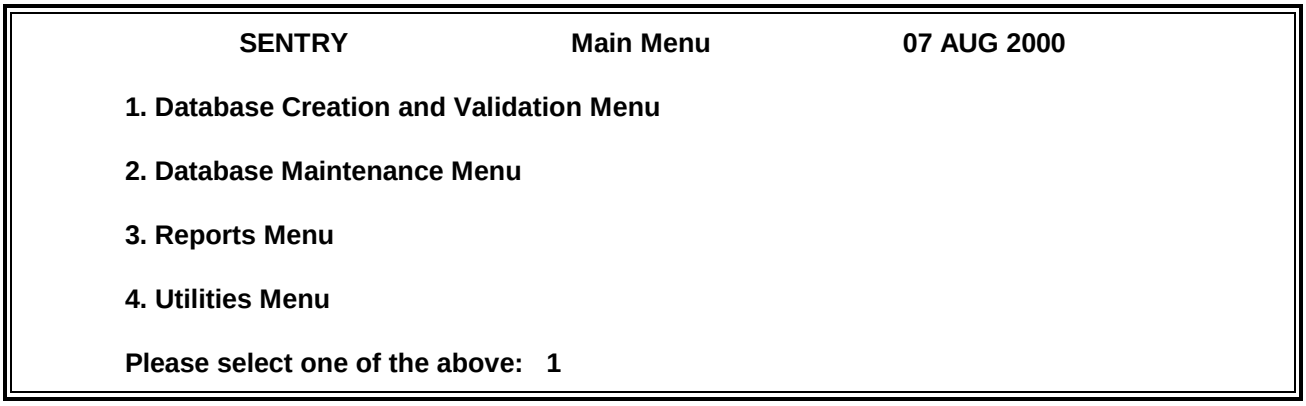

Figure 4 - *This is an example of SENTRY's Main Menu which provides access to the four submenus and divides SENTRY into four logical sections.*

These four selections outline the four logical divisions of SENTRY. Each division is a collection of programs which perform related tasks.

The documentation mirrors this organization: There are four major sections. Each section is introduced via a figure of the Main Menu and a short description of the processes which may be performed from that particular menu selection. Note that the section topic appears in bold print to amplify the Main Menu selection used to invoke the submenu for that topic.

Each submenu is introduced in the same manner. Each selection on each submenu is documented through a sample screen. A description of each field and its use is presented.

In using the menus please note that "on-line" help is available. At the menu selection prompt, enter

HELP <RETURN>

Then enter the number of the menu item for which you would like to receive help.

The first selection, **Database Creation and Validation Menu** offers access to programs which upload the information in the UNIX passwd and group files into SENTRY's database. Another program transverses the disks, reading the permissions, owner and group for each file and directory and loading cross reference information into SENTRY's database. Once the data are loaded, you should test the consistency of the data by executing the validation program.

The second selection, **Database Maintenance Menu**, is the menu for all data entry programs. You may create, delete, and modify users, groups and file permissions. You may also protect commands, peruse files and directories and modify SENTRY system parameters.

This second submenu displays six selections. These are programs to maintain the system profile, user profiles, groups, the file system, SENTRY's Command Protection and SENTRY's User Defined Item Protection.

The third selection on SENTRY's Main Menu invokes the **Reports Menu**. This submenu provides access to reports. These reports describe all aspects of the SENTRY database from the perspectives of system, users, groups, permissions, access violations and SENTRY protected database commands.

The fourth selection on SENTRY's Main Menu is the **Utilities Menu**. This submenu provides a collection of programs to perform such tasks as duplicating Command Protection in one account like that in another account, purging the Violations Log, and rebuilding the cross reference files. You may also use a tool which will generate new passwords for all or selected users. Yet another utility will update the VOC of a protected account with the command protection setup through SENTRY, insuring consistency.

The following sections will describe each menu in detail. Each selection of each submenu is described with examples of the screens and prompts available through these programs.

1. INTRODUCING THE DATABASE CREATION AND VALIDATION MENU

The first selection of SENTRY's Main Menu is Database Creation and Validation. This menu provides access to programs which will build SENTRY's database from your existing user, group and file system data.

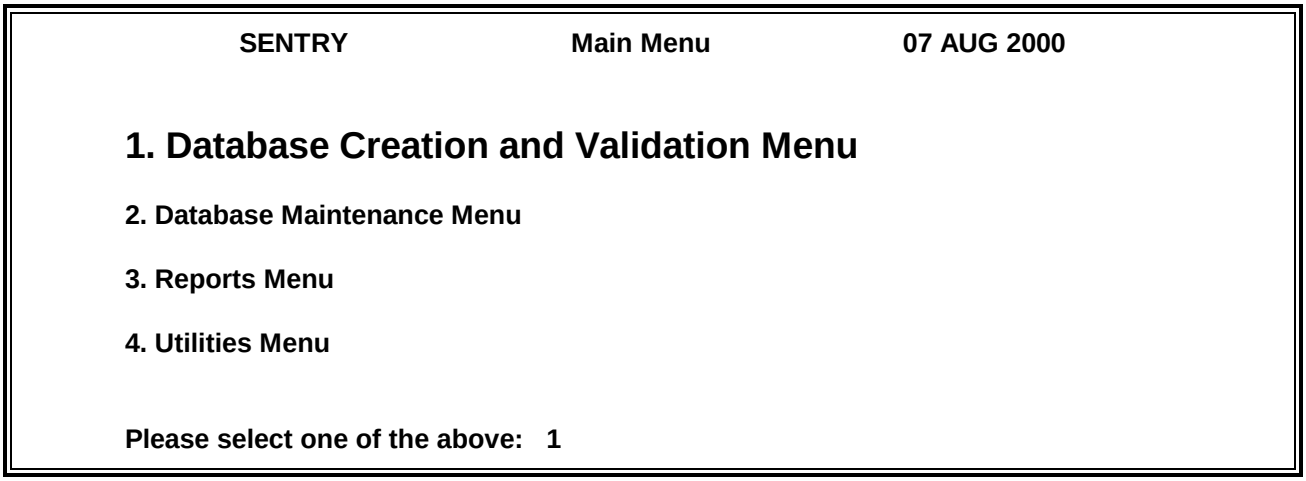

Figure 5 - *Database Creation and Validation is the first selection on the Main Menu.*

These programs provide a quick and easy way to document your existing system. Because all of the data are loaded into SENTRY's database, comprehensive reports are available. Additionally, These programs simplify most of the data entry tasks usually associated with setting up a new security system.

Complimentary to the programs which build the SENTRY database is a program to evaluate the consistency of usage in groups, users, and permissions.

The three selections in the **Database Creation and Validation Menu** are the first three steps you should take after installing SENTRY. The following sections provide detailed descriptions on how, when and why these programs are used.

1.0 DATABASE CREATION AND VALUDATION MENU

This is the first submenu accessible from SENTRY's Main Menu. It is also the first selection you will make after installing SENTRY. Through this menu, you will execute programs which load all the UNIX passwd and group information on your system into SENTRY's database.

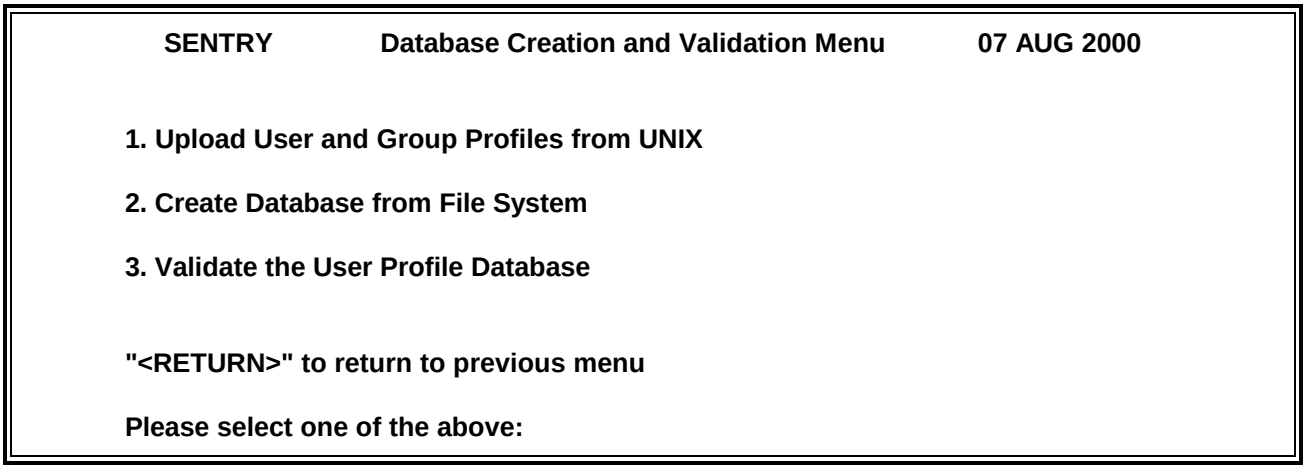

Figure 6 - *The Database Creation and Validation Menu provides access to three programs through which you may create and validate the SENTRY database.*

Three processes are available in this menu. These provide the capability of uploading the passwd and group files into the SENTRY database, uploading file system information and validating the SENTRY database.

The first selection, **1. Upload User and Group profiles from UNIX** reads your existing UNIX passwd and group files and writes the information into SENTRY's database. This is the first program you will execute after SENTRY is installed.

The second selection, **2. Create Database from the File System** transverses your local file systems reading all information and creating B-trees to index this information. Note that no remote (NFS) disks are read.

After SENTRY's database has been loaded with the passwd, group and file system data, selection **3. Validate the User Profile Database** is used to test the consistency of the data in SENTRY's database. Tests include checks to insure that permissions do not reference users who do not exist in the passwd file or groups which have no registered users. Following extensive validation, a report is produced which documents the inconsistencies found.

The following sections present a detailed description of each program, the screens and the prompts.

1.1 UPLOAD USER AND GROUP PROFILES FROM UNIX

This program loads the data from the UNIX passwd and group files into the SENTRY database. Existing data in the SENTRY database is checked and compared to that in these two files. The SENTRY database is updated to reflect the same configuration as these files.

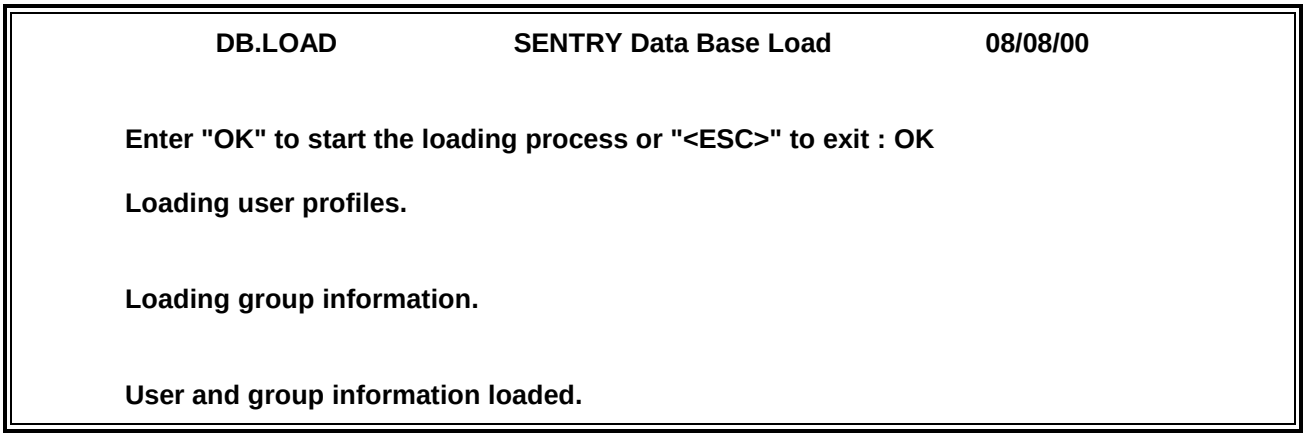

Figure 7 - *This is an example of the "SENTRY Database Load" screen. Enter "OK" to execute the program.*

This is the first program you will execute after SENTRY is installed. After the initial upload you will use this program on a regular basis to insure that SENTRY is consistent with your UNIX files.

To invoke this program, enter **1. Database Creation and Validation Menu** on SENTRY's Main Menu. Then, enter **1. Upload User and Group Profiles from UNIX** from the submenu. This program will be invoked.

On first entering this program, only the prompt **Enter 'OK' to start the loading process:** is displayed. Enter "**OK**" to begin or <ESC> to exit the program.

The loading process is performed in two steps. First, the information in the passwd file is read. Second, the group file information is loaded into the SENTRY database. The screen will report the progress of the program as it begins each step. Figure 7 is an example of this screen after the two steps have been completed.

After loading your system information into SENTRY, you should use the SENTRY maintenance screens to update, add or delete users and groups. You may still continue to use the UNIX utilities to manage users and groups, but changes made will not be reflected in the SENTRY database until you perform the upload again.

We recommend: Upload the passwd and group files into the SENTRY databases on a regular basis to INSURE that SENTRY reflects an accurate view of your system. Because of the numerous file system changes which occur daily in the normal course of operations, we recommend that you execute the program which creates the file system view on a regular basis as well. These programs should be scheduled as "over night" jobs at least once a week on systems with "normal" activity.

Because every site is unique, please discuss your system requirements with us if you are undecided about the frequency with which you should be uploading (recreating) the SENTRY database.

The program that loads the UNIX passwd and group data into SENTRY can be run outside SENTRY's menu system, in "batch" mode. The program can be run at TCL, either directly or using the "PHANTOM" command. This allows you to schedule the process via cron, BENTON or some other utility. The command line to invoke the program is:

SENTRY.DB.LOAD (BATCH)

There is no difference in the actions performed whether the program is run from the menu for in "batch" mode.

1.2 CREATE DATABASE FROM FILE SYSTEM

This section describes the program which create the B-trees to index your file system directories, files, file owners and groups. On a system with a very large number of files, this process may take a number of hours. This is a "read only" process. If does NOT interfere with your normal processing.

```
FILE.LOAD          Load SENTRY Filesystem Data Base          10/19/00

Enter "OK" to begin processing or "<ESC>" to exit : OK

Starting phantom to build sentry.output file...

Phantom task being performed by User 4097.
Output file is "SENT978972046C".

Reading sentry.output file and building BTREE records...

Path - /usr/bin/mediainit

Count - 185
```

Figure 8 - *This is an example of the messages displayed by the program which creates the B-tree indices of your file system.*

We are very proud of SENTRY's balanced B-tree system of indices. Through the use of B-trees, which are ordered cross reference files, we are able to index your entire file system offering you a "file manager" style window to view your file structure, permissions, file owners and groups in a very efficient manner conserving not only CPU cycles but disk storage space as well.

On entering "**OK**" to start execution of this program, the old B-trees (if any) are cleared. Two processes are started. One process reads the UNIX I-node tables and writes the information into a text file. A second process reads in the text file and creates the B-tree entries.

Because this can be a very time consuming process and should be repeated on a regular basis, SENTRY offers a "batch" processing option which may be scheduled through cron or executed through a phantom process. This command is:

SENTRY.FILE.LOAD (BATCH)

To execute as a background job enter:

PHANTOM SENTRY.FILE.LOAD (BATCH)

You must be in the "sentry" directory to execute this job. Therefore, if you plan to use cron, the cron process must "cd" into the "sentry" directory BEFORE executing the command.

1.3 VALIDATE THE USER PROFILE DATABASE

This program is used to check the consistency of the users, groups and permissions which have been loaded into the SENTRY database via the first two programs described in this section. user IDs, groups, and their usage in the file system are analyzed and inconsistencies are reported. For example, the validation report might point out a file whose owner is not registered or a home pathname which does not exist on the system.

```
VALIDATION          SENTRY Database Validation          08/16/00

Enter "OK" to start the validation or "<ESC>" to exit : OK

Do you want to print missing password messages? (Y/N) or <ESC> to exit:  N

Validating user profiles

Validating groups

Validating file owners & groups

Validating COMMANDs

            *** Problems found during validation ***

              See Validation Report for Details

------------------------------ Database Invalid ------------------------------

Press <RETURN> to continue :
```

Figure 9 - *This is an example of the messages displayed to the user during the execution of the validation program.*

Validating the data you have loaded from your passwd and group files and from the file system is the third step which should be performed when you are first building the SENTRY database. Using this program you will be able to locate and correct any inconsistencies in your user profiles and groups. Use this program any time you wish to test for consistency of usage of user IDs, groups and file system protection. We encourage you to use it EVERY TIME you upload data from the passwd and group files and when you rebuild the B-tree files (which should be done on a regular basis).

This program will generate a printed report, using whatever printer setup is in effect at the time the program is run. To modify the printer, destination or form, use the SETPTR command at the TCL prior to running the program. Alternatively, the SENTRY XEQ function may be used to execute the SETPTR command.

To execute this program, select 1. Database Creation and Validation Menu from the SENTRY Main Menu. Next, select 3. Validate the User Profile Database from the Database Creation and Validation Menu.

Enter "OK" to start the validation or "<ESC>" to exit: - This is the first of two input prompts in this program. If you enter "**OK**", the program will continue. To exit at either prompt press <ESC> then enter <RETURN>.

Do you want to print missing password messages?(Y/N) or <ESC> to exit:

Your answer to this prompt controls whether or not the validation program tells you about users who have no passwords in the SENTRY database. If "**Y**" is entered the message

FATAL! User "USER.ID" does not have a password in the SENTRY database.

will print on the validation report.

When SENTRY retrieves the data from the passwd file, the password field is loaded into the SENTRY database. SENTRY cannot read the password or decrypt it! Only passwords created from the User Profile data entry screen, which are encrypted by SENTRY can be decrypted by SENTRY. Some system administrators choose to setup and track all user passwords through SENTRY. Others choose to have users manage their own passwords and not to maintain them in SENTRY. If you are not tracking user passwords, the "missing password" messages will be of little use to you.

We suggest that you answer "**N**"o don't print these messages unless you have created all passwords through the User Profile data entry screen or through one of SENTRY's password utilities.

Two types of errors are reported. These are called "FATAL" and "Warning". "FATAL" errors are those which we believe could possibly create a serious security issue or those which would lead to an operational problem. The following is a list of errors which we have labeled as FATAL.

1. **"User XXXXX not on the SENTRY.USERS file."** - The user name "XXXXX" was found in the list of SENTRY users in the SENTRY.CONTROL file, but no record was found for this user in the SENTRY.USERS file. This indicates an inconsistency in the SENTRY database; we suggest that the User Profiles be uploaded from UNIX again (selection 1 in the Database Creation and Validation Menu.)

2. **"User XXXXX does not have a password in the SENTRY database."** - The user "XXXXX" has no password in SENTRY. This message will ONLY appear if you answered "**Y**" to the prompt, "**Do you want to print missing password messages?**". If you are tracking passwords within SENTRY, this user should be assigned a password.

3. **"Password for User XXXXX is less than N characters."** - The user "XXXXX" has a password which is shorter than the minimum password length specified in the SENTRY System Profile screen, which is **N**. This user's password should be updated to conform to the minimum length restrictions you have instituted.

4. **"User XXXXX has no home directory."** - The user "XXXXX" has no home directory specified. This would prevent the user from logging in, as UNIX would not know where to attach the user upon login. The user should be updated and assigned a home directory.

5. **"User XXXXX has an invalid home directory - /ZZZZZ."** - The user "XXXXX" has a home directory in the SENTRY database of "/ZZZZZ", but SENTRY cannot locate this directory on your file system. Perhaps the directory was removed after it was assigned as the user's home directory. The user should be updated and assigned a valid home directory.

6. **"Group XXXXX is not on the SENTRY.GROUPS file."** - A Group name was found in SENTRY's control list which does not exist in the SENTRY.GROUPS file. This indicates that one of SENTRY's database files is damaged and should be rebuilt. Upload the passwd and group files to fix this problem.

7. **"Command XXXXX not on the SENTRY.COMMANDS file."** - A VOC protection item was found in SENTRY's control list which does not exist in the SENTRY.COMMANDS file. This indicates that one of SENTRY's database files is damaged and should be rebuilt.

Errors beginning with the word "Warning" are informational - not serious database issues but situations you should be aware of. The following is a list of those warnings.

1. **"User XXXXX will default to "other" protection on all objects and commands."** - The user "XXXXX" is not specifically mentioned, either by user ID or group membership, in the permissions for any file system object or any VOC command protected by SENTRY. He will fall into the "other" category for all protection on the system. This is NOT a problem, but could serve as an indication of a user ID which is obsolete and no longer used.

2. **"Group XXXXX is not used by any user."** - The group "XXXXX" is not being used by any user on the system. Therefore, no users will receive their access permissions via this group. This may be a group which is obsolete and should be removed or renamed.

3. **"Group XXXXX is not used to protect any object or command."** - The group "XXXXX" is not referenced in the permissions for any disk object or any VOC command. It may be assigned to users, but is not used to protect anything. This might be an obsolete group which should be removed or renamed.

4. **"Owner (UID) XXXXX on /ZZZZZ does not exist."** - The user ID number "XXXXX" is the owner of a disk object whose path is "/ZZZZZ". However, there is no user who is assigned this user ID number. Possibly, there once was a user but he has been deleted. The owner for this disk object should be replaced with a valid user on the system. Alternatively, a new or existing user could be assigned the same user ID number (UID).

5. **"Group (GID) XXXXX on /ZZZZZ does not exist."** - The group number "XXXXX" is the registered group for a disk object whose path is "/ZZZZZ". However, the group does not exist in SENTRY. Possibly, the group once existed but has been deleted. The group for this disk object should be replaced with a valid group on the system. Alternatively, a new or existing group could be assigned the same group number (GID).

6. **"Command /VVVVV does not have any groups or users assigned."** - The database command whose path is "/VVVVV" has only "other" access rights assigned. No users or groups are referenced in the command's protection. This may be because only "other" access rights are needed; everyone may have the same rights to the command. However, you should review the command protection to be sure it is what you intend.

7. . **"User (UID) XXXXX on command /VVVVV does not exist."** - The user ID number "XXXXX" is referenced in the protection for a database command whose path is "/VVVVV". However, there is no user who is assigned this user ID number. Possibly, there once was a user but he has been deleted. The user in this command's protection should be replaced with a valid user on the system. Alternatively, a new or existing user could be assigned the same user ID number (UID).

8. **"Group (GID) XXXXX on command /VVVVV does not exist."** - The group number "XXXXX" is referenced in the protection for a database command whose path is "/ZZZZZ". However, the group does not exist in SENTRY. Possibly, the group once existed but has been deleted. The group in this command's protection should be replaced with a valid group on the system. Alternatively, a new or existing group could be assigned the same group number (GID).

As the validation program progresses four messages will appear. These are:
Validating user profiles
Validating groups
Validating file owners & groups
Validating COMMANDs

When these four sections of the validation program are completed SENTRY will display "**Problems found during validation, See Validation Report for Details.**" The message "**Database Invalid**" will appear at the bottom of the screen if FATAL errors are encountered. If only WARNINGS are found the message displayed is "**Questionable data found during validation.**"

2. INTRODUCING THE DATABASE MAINTENANCE MENU

The second selection on SENTRY's Main Menu is **2. Database Maintenance Menu**. Through this selection you may access data entry screens to create, delete and modify the system profile, user profiles, groups, permissions, file ownership and Protection Command.

```
SENTRY                Main Menu              07 AUG 2000

    1. Database Creation and Validation Menu

    2. Database Maintenance Menu

    3. Reports Menu

    4. Utilities Menu


    Please select one of the above:  2
```

Figure 10 - *Database Maintenance is the second selection from SENTRY's Main Menu.*

Through using SENTRY to perform these tasks, you will enjoy data entry programs which validate parameters such as home path and group names. Cross reference lists for groups and users will assist you in creating just the users and groups you need without an inadvertent duplication.

These SENTRY maintenance programs assist you in cleaning up obsolete user IDs and groups that you no longer want. Through the data entry programs you may quickly access an unwanted group and remove all references to it. When SENTRY is used to remove a user ID, references to that ID are removed. SENTRY provides the maintenance link between the file system permissions, the passwd file and the group file.

2.0 DATABASE MAINTENANCE

This is the second sub-menu accessible from SENTRY's Main Menu. It is the menu you will use to make changes to the SENTRY database. You may create or modify users, groups and permissions through this menu.

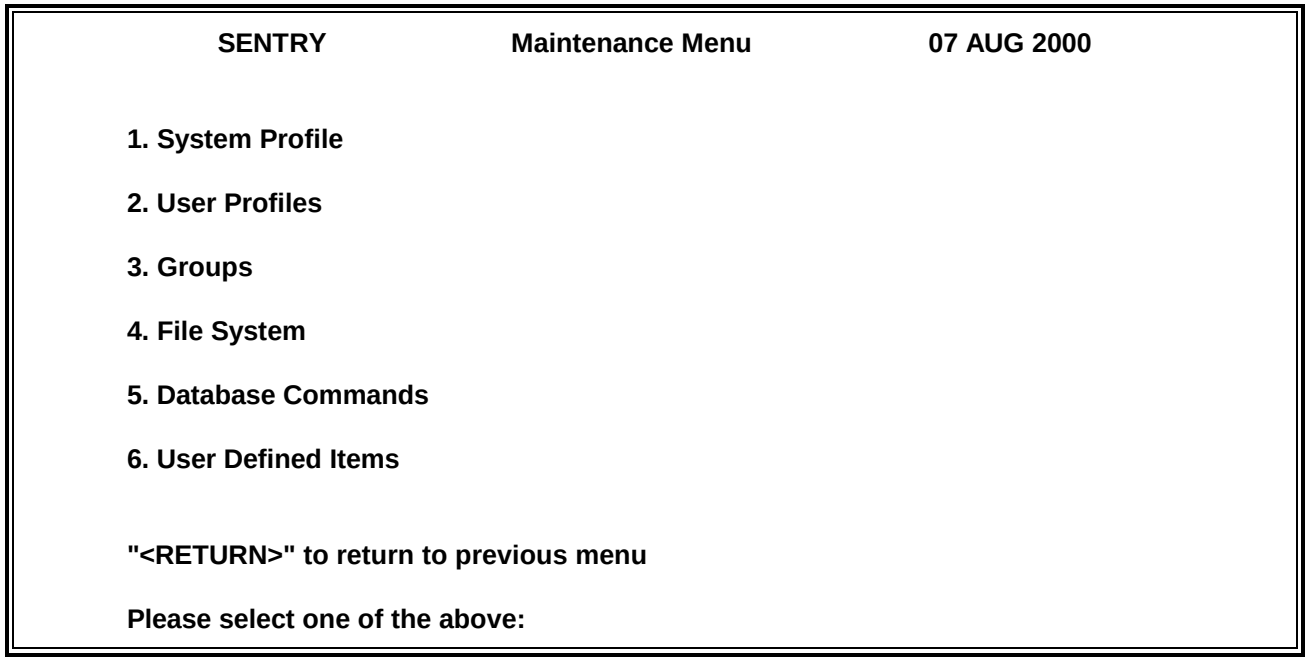

Figure 11 - *This is the "Maintenance Menu" invoked from SENTRY's Main Menu through selection 2.*

The six selections on this menu invoke data entry programs used to update the SENTRY database, file system permissions, the UNIX passwd and group files as well as SENTRY's Database Command Protection and User Defined Item Protection. Notice that we have used the word "Database" here. Depending upon which database system you are using (INFORMATION, uniVerse, or UniData), your actual SENTRY menu will replace the word "Database" with the name of the database which is in use on your system.

1. **System Profile.** This selection provides a data entry screen with which you may review or modify the system parameters. These parameters include password requirements, minimum and maximum lengths for user IDs, group names, pathnames and commands.

2. **User Profiles.** user IDs may be created, deleted and modified through this selection. User profiles include the user's name, department, telephone, password life, UID, GID, home directory, supplementary groups and login shell.

3. **Groups.** This selection offers you the ability to display the group GID, and the users associated with the group plus you may add a description to the record to document your system.

4. **File System.** This entry allows you to scroll through your UNIX tree structure much like you do in Window's File Manager. From this selection you may request "file detail" information which is read from the UNIX I-node. Included in this information is the last time the file was accessed and/or modified. In this screen you may change the owner, the group and the permissions.

5. **Database Commands.** You may create, delete, modify and review the special permission-like protection SENTRY offers for Verbs, Paragraphs, Sentences, Menus, and Procs through this entry. Users and groups may be given rights to execute an item only from within a program and/or from the database prompt. For example, this selection gives you the facility to restrict the use of "**DELETE**" at the database prompt, but still make it available should your application software need to execute it from within a program.

6. **User Defined Items.** This is a special SENTRY feature which allows you to define SENTRY security objects. These objects may be accessed through subroutine calls to solve unique security problems which may not be met through permissions and VOC item security facilities. For example, a personnel report is needed by a secretary who is completing a group insurance report. This report also displays salary information. A User Defined Item could be created so that the salary field displayed only asterisks (*). The User Defined Item could discriminate by user ID or by group to determine when to print the salary field. This would eliminate the need for ANOTHER report (which would increase the software Support burden for the MIS staff).

The following sections describe the functionality of each selection, the prompts, the availability of cross referencing and expected input. Examples of all screens are presented along with sample data.

2.1 SYSTEM PROFILE MAINTENANCE

This data entry program is used to display and change the system profile parameters. A number of these parameters are system specific and must be set to reflect YOUR system's limits. These parameters include maximums and minimums for password length, user ID length, and group name length. During installation, these parameters should be set appropriately for the limitations of your version of UNIX. Generally, UNIX provides an "include" file called limits.h in which most of these maximums and minimums are defined.

```
SYSTEM.MAINT          System Profile Maintenance          08/16/00

1. Null Passwords Allowed              : N
2. Minimum Password Length             : 6
3. Maximum Password Length             : 8
4. Enable Custom User Attributes       : Y
5. Password Format Mask                : ALPHA,LC
6. passwd File Order                   : Y
7. group File Order                    : Y
8. User & Group Case                   : LC
9. Minimum User ID Length              : 6
10. Maximum User ID Length             : 8
11. Maximum Group Name Length          : 8
12. Maximum UID Number                 : 1000
13. Maximum GID Number                 : 1000
14. Default Startup Command            : /bin/sh
15. Maximum Command Length             : 44
16. Maximum Startup Path Length        : 50
17. wtmp Valid Days Old                : 30
18. Punct for File Indexing            : .-_

Enter field number to modify, "C"ustom, "F"ile record or "<ESC>" to exit :
```

Figure 12 - *This is an example of the SENTRY Profile Maintenance Data Entry Screen. The displayed data are considered to be standard settings for most versions of UNIX.*

On first entering this screen you will note that this set of "default" values will be displayed. Review the list and change any parameter which is not appropriate for your version or UNIX or your environment. In the following paragraphs we will describe each parameter and suggest a value.

To execute this program, select 2. Database Maintenance Menu from the Main Menu. Next, select 1. System Profile from the secondary Maintenance Menu.

When this program is executed, the profile data will be read from the SENTRY database and displayed in the appropriate fields. There are 18 items defined on this screen. A detailed description of the data entry screen and prompts follows.

1. **Null Passwords Allowed** - The default of this field is "**N**". When set to "**N**"o, each user must have a password. If this field is set to "**Y**"es, you may create a user with a null password. For good security, passwords should be mandatory. This field controls the data entry program for creating new users. When creating a new user through the SENTRY data entry programs you will be REQUIRED to enter a password for the user or allow SENTRY to generate one for you if this field is set to "**N**". This is not a UNIX parameter. It is used only by SENTRY. This field accepts the values "**Y**" or "**N**".

2. **Minimum Password Length** - This is a UNIX parameter as well as one used by SENTRY when new users are created. The minimum password length may be 0 (zero) to "your maximum value" in length. However, most UNIX systems do not recognize more than 8 (eight) characters. More than 8 are ignored. The recommended and default value for this field is 6. Using at least 6 characters decreases the possibility that someone might guess a password or that a "break-in" might occur through computer generated guesses. A six character password is also short enough so that a user is not overly taxed to remember it (without writing it down). This field accepts only integer values 0 - 16.

3. **Maximum Password Length** - The UNIX limit is normally 8 characters. Your system may simply ignore any characters after the eighth one. The default and recommended value for this field is 8. This field accepts only integer values 0 - 16. The maximum value must be equal to or greater than the minimum password length value.

4. **Enable Custom User Attributes:** - Because the various flavors of UNIX offer different options for controlling passwords and login ids, Sentry manages these options via the "Custom User Attributes" interface. When your version of Sentry was installed this parameter was set to "**Y**" if your system offered additional options which most every system does.

5. **Password Format Mask** - This field is used by the User Profile data entry screen if you use SENTRY's generate new password option in the password field. If you plan to use this functionality you may select a "mask" of either ALPHA or ALPHANUM which generates either alphabetic or alphanumeric passwords. SENTRY will generate either a string of alphabetic characters such that the password is alternating consonants and vowels for the length of the string defined by the Minimum Password Length (selection 2 in this screen), or a string of characters beginning with an alphabetic character and containing at least one numeric. If this field is set to null or ALPHA, only alphabetic characters will be used. If the field is set to ALPHANUM, the generated password will contain at least one embedded numeric. The default and recommended value is ALPHA which will generate a string of alphabetic characters, the length defined by the Minimum Password Length field. If the minimum length field is 0 or null, a password of 6 characters will be used unless otherwise specified when the "**G**"enerate command is used in the password field of the User Profile data entry screen.

You may also control the case of generated passwords by adding either "**,LC**" or "**,UC**" to the password format field. The default is for generated passwords to be all lower case.

Many UNIX systems require that passwords must meet the following requirements:

- Each password must have at least six characters. Only the first eight characters are significant.

- Each password must contain at least two alphabetic characters and at least one numeric or special character.
- Each password must differ from the user name and from any reverse or circular shift of that name.

However, the System Administrator, (UID is zero) may create or change any password and those passwords created by the superuser do not have to comply with password construction requirements.

6. **passwd File Order** - This field is used by the User Profile maintenance program. If the value of this field is "**Y**"es, the names of the users are alphabetized in the UNIX passwd file. If you wish to maintain the current order of the passwd file this field should be set to "**N**"o. The default and recommended value is "**Y**"es. When alphabetized, the user "root" will be placed at the top of the passwd file.

7. **group File Order** - This field is used much the same as the passwd File Order field (item 7). It is used by the programs which create and modify users and groups. If the value of this field is "**Y**"es, the names of the groups are alphabetized in the UNIX group file. If you wish to maintain the current order of the group file this field should be set to "**N**"o. The default and recommended value is "**Y**"es.

8. **User & Group Case** - This field will contain LC (lower case), UC (upper case) or LIT (literal). It is used by the programs which create and modify users and groups. When entering the name of a user or group in User Profile or Groups screens the case of the name of the user or group will be set to the appropriate one selected by this field regardless of the case used when entering the name. For example, if a user name of TEST is entered in the User Profile screen, the case will be changed to "test" if this field is set to "**LC**". This parameter is intended to assist System Administrators who wish to be consistent in their usage of case when creating users and groups. If you do not want SENTRY to alter the case for users and groups set this field to "**LIT**" (literal). SENTRY will not alter the characters you have entered. The default and recommended value for this field is "**LC**" (lower case).

9. **Minimum user ID Length** - This field contains a number defining the minimum number of characters required for a user ID. A user ID must begin with an alphabetic character, contain no spaces and be unique. This field is used to verify the length of the user ID in the User Profile data entry program. The default and recommended value is 6.

10. **Maximum user ID Length** - This field contains a number defining the maximum number of characters allowed for a user ID. Most UNIX systems allow up to 8 alphanumeric characters. This field is used by the User Profile data entry screen to limit the length of user IDs created through SENTRY's data entry screens. The recommended and default value is 8.

11. **Maximum Group Name Length** - This value is used by the program to limit the number of characters in group names. Group names are used only as a translation for the GID for such UNIX utilities as "**ls**" and "**id**". Some UNIX systems allow more than 8 character group names but we recommend that your group names be no longer than 8 characters. The default and recommended value for this field is 8.

12. **Maximum UID Number** - This field defines the largest number which may be used as a UID. This maximum is a UNIX parameter. On some UNIX systems this number may be as large as 60,000.

However, we recommend using UIDs smaller than 5 digits simply to make them easier to read. The default and recommended value for this field is 1000.

13. **Maximum GID Number** - This field defines the largest number which may be used as a GID. This maximum is a UNIX parameter. On some UNIX systems this number may be as large as 60,000. However, we recommend using GIDs smaller than 5 digits simply to make them easier to read. The default and recommended value for this field is 1000.

14. **Default Startup Command** - This field contains the string executed at login for the user. It is generally the "shell" command. The User Profile uses this field as a default value for creating a new user. Simply returning past the startup command field will assign this value. The default value for this field is /bin/sh. The recommended value for this field is the "normal" startup command for your average user.

15. **Maximum Command Length** - This field is a UNIX parameter and is generally documented in the Administrator's Guide for adding a user ID. The value of this field should be consistent with your version of UNIX. On our system this maximum is set at 44 characters. Obviously a normal path to a UNIX shell (such as /bin/sh) will be much smaller than 44 characters. The default value for this field is 44 characters. The recommended value for this field is your system's maximum value.

16. **Maximum Startup Path Length** - This field is a UNIX parameter and is generally documented in the Administrator's Guide for adding a user ID. The value of this field should be consistent with your version of UNIX. On our system this maximum is set at 50 characters. This is the maximum number of characters allowed in the pathname commonly referenced as the "home" directory. It is the directory into which UNIX attaches the user at login. The default value for this field is 50 characters. The recommended value for this field is the maximum number allowed by your version of UNIX.

17. **wtmp Valid Days Old** - SENTRY determines users last login date and time by using a UNIX accounting file called "wtmp" which contains a log of user logins. The UNIX accounting feature which updates "wtmp" may be turned on and off. SENTRY has no way of knowing if accounting is turned on or not, so it looks for recent activity in the "wtmp" file. If no activity is found in the file during the last number of days specified in this parameter, SENTRY assumes that accounting is turned off and doesn't try to determine a user's last login date and time. Our default is set to 30 days.

18. **Punct for File Indexing** - SENTRY builds B-trees to provide rapid cross referencing into the file system. For example, let's imagine that you are looking for a file called "payroll.something". You can't remember the "something". In the File System screen you may enter "payroll" and SENTRY will search the B-trees for all references to "payroll". A list of pathnames to all files and directories whose name contains the string "payroll" will be displayed. The cross referencing on the word "payroll" is dependent upon the characters defined in this field. Special characters such as "." and "-" or "_" are used in file or directory names to make a compound name more readable. SENTRY's B-trees will use the set of characters defined here to break out the components of a compound name such as "payroll.ledger". This file would be indexed on the word "payroll" and on the word "ledger". Care should be taken in selecting these characters for cross referencing; limit them to those which are commonly used. The size of the B-trees increase significantly as the number of characters in this list increases.

Note that the indexing occurs at the time that the "**Create Database from File System**" program is run from the Database Creation and Validation Menu. If the punctuation characters used are changed, the program must be rerun to put the new indexing into effect.
Enter field number to modify, "**C**"ustom, "**F**"ile record or **"<ESC>**" to exit: - This is the primary modifications prompt for this screen. To address any field simply type the associated number, 1 to 18, followed by <RETURN>. That field will be cleared of any data which may currently be displayed there and the program will await your input. To delete a field, enter a space followed by a <RETURN>. If the screen is awaiting input at a prompt and you wish to backup to a previous prompt, enter "**^**" and <RETURN> until you are positioned at the field you wish to modify. You may type "**HELP**" at any input prompt. A HELP screen will be displayed. To exit HELP, simply enter <RETURN>.

To access the Custom User Default Maintenance screen, enter "**C**" <RETURN>. A new data entry screen will be displayed where you may set the parameters which are used as the default in the User Maintenance program. In the User Maintenance program you will be able to access these same parameter and change them on a per user basis. To save time and provide consistency in setting parameters for users, we recommend you set the defaults to those most commonly used.

If you have made changes to the data in this screen remember to enter "**F**" to file or your changes will be discarded. To leave this screen without filing any changes enter <ESC> followed by <RETURN>.

Custom User Default Maintenance – SUN

The SUN operating system offers five options for managing passwords. Our "Custom User Default" program allows you to set these parameters if desired. These defaults are used when you create users in the User Maintenance program. By setting up defaults you may save time during the data entry necessary to create a new user plus you will be aided in creating consistency in the password management for all users if you desire.

```
CUSTOM.USER          Custom User Default Maintenance          08/16/00

                          User :  DEFAULT

1: Minimum password change (days)      :  5
2: Maximum password change (days)      : 90
3: Password change warning (days)      :  5
4: Maximum inactive time (days)        : 21
5: Expiration date (MM/DD/YY)          :

Enter field number, "F"ile or "<ESC>" to exit :
```

Figure 13 - *This is an example of the "Custom User Default Maintenance" data entry screen.*

To execute this program, enter "**1**" System Profile Maintenance from the Main Sentry menu, after recalling an exiting user or entering a new user you may enter "**C**" at the bottom prompt. Entering "**C**" invokes this program. The following paragraphs describe the five available options.

1. **Minimum password change (days):** Enter the number of days before a user is allowed to change his existing password. For example, if UNIX has just expired a users password and the user enters a new one, you can use this parameter to prevent the user from resetting his password to the old one for the number of days you specify. The idea is that if the user is forced to keep the new password for several days, he will not change it back to the older one. We recommend 5 days.

2. **Maximum password change (days):** Enter the number of days before a user is forced by UNIX to change his password. Many companies use 90 days as a standard. This would allow a user to keep a new password for 90 days before he was forced by UNIX to enter a new password. This is 90 calendar days.

3. **Password change warning (days):** Enter the number of days before a new password is required that you would like UNIX to warn the user that his password is about to expire. We recommend 5 days.

4. **Maximum inactive time (days):** This field is used to protect inactive logins. For example, if a user did not use his login id for a specified number of days such as 21, UNIX would automatically expire the password. At that time the system administrator will have to re-instate the password to allow logins for that user id. Enter the number of days the login can remain active before it is expired. We chose 21 because we expect vacations and sick leave to be less than three weeks. Any event greater than three weeks would be a special circumstance and we would deal with that on an individual basis.

5. **Expiration date (MM/DD/YY):** There may be login ids which are created for short term use such as for auditors or seasonal employees. You may wish to enter a date when the login id will expire for these types of users. Because this is the default screen, setting a default expiration date is not very logically unless the entire user system is to be drastically changed on a certain date.

The last line of the screen is:

Enter field number, "F"ile or "<ESC>" to exit:

If you wish to modify any of the fields, 1 through 5, enter the number of the field you wish to change followed by <ENTER>. After you have made changes enter "**F**" to file/save your changes. To exit the program without saving any changes, enter **<ESC>**. You will be returned to the "System Profile Maintenance screen.

2.2 USER MAINTENANCE

This data entry program is used to display, change, and delete user IDs, including documentation for the user, UID, GID, home directory, and initial startup command. Additionally, all supplementary groups are displayed in this screen. Supplementary groups may be added and deleted from the user's profile. Cross referencing is available to list existing users and their UIDs, existing groups and their GIDs, and home directories in use.

```
USER.MAINT              User Maintenance              08/08/00

user ID : peggy                    Last Login : Mon Jun 20 15:05

1. User Name          : Long Peggy
2. Department         : Office 123
3. Telephone          : 303/755-1102
4. Password           : ***************
5. UID                : 0 (peggy,root)
6. GID                : 20 (users)
7. Home Directory     : /users/peggy
8. Command            : /bin/sh
9. Groups             : 01>   20 (users)


Enter field number, "C"ustom, "F"ile, "DEL"ete or "<ESC>" to exit :
```

Figure 14 - *This is an example of the "User Maintenance" data entry screen which is invoked via Selection 2 on the "Database Maintenance Menu".*

This program is used to create, delete and modify a user's profile. It is also a very handy utility to use to review the supplementary groups in use by a particular user. Additionally, you may access this data by entering the user's ID or the user's name through the cross reference facility. For large systems, the user's name, department, and telephone number aids in monitoring computer usage. For example, if you observe that a user with the ID of "usr545" is performing a very CPU intensive task, you may be interested in learning which program he is running. Using this screen you may retrieve the data record for this user, see that he is in the Payroll department, get his name and telephone number and call to inquire what process he is executing.

To execute this program, select 2. Database Maintenance Menu from SENTRY's Main Menu; then, select 2. User Maintenance from the Database Maintenance Menu. The User Maintenance program will be invoked.

A detailed description of the data entry screen (Figure 15) and prompts follows.

When first invoked, no data will be displayed in this screen. You will be prompted to enter the user ID which you wish displayed. For a list of all users defined on the system, enter "@". To search the

SENTRY database using the user's name, enter "**@**" followed by the first or last name of the user. For example, if you wanted to search for user IDs for Peggy Long, you could enter "**@long**". If there were more than one "long" or if Peggy had more than one ID, a list would be displayed from which you could choose the appropriate user. When there are many users with common names, you may enter both first and last names to narrow the search; for example, "tom smith" or "smith tom". Note that this cross reference capability is dependent upon your putting the names of new users in a consistent format. Before setting up a new user ID, you should always search for old IDs to prevent setting up unnecessary or unwanted IDs.

To create a new user ID, enter the ID at the user ID prompt. Use an ID of a length that conforms to the maximum and minimum user ID parameters set in the System Profile screen (the first menu item described in this section). Most UNIX systems use user IDs which are no greater than 8 characters in length and use only letters and numbers.

Use a consistent naming convention to assist the System Administrator. A preferred scheme at many sites is to use the person's first initial and last name (e.g. p.long or the reverse long.p). This is particularly helpful in routing printouts to the proper person. Note that the preferred case is lower. The controlling case parameter is set in the System Profile screen.

1. **User Name** - This field is intended to identify the user. For reporting purposes, it is best to enter the last name, first name, and middle initial. For user IDs which are not related to a specific user such as "payroll", you may wish to enter a descriptive phrase such as "Special ID for check runs". This field provides cross referencing for the user ID field.

2. **Department** - Enter the department name or some meaningful descriptor such as floor or building location. This is a free form optional text field used for reporting only. Use some scheme which will be valuable in your environment.

3. **Telephone** - Enter the telephone number where the user of this ID may be reached. This too is an optional field which is intended to assist the System Administrator in locating a user when needed. A recommended format for telephone numbers is area/nnn-nnnn (e.g. 303/755-1102). If all area codes are the same for your users then you may wish not to include it in this field. Perhaps only the extension number is needed in your environment.

4. **Password** - User passwords must conform to the specifications for length and requirements set in the System Profile. If you are creating a new user ID, enter the user's password at this prompt. It will be displayed in the screen only while you are using this prompt. Passwords are encrypted on the SENTRY database so that they may be protected from disclosure. Only the System Administrator may view passwords.

Because it is a good security policy to change all passwords frequently, SENTRY provides a password generator to assist the System Administrator in creating pronounceable yet meaningless passwords. To use the SENTRY password generation program, enter "**G**" at the password prompt. A password conforming to the System Profile specifications will be generated. Passwords generated by this program will be composed of a consonant and vowel pattern in order to be pronounceable and therefore easier for the user to remember WITHOUT writing them down! Optionally, the password generation program may be

configured (through the System Profile screen) to generate alphanumeric passwords, which will contain at least 1 numeric character.

If the System Profile is set to allow null passwords to be optional, you may <RETURN> past this prompt leaving it null. We do not recommend null passwords. Every user should have a unique user ID and passwords should be changed on a regular basis.

5. **UID** - This field defines the UID number for the user. Because UNIX references users internally by their number, not their user ID, a UID may not be unique (e.g. root UID = zero). All users with the same UID have the same privileges. File ownership is defined by the UID not the user name. In our example screen note that the UID of 0 (zero) for the user ID "peggy" is used for both "peggy" and "root". These user IDs appear to the right of the field in parentheses. Cross referencing is available at this prompt. Enter "@" for a list of all users and their UID's. Enter "@" followed by part of a user name to cross reference by name. For example, enter "**@long**" to see a list of users with the name "Long". SENTRY will generate a new UID if the character "**N**" is entered at this prompt. Generally speaking, it not a good security practice to have more than one user ID with the same UID. A standard UNIX convention is to assign all "normal" users UID's greater than 100. Numbers lower then 100 are customarily assigned to special system user IDs. A record called NEXT.NUMBER in the SENTRY.CONTROL file is maintained by SENTRY to provide the next available number. You may edit this record and start it at your preferred starting number. The largest UID number is defined by the System Profile program and should be set no higher than your system's limit.

6. **GID** - This field defines the GID number for the user. This number specifies the user's primary group membership. Although the user may belong to supplementary groups, this field defines the primary group. The name of this group is translated via the UNIX "group" file and the GID may be used in assigning file system permissions.

To review a list of groups defined on your system and their GIDs, enter "@" at this prompt. You may choose a group from this "pick" list. The name of the group will display in parentheses to the right of the file. If you enter an "**N**" SENTRY assumes that you wish to create a new group. The next available GID will be assigned and you will be prompted to provide a Group Name.

At this prompt you may enter "@" for a list of defined groups, "@" followed by part of a group name to see a cross reference list, an existing GID, a new GID, the name of an existing group (SENTRY will look up the GID), or an "**N**" and SENTRY will generate the next available GID. Because some versions of UNIX limit the number of simultaneous supplementary groups to 8 your group assignments should be carefully planned so that you have no user who requires membership in more than 9 groups (one primary and 8 supplemental).

7. **Home Directory** - The directory to which the user is initially attached at login is commonly called the "home" directory. Enter the path to this directory here. A cross reference list is available by entering "@". This will provide a list of all the paths defined as "home" directories in use by the users on your system.

8. **Command** - This field normally defines the startup UNIX shell the user invokes. The System Profile provides a "default". If you wish to use the default you need only press <RETURN>. Otherwise, enter the path to the UNIX shell you wish this user to invoke at startup.

9. **Groups** - This field is multi-valued and lists the user's supplementary groups. The GID for each group is displayed along with the group name in parentheses. Some systems allow only 8 simultaneous supplementary groups. Take care that you plan your group memberships carefully so that you do not need to exceed this limit.

At this prompt you may enter a new group name, an existing group name, a "@" for a list of existing groups and their GID's, or a "@" followed by part of a group name to see a cross reference list by group name.

Enter field number, "C"ustom, "F"ile, "DEL"ete or <ESC> to exit - This is the standard modifications prompt for the User Maintenance program. You may access any field by entering the number to the left of the field, such as "**2**" for the Department field prompt.

```
                                SUN
                    Custom User Data Maintenance
08/16/00
                                User :  peggy

  1: Minimum password change (days)      :   5
  2: Maximum password change (days)      :  90
  3: Password change warning (days)      :   5
  4: Maximum inactive time (days)        :  21
  5: Expiration date (MM/DD/YY)          :  12/31/00

Enter field number, "F"ile or "<ESC>" to exit :
```

Figure 15 - *This is an example of the "Custom User Data Maintenance" data entry screen.*

To execute this program, enter "**2**." User Maintenance from the Main Sentry menu, after recalling an exiting user or entering a new user you may enter "**C**" at the bottom prompt. Entering "**C**" invokes this program. The following paragraphs describe the five available options.

1. **Minimum password change (days):** Enter the number of days before a user is allowed to change his existing password. For example, if UNIX has just expired a users password and the user enters a new one, you can use this parameter to prevent the user from resetting his password to the old one for the number of days you specify. The idea is that if the user is forced to keep the new password for several days, he will not change it back to the older one. We recommend 5 days.

2. **Maximum password change (days):** Enter the number of days before a user is forced by UNIX to change his password. Many companies use 90 days as a standard. This would allow a user to keep a

new password for 90 days before he was forced by UNIX to enter a new password. This is 90 calendar days.

3. **Password change warning (days):** Enter the number of days before a new password is required that you would like UNIX to warn the user that his password is about to expire. We recommend 5 days.

4. **Maximum inactive time (days):** This field is used to protect inactive logins. For example, if a user did not use his login id for a specified number of days such as 21, UNIX would automatically expire the password. At that time the system administrator will have to re-instate the password to allow logins for that user id. Enter the number of days the login can remain active before it is expired.

5. **Expiration date (MM/DD/YY):** There may be login ids which are created for short term use such as for auditors or seasonal employees. You may wish to enter a date when the login id will expire for these types of users.

The last line of the screen is:

Enter field number, "F"ile or "<ESC>" to exit:

If you wish to modify any of the fields, 1 through 5, enter the number of the field you wish to change followed by <ENTER>. After you have made changes enter "**F**" to file/save your changes. To exit the program without saving any changes, enter **<ESC>**. You will be returned to the "User Maintenance" screen.

In UNIX every file has an owner and a group. The references to owners and groups are the UID and the GID for each. The actual names are NOT stored, only the number. The numbers are translated to names by various UNIX utilities through a "lookup" process in the passwd and group files. If a user is deleted who owns files, his UID will continue to be the "owner". Because this relationship between user IDs, UIDs and file ownership is only a logical link, it is common to find files with UIDs which don't exist on the system. This can be a serious security problem should the System Administrator delete a user ID (where the user was a file owner) and later reassign that old user's UID to a new user. It is possible that the new user would then have access to files he should not be allowed to use. SENTRY will notify the System Administrator of this issue when a user ID is deleted.

If you delete a user ID who shares the same UID with another user and that UID "owns" files, the delete will proceed without notification. You will be able to recognize this condition because the display for UID on the User Profile screen will list all users with the same UID.

When a user is deleted who "owns" files and the UID is unique, SENTRY will advise the Administrator and offer a menu of four choices. Here is an example of this screen.

To invoke the Custom User Data Maintenance screen enter "**C**" followed by <ENTER>. The fields and prompts in this screen are dependent upon the brand (e.g. HP, DG, SUN, IBM) of computer you have. Please locate the appropriate documentation in the following pages. If you do not find documentation which matches the Custom screen on your copy of Sentry, please give us a call.

To exit you must save your changes by entering "**F**". If you make no changes or wish to cancel your session without saving changes, enter "**<ESC>**". The User Maintenance screen will be redisplayed sans data.

To delete a user enter "**DEL**" at this prompt. You will be prompted:

Are you sure you want to delete the entire record(YES/NO)?

Entering "**YES**" will cause the deletion to proceed. Entering "**NO**" will cause the program to return to the primary User Maintenance screen.

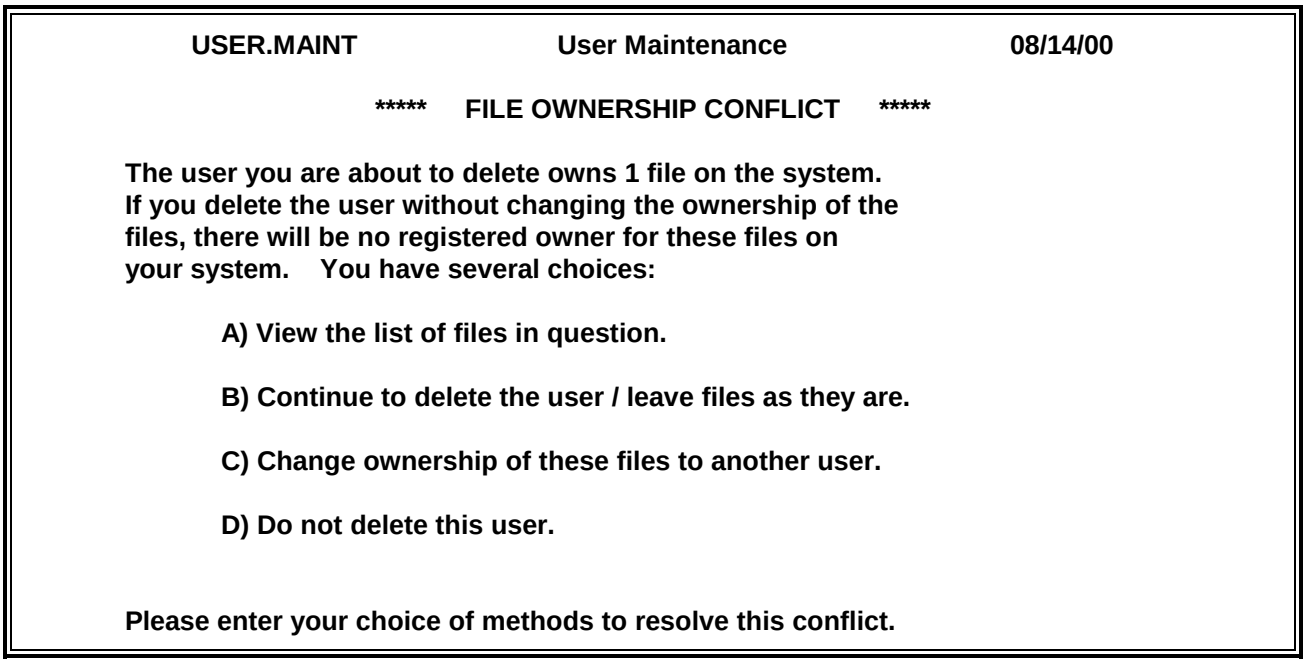

Figure 16 - *This is a sample of the FILE OWNERSHIP CONFLICT screen. The user is offered four choices. Enter the letter to the left of your choice to execute.*

The four choices provided through this screen are described in the following paragraphs.

A) View the list of files in question. This list of files will be displayed in a scrolling window. Note that the number of files owned by the user will be displayed in the "FILE OWNERSHIP CONFLICT" screen (Figure 16). Enter "**A**" to view this list.

In the following screen note that SENTRY displays a list of all files owned by this user. This is a scrolling window if there are more files than can be displayed on one screen. User "**F**" or "**B**" to scroll forward or backward. Enter **<ESC>** to leave this screen.

```
/jaf

Enter "<ESC>" to quit :
```

Figure 17 - *This is an example of the list of files owned by the user being deleted - Selection A.*

B) Continue to delete the user / leave files as they are. This option deletes the user from the passwd and group files but leaves the UID as the owner of the files. Enter "**B**" to select this option.

C) Change ownership of these files to another user. This selection will prompt for a new owner. All of the standard user prompt option function at this prompt, including cross referencing using the "@" character. This is a global change. All files "owned" by the old user will be "owned" by the specified new user. If you wish to change some of the old owner's files to one user and some to another user, you must make your changes through the File System maintenance screen. To select this *global* change option, enter "**C**". SENTRY will display the file pathname and it's progress through the list of files. Here is a sample of the screen SENTRY displays when this choice is invoked (Figure 19).

```
USER.MAINT          User Maintenance          08/14/00

Changing file ownership from user 119 (test)

New owner : 0 (peggy,root)


Do you want to change file ownership from UID 119 to UID 0 (Y/N)?
```

Figure 18 - *This screen is an example of the prompt for a replacement file owner - Selection C.*

```
USER.MAINT          User Maintenance          08/14/00

Changing file ownership from user 119 (test)

New owner : 0 (peggy,root)

Path  : /jaf

Count : 1 of 1

Press return to continue...
```

Figure 19 - *This is an example of the screen as it appears after the new owner has been installed in the example above.*

D) Do not delete this user. This option allows the user to return to the main User Maintenance menu without altering the user ID or the file system. No changes are made. To select this option enter "**D**". You will be returned to the User Maintenance screen.

In summary, the User Maintenance screen allows you to create new users, modify existing users and delete users. Remember that file ownership is linked to users via the UID. SENTRY will advise you when deleting a user will cause a file to have an "unregistered" owner.

2.3 GROUP MAINTENANCE

Through this data entry program you may add and delete groups from the system, add a descriptive text field to document a group and assign the group's GID.

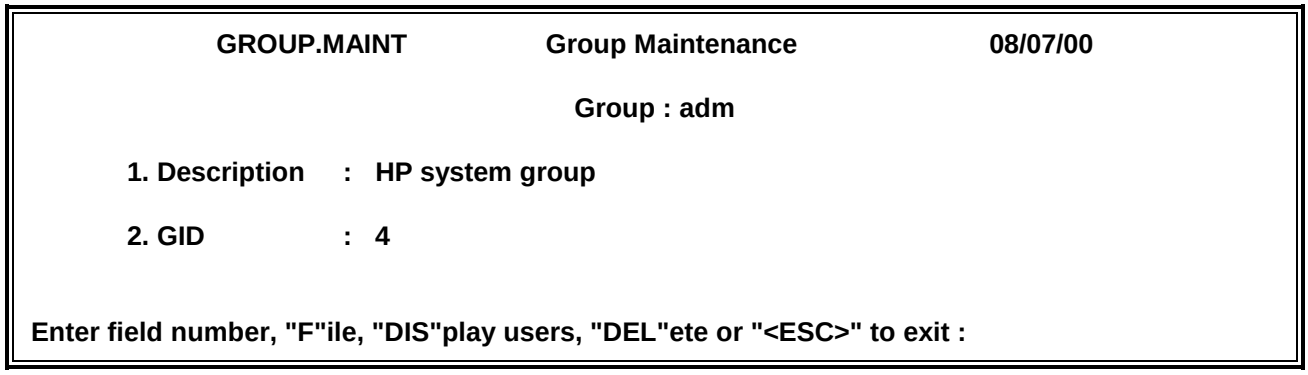

Figure 20 - *This is an example of the "Group Maintenance" data entry screen. This program is invoked via Selection 3 of the "Database Maintenance Menu".*

This screen is predominately used for display purposes. It provides an easy way to view the list of users who are assigned to a particular group plus the screen defines whether the group is a GID for a user or a supplementary group.

To execute this program, select 2. Database Maintenance Menu from the SENTRY main menu then select 3. Group Maintenance from the Database Maintenance Menu. This program will be invoked.

A detailed description of the Group Maintenance screen (Figure 21) and prompts follow. Examples of the "Users using group" screen and the FILE GROUP CONFLICT screens are also included in this chapter.

When first invoked, no data will be displayed in this screen. You will be prompted to enter the name of a group. For a listing of all groups defined for the system enter "**@**". You may also search for a group by using any word from the Group Description field. For example, if you recall that a group description uses the word "ACCOUNTING", you may access the group name by entering "**@ACCOUNTING**" in the first prompt of this screen. If more than one group is found using this description, a list of group names will be presented from which you may choose the appropriate one.

To create a new group simply enter the name of the new group. You will be prompted for a description and GID for the new group.

1. **Description** - Enter a word or phrase which documents the purpose or nature of this group. This is a text field which is used for reporting, documentation and as a cross reference for the group name.

2. **GID -** This is the number assigned to this group name. You may use "**@**" for a list of all groups and their associated GID's. You may assign a number or enter "**N**" and SENTRY will assign the next available number.

Enter field number, "F"ile, "DIS"play users, "DEL"ete or <ESC> to exit. The is the standard modifications prompt for the Group Maintenance program. To access any selection on the screen, enter the number associated with that selection. If you have created a group or changed/added a description, or GID you must enter "**F**" to save your work and exit. You will then be asked

Do you want to update the UNIX group file (Y/N)?

Enter "**Y**"es to save the changes in the UNIX group file.

If you have only changed or added a description, this is not stored in the UNIX file and there is no need to update UNIX.

Entering "**DIS**" will cause SENTRY to display a list of users who are members of the group which you have retrieved from the SENTRY database. SENTRY will display the following screen.

Users using group adm (2 Users)

user ID	GID	Groups
adm	Yes	Yes
root		Yes

"F"orward page, "B"ackward page or <RETURN> :

Figure 21 - *This is a sample of the "Users using group ..." screen. Note that the header contains the name of the group and the number of users who are members of this group.*

The left most column is the alphabetized list of user IDs. The next column labeled "GID" will contain "Yes" if the user to the left is assigned this group in the passwd file. We refer to this group as the user's primary group or GID group. The right most column with the heading of "Groups" displays a "Yes" if the user was assigned membership to the group in the UNIX group file. These are commonly referenced as "supplementary" groups. If the list is longer than can be displayed, use "**F**" or "**B**" to scroll forward and backward through the list. Enter <RETURN> to go back to the Group Maintenance screen.

To delete a group enter "**DEL**" at the "modifications" prompt. You will be prompted:

Are you sure you want to delete the entire record(YES/NO)?

Entering "**YES**" will cause the program to proceed. Entering "**NO**" will cause the program to return to the primary Group Maintenance screen.

In UNIX every file has an owner and a group. The references to owners and groups are the UID and the GID for each. The actual names are NOT stored, only the number. The numbers are translated by various UNIX utilities through a "lookup" process in the passwd and group files. If a group is deleted which is the group for files, the GID will continue to be the file group. Because this relationship between group, GIDs and file group is only a logical link, it is common to find files with GIDs which don't exist on the system. This can be a serious security problem should the System Administrator delete a group (where the group is associated with files) and later reassign a new group name and new users to an old number. It is possible the users in the new group would then have access to files they should not be allowed to use. SENTRY will notify the System Administrator of this issue when a group is deleted.

When a group is deleted which is the group for files and the GID is unique, SENTRY will advise the Administrator and offer a menu of four choices. Here is an example of this screen.

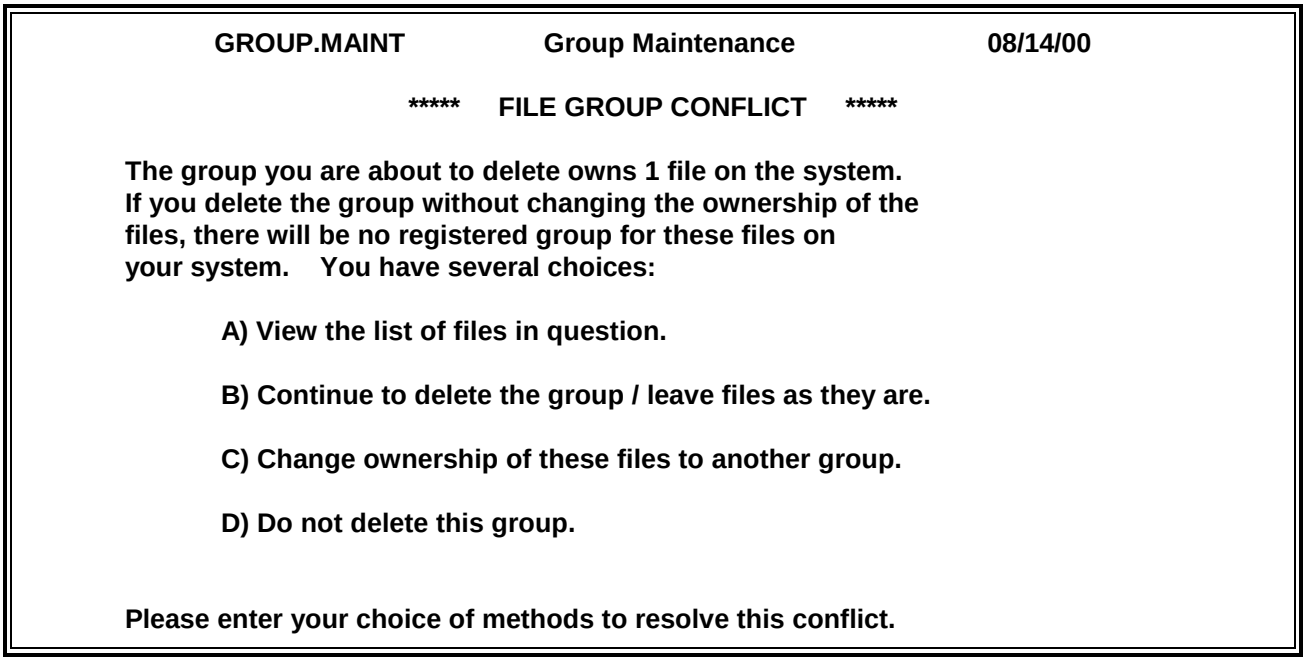

Figure 22 - *This is a sample of the FILE GROUP CONFLICT screen. The user is offered four choices. Enter the letter to the left of your choice to execute.*

The four choices provided through this screen are described in the following paragraphs.

A) View the list of files in question. This list of files will be displayed in a scrolling window. Note that the number of files owned by the group will be displayed in the "FILE GROUP CONFLICT" screen (Figure 22). Enter "**A**" to view this list.

In the following screen note that SENTRY displays a list of all files owned by this group. This is a scrolling window if there are more files than can be displayed on one screen. User "**F**" or "**B**" to scroll forward or backward. Enter <ESC> to leave this screen.

```
GROUP.MAINT          Group Maintenance          08/14/00

Files owned by group 140 (devel)
        /jaf

        Enter "<ESC>" to quit :
```

Figure 23 - *This is an example of the list of files owned by the group "devel". Selection A displays this list.*

B) Continue to delete the group/leave files as they are. This option deletes the group from the group file but leaves the GID as the file group. If there are users with this group as their GID in the passwd file, these references are not deleted. Enter "**B**" to select this option.

C) Change ownership of these files to another group. This selection will prompt for a new group. This is a global change. All files with the old group will be changed to the specified new group. If you wish to change some of the old group's files to one group and others to another group, you must make your changes through the File System maintenance screen. To select this *global* change option enter "**C**". SENTRY will display the file pathnames and its progress through the list of files. Here is a sample of the screen SENTRY displays when this choice is invoked (Figure 25).

```
GROUP.MAINT          Group Maintenance          08/14/00

        Changing file ownership from group 140 (devel)
        New group : 20 (users)

        Do you want to change file group from GID 140 to GID 20 (Y/N)?
```

Figure 24 - *This is an example of the prompt for a replacement group - Selection C.*

```
GROUP.MAINT          Group Maintenance          08/14/00

        Changing file ownership from group 140 (devel)
        New group : 20 (users)
        Path  : /jaf
        Count : 1 of 1

        Press return to continue...
```

Figure 25 - *This is an example of the screen which is displayed after the replacement group (previous example) is chosen.*

D) Do not delete this group. This option allows the user to return to the main Group Maintenance menu without altering the group or the file system. No changes are made. To select this option enter "**D**". You will be returned to the Group Maintenance screen.

2.4 FILE SYSTEM

With this program you may change owners, groups and the permissions for any file or directory in your file system. With Sentry's extensive B-tree system of cross references, you may use this program to locate the path to any object on your system.

FILE.MANAGER **General File Utility** **12:02:32 08 AUG 2000**

Path : / **(32 entries.)**

top...

-->	**drwx------**	**root**	**mail**		**.elm**
	r--r--r--	**bin**	**bin**	**9675**	**.profile**
	-r--r--r--	**bin**	**bin**	**8507**	**.profile.orig**
	-rw-------	**root**	**sys**	**7**	**.rhosts**
	-rw-rw-rw-	**root**	**sys**	**362**	**.sh_history**
	-rw-rw-rw-	**root**	**sys**	**816**	**.ustk_root**
	-r--r--r--	**root**	**sys**	**10**	**.uvhome**
	-rw-rw----	**root**	**sys**	**0**	**IDMERROR.console**
	-rw-rw----	**root**	**sys**	**0**	**IDMERROR.pty-ttyp3**
	drwx------	**root**	**mail**		**Mail**
	-rwxr-xr-x	**root**	**root**	**2637824**	**SYSBCKUP**
	drwxr-xr-x	**root**	**other**		**bin**
	drwxr-xr-x	**root**	**other**		**dev**
	drwxr-xr-x	**root**	**other**		**etc**
	drwxr-xr-x	**root**	**other**		**exl_usr**
	-rwxr-xr-x	**root**	**sys**	**2691072**	**hp-ux**
	-rw-rw-rw-	**root**	**sys**	**233**	**jaf**

Figure 26 - *This is an example of the "General File Utility" screen. You may scroll through directories and files, displaying their owner, group, permissions and size.*

Although you may make few changes to the permissions on your system once they are set, you will find that this screen offers you easier access to your file system and much more detail concerning your files than is available through the common UNIX utilities. On entering this program note that SENTRY displays the root path (/) at the top left of the screen. To the right, the number of entries in the currently displayed directory is reported. In our example there are 32.

There are 20 easy-to-remember key strokes which you will want to learn to fully utilize the power of this screen. Should you forget one, simply enter "**H**" or "**?**" for HELP. The following screen will be presented.

```
FILE.MANAGER          General File Utility          16:24:02 07 AUG 2000

                              CURSOR.MAIN

=============================================================================

HELP for "Cursor Control and Commands"
There are twenty commands which may be entered at any position on the
screen.  None of the commands require a carriage return -- simply type
the keystrokes for the command.

          UP -  U                    EXPLODE -  EXP
        DOWN -  D                    IMPLODE -  I
     PAGE.UP -  ^U                ROOT LEVEL -  R
   PAGE.DOWN -  ^D          CROSS REFERENCE -  @
         TOP -  T              CURSOR RESET -  C
      BOTTOM -  B
                                 FILE DETAIL -  F
        QUIT -  <ESC>          VIEW DEFAULT -  VD
        HELP -  '?' or 'H'       VIEW GROUP -  VG
     EXECUTE -  XEQ              VIEW USER -  VU
     REPAINT -  ^^


Press <RETURN> to continue . . .
```

Figure 27 - *This is an example of the help screen which defines the special key strokes available in the "General File Utility" program. Please note that ALL key strokes use upper case letters.*

The first set of 6 key strokes described in the Help screen are key strokes used to "move around" in the display of the file system. These are very simple to remember. "**U**"p and "**D**"own moves the cursor one line. "**^U**"p and "**^D**"own scrolls the screen up one page or down one page just like Page UP and Page Down in a word processor. Note that the caret "^" before a letter means to hold down the "control" key when pressing the letter - for example, "**^A**" means control-A, one key stroke. "**T**"op and "**B**"ottom moves the cursor to the top or bottom of the screen.

To display the contents of a subdirectory first position the cursor on the directory you want to "explode". Note the "d" to the left of the permissions string defines which entries are directories. Next enter "**EXP**". SENTRY will repaint the screen displaying the contents of the targeted subdirectory.

To move from a subdirectory to one level "up" use "**I**"mplode.

To move to the root directory enter "**R**" for root directory.

To reset the cursor enter "**C**".

One of the most valuable functions of this program is the ability to find files and directories without knowing the full path or the full name in some cases. To use the cross reference enter "@". You will be prompted:

Enter name for cross reference:

In our following example, we used "peggy" as input. Note that all of the files and directories contain the word "peggy" in the pathname.

```
     FILE.MANAGER        General File Utility        14:49:04 14 AUG 2000

Cross Reference for "peggy"                          (3 found.)

top...
--> /users/pc_archive/peggy                          directory
    /users/peggy                                     directory
    /usr/spool/cron/crontabs/peggy


bottom
```

Figure 28 - *This is an example of the cross reference list SENTRY provides through the General File Utility screen. To invoke the cross reference function, enter "@". From the cross reference display, you may choose many of the standard commands. For example, to go to the directory containing one of the displayed files, position to that line and enter "I" (implode). To view the contents of a displayed directory, use "EXP" (explode).*

If your system uses ACLs, please turn to the "ACLs Maintenance" topic on page 2-26. To change the permissions, owner or group of a file or directory, first position the cursor to the object you wish to change, then enter "**F**"ile Detail. The "**Detailed File View**" screen will be displayed.

NOTE: If your UNIX system does not support ACLs or if you have chosen not to use ACLs, your copy of SENTRY will display the screen called "Detailed File View". An example is shown on the following page.

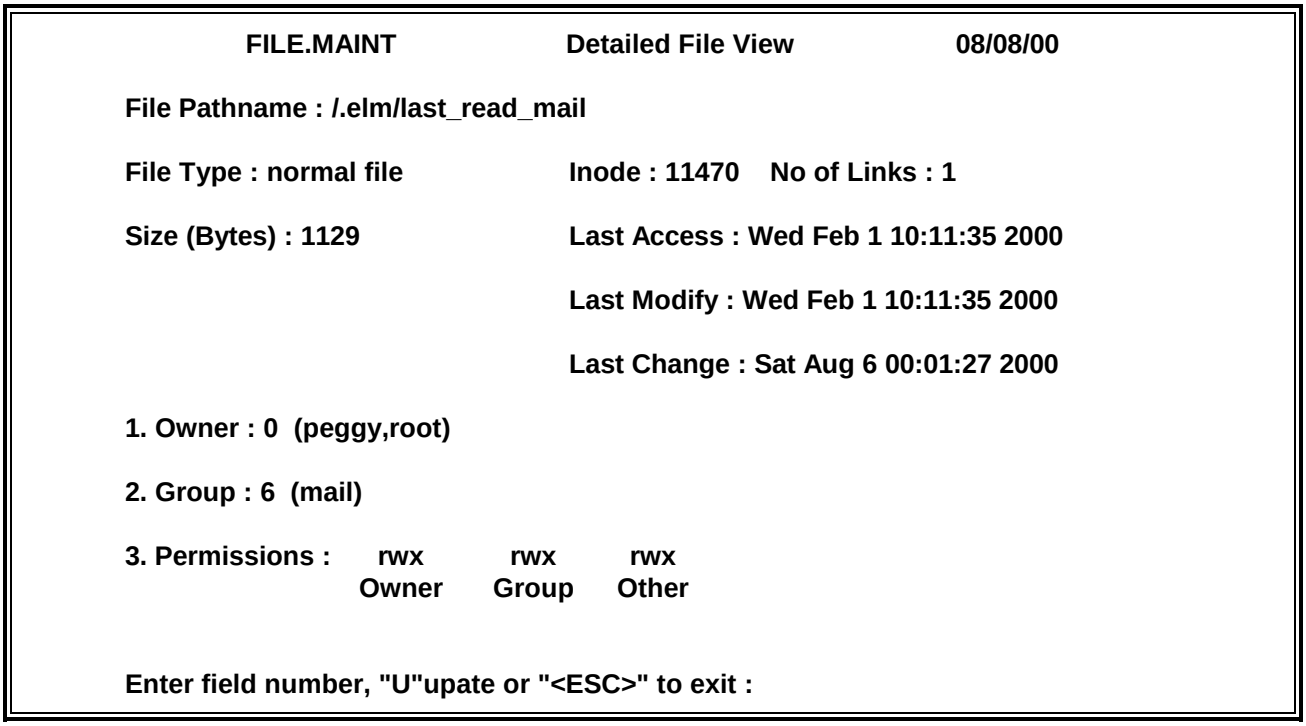

Figure 29 - *This is an example of the "Detailed File View" screen which is accessed through the "General File Utility" by positioning the cursor to the line displaying the file or directory and entering "F".*

SENTRY reads the file information and displays it. Note in our example screen (left top three fields) SENTRY displays the full pathname, the type of file, and the number of bytes used by the file. The possible file types are socket, symbolic link, normal, block mode special, directory, character mode special, and pipe. If the file is not a standard UNIX type SENTRY will report it as "Unknown File Type".

In the right top half of the screen SENTRY displays the I-node number and the number of links plus three date/time stamps. The following paragraphs are quoted from UNIX documentation for these three dates. Check YOUR system documentation for possible differences.

Last Access: Time when file data was last read or modified. Changed by the following system calls: mknod, utimes, read and write. For reasons of efficiency, this value is not set when a directory is searched, although this would be more logical.

Last Modify: Time when data was last modified. It is not set by changes of owner, group, link, count, or mode. Changed by the following system calls: mknod, utimes, write.

Last Change: Time when file status was last changed. It is set both by writing and changing the I-node. Changed by the following system calls: chmod, chown, link, mknod, rename, unlink, utimes, write.

In the lower half of the screen the file owner, group and permissions are displayed. You may use this screen to modify any of these three fields.

1. **Owner** - SENTRY displays the UID of the file owner plus the user ID (may be more than one) for the displayed UID. To change the owner, enter "**1**" followed by <RETURN>. You will be prompted "**Enter the user to be the file owner**". You may choose from a "pick" list by entering "@".

2. **Group** - SENTRY displays the GID of the group as well as the name of the group in parentheses. To change the group, enter "**2**" followed by <RETURN>. You will be prompted "Enter the group for the file". You may choose from a list by entering "@".

3. **Permissions** - SENTRY displays the permissions for Owner, Group and Other. Only valid UNIX permissions are allowed.

r - read permission
w - write permission
x - execute permission

The cursor will be positioned at the owner's set of permissions. Enter the new set of characters you wish to assign to this owner. For example, to give the owner read and write permissions enter "**rw**". To deny all permissions enter "**---**". If you do not want to change the owner's permissions simply enter <RETURN>. SENTRY will position the cursor at the Group permissions field. Make any changes you would like then <RETURN>. SENTRY will position the cursor at the Other permissions field. You may enter your changes or <RETURN> to leave this field.

Enter field number, "U"pdate or <ESC> to exit: - At this prompt enter the number to the left of the field you wish to change (1-3). After making your modifications enter "**U**" to update your changes. Enter <ESC> to leave this screen without making any changes.

If you are changing a directory you will be prompted:

Do you want to update ALL files within this DIRECTORY also?

If you answer "**Y**", all files and directories in that directory will be modified. Please note that files in subdirectories will NOT be modified. If you answer "**N**", only the directory permissions will change. This option is especially useful when the directory is being used as a dynamic database file.

ACLs Maintenance

Access Control Lists (ACLs) are an extension the standard UNIX file permissions. If you have attempted to provide database protection through the use of UNIX file permissions you will have experienced the limitation that each file may have only one owner and one owning group with all other users receiving what is called the "other" category of access rights.

UNIX provides three "permissions" with regard to a file. These are permission to read, write and execute. Read and write permissions are obvious but permission to execute applies to UNIX scripts and programs. Additionally, permission to execute allows the use of a directory in a pathname. For example, if the user wished to "cd" (change directories) to a path such as /data1/subdir/mydirectory. The user could not use this pathname if he did not have "x" rights to subdir.

Access Control Lists augment the standard UNIX file permissions by allowing more than one "owner" and more than one "owning group". With ACLs you can create a list of users and a list of groups in addition to the owner and the owning group (i.e. UID and GID) for each file and directory. Each user and each group is assigned file permissions to allow or deny read, write and execute privileges. ACLs are unique to the file for which they were created. There are not defaults (as there were with ACL implementation on the Prime).

Sentry provides a data entry screen to allow you to create and modify ACLs. To access this data entry screen, invoke the second selection from the Main Menu, "2. Database Maintenance Menu". For the Database Maintenance Menu select number four "4. File System". Navigate to the desired file and use "**FD**" (file detail) to display the existing permissions for that file.

```
                ACL.MAINT          ACL Maintenance          08/14/00

    File Pathname     : /users/sentry/VOC

    1. Owner          : 0  (fastcs,root)
    2. Owning Group   : 3  (sys)
    3. Permissions    : rwx   rwx   ---

============================================================
          4.  Additional Users        5.  Rights
          01) 900 (fred)              ALL
          02) 111 (jeff)              ALL

============================================================
          6.  Additional Groups       7.  Rights
          01) 20 (users)              ALL

Enter field number, "F"ile to save changes or "<ESC>" to exit :
```

This is an example of the "ACL Maintenance Screen". Not all UNIX systems support ACLs. Additionally, you may elect not to use them. If your copy of SENTRY displays this screen you may create and change ACLs with this program.

When this screen is displayed, the pathname of the selected file will appear in the first data field "File pathname". In our example the pathname is "/usr/sentry/VOC". You cannot modify this pathname in this screen. To change pathnames return to the previous screen and navigate to the desired file pathname.

The first field "1. Owner" displays the UID (the number) and the name associated with that UID which is commonly called the "user ID or login ID". If no name is displayed there is no "login ID" in the UNIX password file which corresponds to that UID. This situation could be caused by deleting the user ID from the password file after the user created the file or changed the ownership. Another possibility is that the file was created on another computer and the ownership was never changed.

In our example the file owner is UID 0 (zero). In parentheses there are two user names, "fastcs and root". Normally there is only one name associated with a UID but when there is more than one, such as this case, Sentry will display both.

To change the owner of this file enter the field number (which is located to the left of the field label) "**1**" followed by <ENTER>. Sentry will then prompt you at the bottom of the screen "Enter user to be the file owner." You may enter the UID number or the user name or for a list of all users you may enter the "**@**" cross reference symbol. A listing of all users will be displayed. You may select the desired name by the associated number of simply <ENTER> to return to this screen and type the UID number or user name. You may not enter a name or UID which does not exist. To create a new user enter the Maintenance Menu, User Profiles.

The next field is "2. Owning Group" or GID. All members of this group receive the same privileges indicated in the Permissions field, item # 3, middle set.

In our example the "owning group" is "sys" which has a GID of "3". If no name associated with "3" it would indicate that no name existed in the /etc/group file corresponding to the GID of "3". The circumstances which might create this situation are the same as those described for the missing user ID described previously.

To change the owning group of this file enter the field number (which is located to the left of the field label) "**2**" followed by <ENTER>. Sentry will then prompt you at the bottom of the screen "Enter owning group for the file." You may enter the GID number or the group name or for a list of all groups you may enter the "**@**" cross reference symbol. A listing of all groups will be displayed. You may select the desired name by the associated number of simply <ENTER> to return to this screen and type the GID number or group name. You may not enter a group name or GID which does not exist. To create a new group enter the Maintenance Menu, Groups.

To add members to a group use the Maintenance Menu, User Profiles and access the User you wish to add to a group. Field 9 "Groups" allows you to enter the group name. This may not seem very intuitive to you because you are logically adding the group name to the user profile. The Groups program allows only the creation of the group name and the GID for the group. Users must be added via the User Profiles program.

The next field "3. Permissions" consists of three sets of three permissions. In our example they are "rwx rwx ---". The first three, left most characters are the rights assigned to the Owner. The second set of characters are rights assigned to the Owning Group and the third set "---" are the rights assigned to every one else, generally called "other". In our example, the three dashes indicate that "other" has no privileges to read, write or execute. Because the owner and the members of the owning group have all three privileges no other users would be allowed access to the file.

To change any of the 9 characters associated with the file permissions enter the field number "**3**". The cursor will be positioned in the left most set of characters for the Owner. Simply type over the current parameters to change or <ENTER> to move to the Owning Group field. Press <ENTER> to advance to the Other field of permissions. Enter <ESC> to leave the screen without making changes. No changes are made unless the changes are "filed" via the modifications prompt by entering "**F**" to save the changes.

Field # 4 Additional Users allows you to add more users and permissions to the file thus the name "access control list". In our example we have added the user "fred" and given him ALL rights which are "rwx". This extends the number of users who can read, write and execute this file (although execute doesn't apply in this case). Fred is not a member of the group "sys" and he is not the users "fastcs" or "root". If he were not added to the list he would fall into the "other" designation and would have no rights (---).

To add, change or delete Additional Users, select # 4 at the "Enter field number…" prompt. To change or delete user "fred" enter the line number to the left of that line. In our example the number is 1. To delete the user press <SPACE> and then <ENTER>. The line and the associated permissions to the right will be removed. To change the user, simply type over the user's name. To add a user, press "**A**" then <ENTER>. You will be prompted to enter the user's name or UID.

To change the permissions for a user enter #5 at the "Enter field number…" prompt then the line number associated with the rights you wish to change. You will be prompted to "Enter the access rights for the user." Valid entries are ALL, r, w, x and -. The default is ALL.

Add, change and delete Additional Groups in the same manner as Additional Users.

To save your changes use "**F**" at the "Enter field number…" prompt. When you enter "**F**" or <ESC>. This screen will be closed and the previous screen will be displayed.

More File Manager Views

Another feature available through the file manager screen is the ability to view the rights for a particular user on any directory or file. Enter "**VU**" (view user). SENTRY will prompt:

Enter the user name or UID to view (@ for X-ref) :

At this prompt enter the name of the user for whom you wish to display permissions for files and directories. The screen will be repainted. On the right side of the screen will be a column of three permissions, next to the name of the file. These are the rights available to this user for each item displayed. SENTRY will evaluate the owner and group to determine if either set of permissions apply to this user. If

the user is not the owner and not a member of the group associated with a file, the permissions displayed for the user will be that of "other". The benefit of this feature is that you may browse through your file system, viewing access rights without having to know if a user is in a particular group or not. This saves time!

```
        FILE.MANAGER          General File Utility          14:34:37 18 AUG 2000

   Path : /                                                          (32 entries.)
          Access shown for user bee (201)
   top...
   -->    drwx------      root        mail        ---     .elm
          -r--r--r--      bin         bin         r--     .profile
          -r--r--r--      bin         bin         r--     .profile.orig
          -rw-------      root        sys         ---     .rhosts
          -rw-rw-rw-      root        sys         rw-     .sh_history
          -rw-rw-rw-      root        sys         rw-     .ustk_root
          -r--r--r--      root        sys         r--     .uvhome
          -rw-rw----      root        sys         ---     IDMERROR.console
          -rw-rw----      root        sys         ---     IDMERROR.pty-ttyp3
          drwx------      root        mail        ---     Mail
          -rwxr-xr-x      root        root        r-x     SYSBCKUP
          drwxr-xr-x      root        other       r-x     bin
          drwxr-xr-x      root        other       r-x     dev
          drwxr-xr-x      root        other       r-x     etc
          drwxr-xr-x      root        other       r-x     exl_usr
          -rwxr-xr-x      root        sys         r-x     hp-ux
          -rwx-----x      root        adm         --x     jaf

   Enter the user name or UID to view (@ for X-ref).bee
```

Figure 30 - *This is an example of the permissions in force for the user "bee".*

You may also view the permissions for a specified group. As you can see in the next example. This feature allows you to quickly check permissions with little effort.

```
     FILE.MANAGER          General File Utility          14:39:56 18 AUG 2000

Path : /                                                          (32 entries.)
       Access shown for group piadm (9)
top...
-->    drwx------    root      mail      ---     .elm
       -r--r--r--    bin       bin       r--     .profile
       -r--r--r--    bin       bin       r--     .profile.orig
       -rw-------    root      sys       ---     .rhosts
       -rw-rw-rw-    root      sys       rw-     .sh_history
       -rw-rw-rw-    root      sys       rw-     .ustk_root
       -r--r--r--    root      sys       r--     .uvhome
       -rw-rw----    root      sys       ---     IDMERROR.console
       -rw-rw----    root      sys       ---     IDMERROR.pty-ttyp3
       drwx------    root      mail      ---     Mail
       -rwxr-xr-x    root      root      r-x     SYSBCKUP
       drwxr-xr-x    root      other     r-x     bin
       drwxr-xr-x    root      other     r-x     dev
       drwxr-xr-x    root      other     r-x     etc
       drwxr-xr-x    root      other     r-x     exl_usr
       -rwxr-xr-x    root      sys       r-x     hp-ux
       -rwx-----x    root      adm       --x  jaf

Enter the group name or GID to view (@ for X-ref).piadm
```

Figure 31 - *This is an example of the permissions in force for group "piadm".*

To check group permissions, enter "**VG**" (view group). You will be prompted:

Enter the group name or GID to view (@ for X-ref):

To return to the standard view enter "**VD**" (view default).

2.5 COMMAND MAINTENANCE

This program is used to update protection of VOC items in uniVerse, PI/open and UniData accounts. It is also a convenient means of reviewing the existing protection (created by SENTRY) which may be in effect.

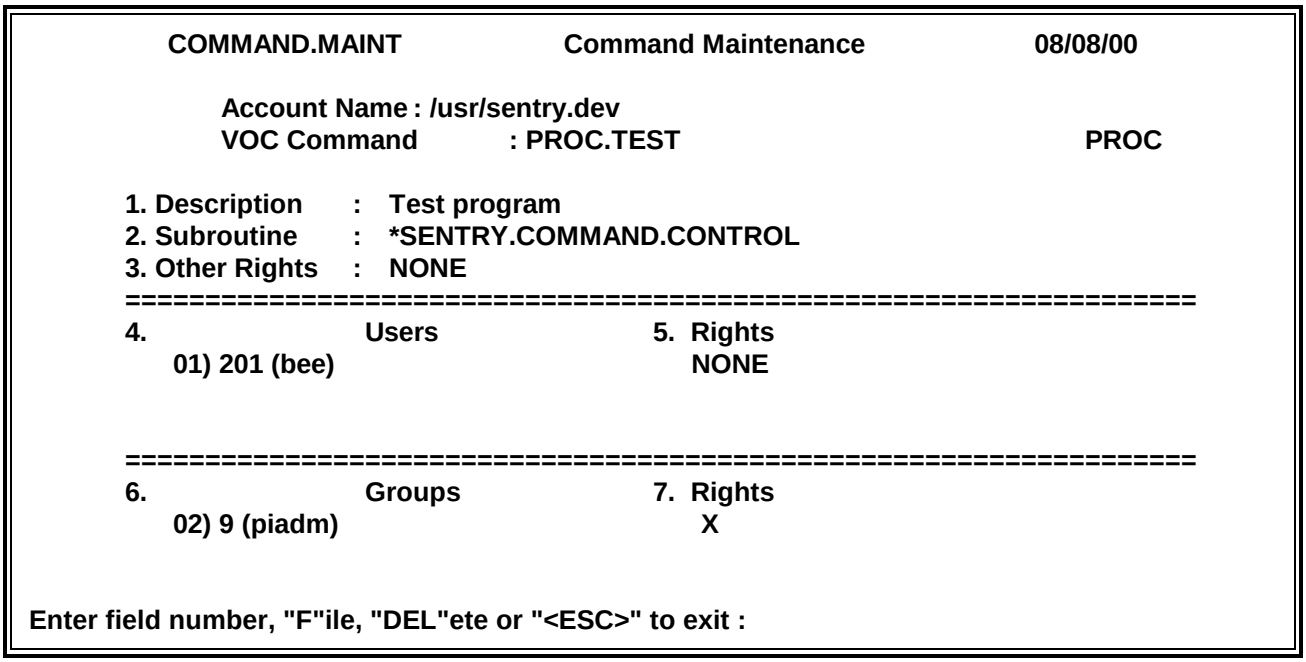

Figure 32 - *This is an example of the "Command Maintenance" data entry screen which is used to set protection on verbs, paragraphs, sentences, PROCs, and menus. Selection 5 on the "Database Maintenance Menu" invokes this program.*

Through the use of permissions, protection for directories and files may be satisfactorily implemented. However, there are *processes* which also need to be protected. It is usually appropriate for users to execute programs in their application software which updates files. This type of update is acceptable and desirable. Updating a file via the editor or deleting records at the database prompt are actions which you would generally prefer users not perform.

SENTRY extends the concept of permissions protection to menus, verbs, PROCs, sentences, and paragraphs. You may allow a user to use DELETE in an application program but disallow that usage at a database prompt. You may protect the editor so that you, or perhaps the MIS group may use it but no other user is allowed to.

To execute this program, select **2. Database Maintenance Menu** from SENTRY's **Main Menu**; then, select **5. Database Commands** from the Database Maintenance Menu. The **Command Maintenance** program will be invoked.
A detailed description of the data entry screen (Figure 33) and prompts follows.

On first entering this program, no data will be displayed on the screen. You will be prompted to enter the name of a database account then the name of the VOC item you wish to protect.

Account Name - Enter the full pathname for the account containing the VOC item you wish to protect. SENTRY will search for the account. If it is not found on the disk, you will be prompted to re-enter the account name. This field is NOT cross referenced.

VOC Command - Having entered the account name, SENTRY will then prompt for the VOC item name. Enter "@" to retrieve a list of currently protected items. If the VOC item is not found, SENTRY will respond with an error message and you will be prompted to reenter the VOC name.

To the far right of this field is a display only field used to report the VOC item type. The valid types are Verbs, Menus, Sentences, PROCs, and Paragraphs. This field may not be deleted or changed through this program. It is read from the first field of the VOC item.

To protect a VOC item, enter the name of the item. You will then be prompted for a description.

1. **Description** - This is a text field used for reporting and documentation. You are encouraged to use a descriptive phrase appropriate for the item.

You may also use the SENTRY "-LIKE" function at this prompt. To protect a VOC item with the same protection as another protected item, enter "-LIKE VOC.item.name". For example, let's assume you have protected "CNAME" the way you plan to protect "DELETE". This is quickly done by entering "-LIKE CNAME" at this prompt. This feature is restricted to copying protection rights from item to item within the same account.

2. **Subroutine** - The name of SENTRY's standard subroutine appears here. This program provides the security screening for your VOC commands. Should you need functionality which is not performed by this subroutine, custom programs may be easily substituted here.

Custom subroutines must conform to the use of the fourth field of the remote VOC items as documented for your database (uniVerse, PI/open or UniData).

3. **Other Rights** - This field is used to define rights for all users who are not included in the specific users and groups you specify for this protection item. The possible choices are:

U - Use at database prompt only

X - Execute from inside a program only
UX - Both use at database prompt and from within a program
ALL - Unlimited use
NONE - No use

The default protection is "**NONE**".

4. **Users** - Enter the user ID for which you wish to define protection rights. The user ID must already exist on the SENTRY database. Type **"@ name"** for a listing of all user IDs having "name" in their user name. Type "@" for a listing of all user IDs on the system.

To remove a user from the protection list, enter the line number associated with that user and then enter a space, followed by <RETURN>. Enter <RETURN> to exit this prompt.

After each user ID is entered, you will be prompted for access rights for that user. The default is "**ALL**".

5. **User Rights** - Enter the access rights for the user. The possible choices are:

U - Use at database prompt only
X - Execute from inside a program only
UX - Both use at database prompt and from within a program
ALL - Unlimited use
NONE - No use

The default protection is "**ALL**".

6. **Groups** - Enter the names of the groups who are allowed to use this VOC item. The group(s) must already exist on the SENTRY database. Enter "@" for a list of all defined groups. To remove a group, enter a space, then <RETURN>. To replace a group simply type over the field to be replaced. After each group is entered, you will be prompted for access rights for that group. The default is "**ALL**". Entering <RETURN> at the rights prompt selects the default protection.

7. **Group Rights** - Enter the access rights for the group. The possible choices are:

U - Use at database prompt only
X - Execute from inside a program only
UX - Both use at database prompt and from within a program
ALL - Unlimited use
NONE - No use

The default protection is "**ALL**".

Enter Field Number, "F"ile, "DEL"ete or <ESC> to Exit: - This is the main modifications prompt for this data entry screen. If you wish to change any of the information, enter the number associated with the entry field, 1 through 7. The cursor will move to the selected input field and allow you to modify the current information. Because Groups, Group Rights, Users, and User Rights are multi-valued fields, you will be asked which line number you wish to change or "**A**" to add a new user or group.

When deleting protection from an item, enter "**DEL**". You will be asked if you are sure you want to delete the entry. A response of "**YES**" will cause the protection on a VOC item to be removed and the item to be restored in the VOC in its standard form.

To save changes you have made, enter "**F**" to file. You will then be asked if you wish to update the disk. Answering "**Y**"es will cause the changes to become effective. After filing or deleting, the screen will be repainted and you will be prompted for another VOC item. If you wish to make changes in another account a second <RETURN> will position you at the Account Name prompt. A <RETURN> at this prompt will cause SENTRY to return to the **Database Maintenance Menu**.

Enter Line # of Groups (or Users) (1-N), "A"dd, "F"orward or "B"ack Page: - When using the Groups or Users windows, you will see the prompt "**Enter line # of Group (or User) (1-n) or (A)dd**". If there are more than five entries in a window, "(F)orward page or (B)ack" page will be appended to this prompt. These commands scroll the window to the next set of four entries or to the previous set.

You may exit this program and cancel all changes not filed by pressing the <ESC> key followed by <RETURN> at any prompt.

2.6 USER ITEM PROTECTION MAINTENANCE

This is a special SENTRY feature which allows you to define SENTRY security objects. These objects may be accessed through subroutine calls to solve unique security problems which may not be met through permissions and VOC item security facilities. For example, you may have a personnel inquiry screen in which you would like to limit the display of the salary field to only a certain group. Through defining a user item which specifies the rights for users and/or groups, you may then add a call to the SENTRY.USER.ITEM.CONTROL subroutine to check the rights of the user before displaying the salary field. By using this technique, individual fields may be protected in data entry/inquiry programs as well as in the database reporting language. You may also call our violations logging subroutine to log program or report use.

```
USER.ITEM.MAINT          User Item Protection Maintenance          08/07/00


        Account Name   : /usr/sentry
        User Item Name : PAYROLL

1. Description :  Protect the Payroll file from LIST
2. Other Rights:  NONE
=================================================================
3.                Users                 4.  Rights
    01) 201 bee                             ALL


=================================================================
5.                Groups                6.  Rights
    01) 9 piadm                             ALL


Enter field number, "F"ile, "DEL"ete or "<ESC>" to exit :
```

Figure 33 - *This is an example of the "User Item Protection Maintenance" screen. Selection 6 on the "Database Maintenance Menu" invokes this program.*

Use of this feature of SENTRY requires some programming effort. Because of the flexibility of the SENTRY routines, this effort is generally very nominal. For an experienced Basic programmer, SENTRY offers a very sophisticated level of security for very little effort. Please refer to the appendices for documentation of the user callable SENTRY subroutines, the arguments, and examples on how to implement their use.

To execute this program, select **2. Database Maintenance Menu** from SENTRY's **Main Menu**; then, select **6. User Defined Items** from the **Database Maintenance Menu**. The **User Item Protection Maintenance** program will be invoked.

A detailed description of the data entry screen (Figure 34) and prompts follows.

On first entering this program, no data will be displayed on the screen. You will be prompted to enter the pathname of a database account then the name of the User Item you wish to create or review.

ACCOUNT NAME - Enter the pathname of the account for the User item you wish to create or review. If the pathname is not found on the disk, you will be prompted to reenter the ACCOUNT NAME. This field is not cross referenced.

Use the pathname to the sentry directory unless you wish to use the same item with different rights for the same user in different accounts. A file called "SENTRY.USER.ITEMS" will be used to store your protection items. The subroutine "SENTRY.USER.ITEM.CONTROL" opens this file via a pointer from the VOC in the account where users will be executing the call.

If you wish to use an account other than SENTRY you must first create a file in the desired account called "**SENTRY.USER.ITEMS**". SENTRY will search this file first (if it exists) for your User Item.

Please refer to appendices for documentation on the subroutine "SENTRY.USER.ITEM.CONTROL".

User Item Name - This is the name you will use in your call to the SENTRY subroutine, "SENTRY.USER.ITEM.CONTROL" to check access rights for the group or user executing the program or report. Using a meaningful, descriptive name is suggested. This field is not validated. Take care that you enter the same name you used or plan to use in your subroutine call.

1. **Description** - This is a text field used for reporting and documentation. Enter a descriptive phrase which identifies the purpose of your user item.

A special SENTRY feature at this prompt is the "-LIKE" function. To protect a User Item "like" an existing User Item, enter the name of the User Item preceded by "-LIKE" (e.g. -LIKE SALARY.FIELD.DISPLAY). This will copy the protection rights on "SALARY.FIELD.DISPLAY" to your new User Item. You may then edit the protection if you wish. This can be a time saver if there are several items which should have similar protection.

2. **Other Rights** - This field is used to define rights for all users who are not included in the specific users and groups you specify for this protection item.

Valid entries are ALL, NONE, and combinations of any of the letters U, R, W, X (Use, Read, Write, Execute).

5. **Groups** - This is a input window used to enter the groups associated with this User Item. Enter the name of a group. The groups entered must already exist in the SENTRY database. A list of groups may be viewed by entering "**@**" at this input prompt. A group may be entered only once. An error message will be displayed should you enter a duplicate name into the list. To remove or replace a group currently in the list, enter the line number associated with that group. Then, enter a space to remove the group. The rights associated with the group will be removed also. If you want to replace the group, simply type the new name over the name to be replaced.

6. **Rights** - Enter the access rights for the group. Rights must be specified for each group named. Rights cannot be undefined. The default is "**ALL**".

The lower half of this screen displays users and their associated permissions.

3. **Users** - Enter the user IDs for User Item protection. The user ID must already exist on the SENTRY database. For a list of all user IDs enter "**@**". You may also enter the name of a user (not the ID) to search for IDs assigned to that person. For example, if there are two or more users named Long, the cross reference on LONG would show all IDs associated with users by that name. To search on a name enter "**@name**" (e.g. @LONG).

To remove an ID from the list, enter the line number associated with that ID; SENTRY will position the cursor at that ID. Enter a space to clear the value. The rights will be removed automatically. To replace the ID simply type over the existing entry.

4. **User Rights** - If you enter a new user ID (which is not in the current list) in this screen, SENTRY will prompt you for the rights. Enter the access rights for the user. Rights must be specified for each user named. Rights cannot be undefined. The default is "**ALL**".

Valid entries are ALL, NONE, and combinations of any of the letters U, R, W, X (Use, Read, Write, Execute).

Enter Field Number, "F"ile, "DEL"ete or <ESC> to Exit: - This is the main modifications prompt for this screen. If you wish to change any of the information for the User Item Protection, enter the number associated with the entry field, 1 through 6. The cursor will move to the selected input field and allow you to modify the current information. Because Groups, Group Rights, Users, and User Rights are multi-valued fields, you will be asked which line number you wish to change or "**A**" to add a new user or group.

When deleting a User Item, enter "**DEL**". You will be asked if you are sure you want to delete the record. A response of "**YES**" will cause the User Item to be deleted from the SENTRY database. A response of "**N**"o causes a return to the modifications prompt.

To save changes you have made to the User Items, enter "**F**" to file. After filing or deleting a User Item, the screen will be repainted and you will be prompted for a User Item name. To enter another Account Name press <RETURN>. Enter <RETURN> at the Account Name prompt to exit this program.

Enter Line # of Groups (or Users) (1-N), "A"dd, "F"orward or "B"ack Page: - When using the Groups or Users windows, you will see the prompt "Enter line # of Groups (or Users) (1-n) or "**A**"dd. If there are more than five entries in a window, "**F**"orward page or "**B**"ack page will be appended to this prompt. These commands scroll the window to the next set of five entries or to the previous set.

You may exit this program and cancel all changes not filed by pressing the <ESC> key followed by <RETURN> at any prompt.

3. INTRODUCING THE REPORTS MENU

The third selection on SENTRY's Main Menu is **3. Reports Menu**. Through this selection you may print reports documenting the system environment, user details, group details, and VOC item protection.

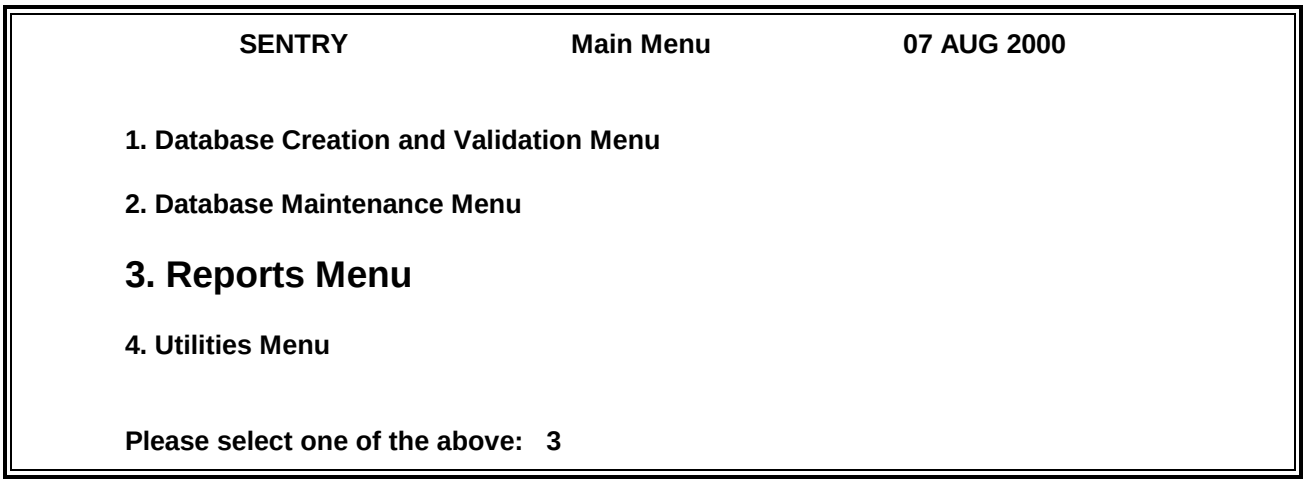

Figure 34 - *Using the third selection on the Main Menu, you may invoke the Reports Menu.*

Through this selection, SENTRY provides extensive reporting capability, integrating user and group details. These reports also provide excellent system documentation of users, groups, and the objects protected through SENTRY Command and User Item protection.

Although system wide reports for users, groups, and permissions are not readily available through UNIX, SENTRY provides reports from several perspectives; showing all users, groups, and their relationships. Additionally, SENTRY's Command Protection entries are also reported.

3.0 REPORTS MENU

This is the third submenu accessible from SENTRY's **Main Menu**. All reports are printed from this menu. You may select any of six reports. Set your default printer parameters BEFORE entering SENTRY.

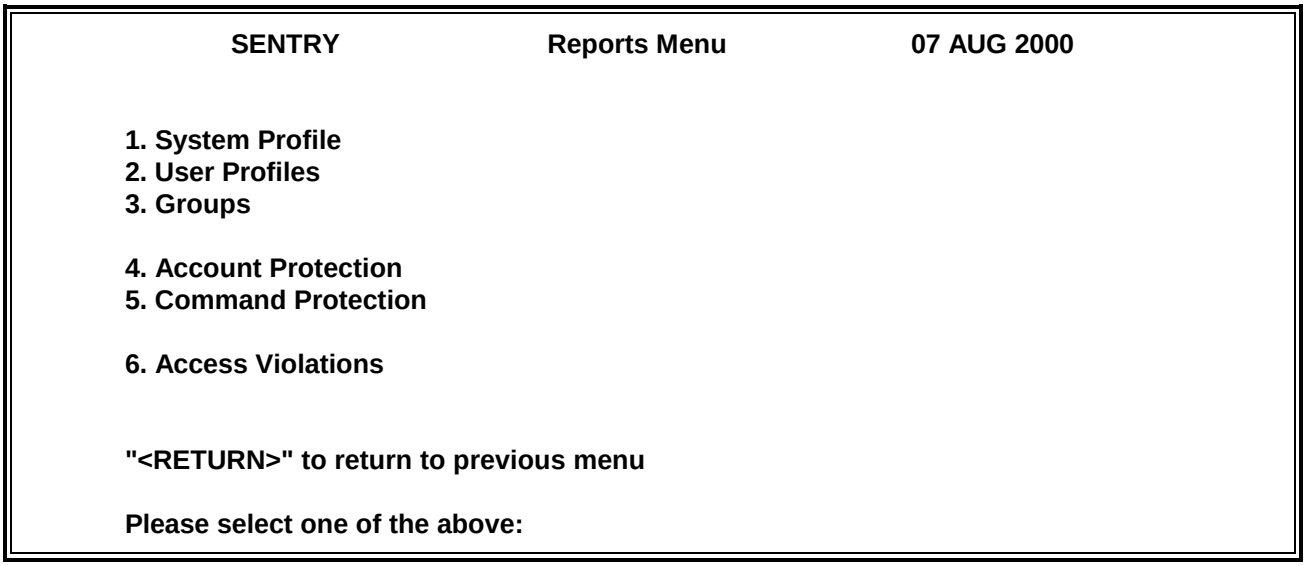

Figure 35 - *All reports are executed through this report menu*

Through these selections you may print comprehensive reports describing your system's users, groups, and their relationships, plus the SENTRY Command Protection reports (selections 4 and 5).

The first selection is **System Profile**. This report displays the system parameters for SENTRY, password attributes, and SENTRY configuration parameters.

Selection two, **Users Profiles**, reports user name, department, telephone, supplementary groups, home pathname, shell, UID and GID.

Selection three, **Groups**, includes details for all groups and users, plus GID and supplementary group status.

Selection four, **Account Protection**, lists the verbs, sentences, paragraphs, PROCs, and menus protected by SENTRY for each account protected.

Selection five **Command Protection**, is the same information as selection four except the report is sorted by the name of the command which is protected. A list of accounts where that command is protected is displayed.

Choosing selection six, **Access Violations**, prints the SENTRY Violations Log. Entries are printed in chronological order. Each record includes date, time, port number, USER ID, pathname and the protected command which was executed creating the violation.

In the following sections, each report is described and an example is provided.

3.1 SYSTEM PROFILE REPORT

Selection one, **System Profile,** generates a report detailing the contents of SENTRY's system limits record. These parameters are used by SENTRY to enforce password, user ID and group name lengths in keeping with the limitations of your version of UNIX and standards set by the System Administrator for your site.

```
SENTRY.SYSTEM.LIMITS.REPORT     SENTRY System Profile as of 13:39:22  08-16-00


Null Passwords Allowed..... No
Minimum Password Length..... 6
Maximum Password Length..... 8
Enable Password Aging ..... Yes
Default Password Life..... 12,2 weeks
Password Format Mask ..... ALPHA,LC
Alpha Order passwd file ..... Yes
Alpha Order group file..... Yes
Case for Users & Groups..... LC
Minimum user ID Length ..... 6
Maximum ID Length..... 8
Maximum Group Length..... 8
Maximum Number for UID ..... 1000
Maximum Number for GID ..... 1000
Default Startup Command ..... /bin/sh
Maximum Command Length ..... 44
Maximum Path Length..... 50
wtmp Valid days old ..... 30 days old
Punct for File Indexing ..... .-_

One record listed.
```

Figure 36 - *This is an example of the System Profile Report which displays various UNIX and SENTRY configuration parameters.*

The following paragraphs describe each field on this report.

Null Passwords Allowed - The default for this field is "**N**". When set to "**N**"o, each user must have a password. If this field is set to "Y"es, a user's password may be blank, so that the user may login without using a password and simply <RETURN> at the password prompt. For good security, passwords should be mandatory. This field controls the data entry program for creating new users. When creating a new user through the SENTRY data entry programs you will be REQUIRED to enter a password for the user or allow SENTRY to generate one for you if this field is set to "**N**". This is not a UNIX parameter. It is used only by SENTRY. This field accepts the values "**Y**" or "**N**".

Minimum Password Length - This is a UNIX defined parameter as well as one used by SENTRY when new users are created. Passwords may be 0 (zero) to "your maximum value" in length. However, most UNIX systems do not recognize more than 8 (eight) characters. More than 8 are ignored. The recommended and default value for this field is 6. Using at least 6 characters decreases the possibility that someone might guess a password or that a "break-in" might occur through computer generated guesses. A six character password is also short enough so that a user is not overly taxed to remember it (without writing it down).

Maximum Password Length - The UNIX limit is normally 8 characters. However, your system may simply ignore any characters after the eighth one. The default and recommended value for this field is 8. This field accepts only integer values 0 - 16. The maximum value must be equal to or greater than the minimum password length value.

Enable Password Aging - This is a SENTRY value used by the program through which you create new users. Some versions of UNIX support password aging. On these systems, the System Administrator can set a minimum number of weeks before a user is allowed to change his password and a maximum number of weeks after which the user is forced to change his password. This functionality may also allow the System Administrator to determine if a user is allowed to change his own password or whether only the System Administrator is allowed to change it. When this field is set to "Y"es, the program for creating new users will prompt for a "Password Lifetime". The default and recommended value for this field is "Y" if your version of UNIX supports this functionality.

Password Life Default - This field is also used by the program through which you create new users, if password aging is enabled through the previous field. If your version on UNIX supports this functionality you may set a minimum and maximum number of weeks for the password life. The minimum is the number of weeks before which the user CANNOT change his password and the maximum is the number of weeks until the user is FORCED to change his password. The value entered here is used as the default value in the User Profile data entry screen to assist you in creating "normal" users with a consistent set of parameters and to eliminate a few key strokes when creating a new user. You may select "INF" (infinite) which means there are no requirements for changing passwords at the default level. "INF" should be entered if password aging is not enabled in the previous field. You will still be able to set password life parameters in the User Profile screen. You may select 0 to 63 as a maximum and 0 to 63 as a minimum. Enter the maximum and minimum separated by spaces - for example "12,2". To insure that a user MUST change his password the first time he logs in use "0,0" if you wish this to be the default.

Password Format Mask - This field is used by the User Profile data entry screen if you use SENTRY's generate new password option in the password field. If you plan to use this functionality you may select a "mask" of either ALPHA or ALPHANUM which generates either alphabetic or alphanumeric passwords. SENTRY will generate either a string of alphabetic characters such that the password format is alternating consonant/vowel for the length of the string defined by the Minimum Password Length (selection 2 in this screen), or a string of characters beginning with an alphabetic character and containing at least one numeric. If this field is set to ALPHA, only alphabetic characters will be used. If the field is set to ALPHANUM, the generated password will contain at least one

embedded numeric. The default and recommended value is ALPHA which will generate a string of alphabetic characters, the length defined by the Minimum Password Length field. If the minimum length field is 0 or null, a password of 6 characters will be used unless otherwise specified when the "**G**"enerate command is used in the password field of the User Profile data entry screen.

The value in this field may be followed by a comma and either "UC" or "LC" to specify that generated passwords be either upper case or lower case characters.

Many UNIX systems require that passwords meet the following requirements:

1. Each password must have at least six characters. Only the first eight characters are significant.
2. Each password must contain at least two alphabetic characters and at least one numeric or special character.
3. Each password must differ from the user name and from any reverse or circular shift of that name.

However, the System Administrator, (UID = 0) may create or change any password and those passwords created by the superuser do not have to comply with password construction requirements.

passwd File Order - This field is used by the program which creates and modifies users. If the value of this field is "Y"es, the names of the users are alphabetized in the UNIX passwds file. If you wish to maintain the current order of the passwd file this field should be set to "N"o. The default and recommended value is "Y"es. Note, however, that the passwd files should first be arranged to be in alphabetical order if this option is set to "Y"es. That is, setting this option will not rearrange existing users to be ordered.

group File Order - This field is used much the same as the passwd File Order field (above). It is used by the program which creates and modifies groups. If the value of this field is "Y"es, the names of the groups are alphabetized in the UNIX group file. If you wish to maintain the current order of the group file this field should be set to "N"o. The default and recommended value is "Y"es. Note, however, that the group files should first be arranged to be in alphabetical order if this option is set to "Y"es. That is, setting this option will not rearrange existing groups to be ordered.

User & Group Case - This field will contain LC (lower case), UC (upper case or (LIT literal). It is used by the programs which create and modify users and groups. When entering the name of a user or group in the User Profile or Groups screens the case of the name of the user or group will be set to the appropriate one selected by this field regardless of the case used when entering the name. For example, if a user name of TEST is entered in the User Profile screen, the case will be changed to "test" if this field is set to "LC". This parameter is intended to assist System Administrators who wish to be consistent in their usage of case when creating users and groups. If you do not want SENTRY to alter the case for users and groups, set this field to "LIT" (literal). SENTRY will not alter the characters you have entered. The default and recommended value for this field is "LC" (lower case).

Minimum user ID Length - This field contains a number defining the minimum number of characters required for a user ID. A user ID must begin with an alphabetic character, contain no spaces and be unique. This field is used to verify the length of the user ID in the User Profile data entry program. The default and recommended value is 6.

Maximum user ID Length - This field contains a number defining the maximum number of characters allowed for a user ID. Most UNIX systems allow up to 8 alphanumeric characters. This field is used by the User Profile data entry screen to limit the length of user IDs created through SENTRY's data entry screen. The recommended and default value is 8.

Maximum Group Name Length - This value is used by the program to limit the number of characters in group names. Some UNIX systems allow longer than 8 character group names but we recommend that your group names be no longer than 8 characters. The default and recommended value for this field is 8.

Maximum UID Number - This field defines the largest number which may be used as a UID. This maximum is a UNIX parameter. On some UNIX systems this number may be as large as 60,000. However, we recommend using UIDs smaller than 5 digits simply to make them easier to read. The default and recommended value for this field is 1000.

Maximum GID Number - This field defined the largest number which may be used as a GID. This maximum is a UNIX parameter. On some UNIX systems this number may be as large as 60,000. However, we recommend using GIDs smaller than 5 digits simply to make them easier to read. The default and recommended value for this field is 1000.

Default Startup Command - This field contains the command executed at login for the user. It is generally the "shell" command. The User Profile uses this field as a default value for creating a new user. Simply returning past the startup command field will assign this value. The default value for this field is /bin/sh. The recommended value for this field is the "normal" startup command for your average user.

Maximum Command Length - This field is a UNIX parameter and is generally documented in the Administrator's Guide for adding a user ID. The value of this field should be consistent with your version of UNIX. On our system this maximum is set at 44 characters. Obviously a normal path to a UNIX shell (such as /bin/sh) will be much smaller than 44 characters. The default value for this field is 44 characters. The recommended value for this field is your system's maximum value.

Maximum Startup Path Length - This field is a UNIX parameter and is generally documented in the Administrator's Guide for adding a user ID. The value of this field should be consistent with your version of UNIX. On our system this maximum is set at 50 characters. This is the maximum number of characters allowed in the pathname commonly referenced as the "home" directory. It is the directory into which UNIX attaches the user at login. The default value for this field is 50 characters. The recommended value for this field is the maximum number your version of UNIX allows.

wtmp Valid Days Old - SENTRY uses an UNIX accounting file called "wtmp" which contains a log of user logins. The file is used to determine the last login date and time for users. However, the UNIX accounting system which updates "wtmp" can be disabled, causing the file's date to be invalid. SENTRY considers the file to be invalid of no data for the user "root" is found within the last number of days represented by this parameter. The commands to enable system accounting vary by system and may be found in your UNIX documentation. Our default is set to 30 days.

Punct for File Indexing - SENTRY builds B-trees to provide rapid cross referencing into the file system. For example, let's imagine that you are looking for a file called "payroll.something". You can't remember the "something". In the File System screen you may enter "payroll" and SENTRY will search the B-trees for all references to "payroll". A list of pathnames to all files and directories whose name contains the string "payroll" will be displayed. The cross referencing on the word "payroll" is dependent upon the characters defined in this field. Special characters such as "." and "-" or "_" are used in file or directory names to make a compound name more readable. SENTRY's B-trees will use the set of characters defined here to break out the components of a compound name such as "payroll.ledger". This file would be indexed on the word "payroll" and on the word "ledger". Care such be taken in selecting these characters for cross referencing so that they are limited to those which are commonly used. The size of the B-trees increases significantly as the number of characters in this list increases.

3.2 USER PROFILES

The SENTRY User Profile Report displays all parameters in effect for each user registered in your system. Additionally such information as the users name, department and telephone may be added to the system data.

SENTRY.USERS.REPORT SENTRY User Details 12:15:01 08-08-00

User Login ID	uid	GID Name	Supplementary Groups	Login Shell or Command	Home Directory	User Name Department Telephone
======	===	==========	=============	==========	========	==========
adm	4	adm	adm	/bin/sh	/usr/adm	
bee	201	users	users	/bin/sh	/users/fl_sales	Bee Fiore
bin	2	bin	bin	/bin/sh	/bin	
daemon	1	daemon	daemon	/bin/sh	/	
lewis	203	users	users	/bin/sh	/users/fl_data	Lewis Eckhoff
lewis1	203	users		/bin/sh	/users/fast.practice	
lp	9	lp	lp	/bin/sh	/usr/spool/lp	
peggy	0	users	users	/bin/sh	/users/peggy	Peggy Long Office 123 1102
root	0	sys	root other bin users sys adm daemon mail lp piadm	/bin/sh	/	

9 records listed.

Figure 37 - *This is an example of the User Profiles Report which displays the user's ID, UID, GID name, list of supplementary groups, login shell, home directory, name, department, and telephone number.*

In the following paragraphs, we will describe each column of the report.

User Login Id - This the ID which is entered to log into your UNIX system. Most UNIX systems use lower case characters for IDs.

UID - UNIX maintains a relationship between users and files by assigning ownership via the UID, the user's number. To maintain the translation of UIDs to user IDs (used by the file system), the Administrator should take care when creating or changing this relationship.

GID Name - When a user login ID is created, UNIX allows the user to be assigned to a group. Here again, the name of the group is not held in the passwd file, only the group's number or GID. In this report we translate so that the name appears instead of the number.

Supplementary Groups - This may be a multi-valued list of group names in which this user has membership. These are groups "in addition to" the GID to which the user belongs.

Login Shell or Command - When a user logs in, UNIX will execute whatever "startup" command the Administrator specified for that user. This startup command is commonly the pathname to one of the various UNIX shells. In our example we are using /bin/sh, the Bourne shell.

Home Directory - When a user logs into your system, he will be "attached to" a "home" directory. This field defines the directory to be used.

User Name - This is a text field used for documentation and display only. We recommend that user names be entered LAST, FIRST in order to offer greater reporting functionality.

Department - This is another text field used for documentation and display only. We recommend that you consider your reporting needs and use this field for whatever purpose seems of most benefit in your environment.

Telephone - Here again is another text field used for documentation and display only. Telephone numbers may be of importance to the System Administrator. However, if there are other types of data which would be more useful to you, please feel encouraged to enter that data which makes the best use of this field in your environment.

Note that the user "Name", "Department", and "Telephone" data is written into the "GCOS" field of the UNIX passwd file. This data is displayed by the UNIX "finger" command.

This report was created by the reporting language in your database system. The paragraph which generated this report is VOCLIB/SENTRY.USERS.REPORT. The data file used is SENTRY.USERS. In addition to the data displayed here you may create a report which displays the last login date and time. The name of the dictionary item is LAST.LOGIN. It is not included on this report because of its ever changing values. Additionally, a subroutine call is executed to "look-up" the last date/time the user logged in. Given a large number of users, the amount of time to "look up" this data could excessive.

If you need to modify the file dictionary records to produce custom reports, we recommend that you create new records rather than modifying the provided records. This will reduce the impact of upgrades on your work.

3.3 GROUPS REPORT

The SENTRY Groups Report displays, in a very concise format, all data related to groups on your system. Along with the name and description of each group are all user IDs associated with the group. The user's relationship with each group (GID or supplementary) is reported also.

SENTRY.GROUPS.REPORT **SENTRY Group Details** **12:16:01 08-08-00**

Group Name	GID	Supplementary for Users	GID for Users	Description
adm	4	adm root	adm	HP system group
bin	2	bin root	bin	System group
daemon	5	daemon root	daemon	Phantom group
lp	7	lp root	lp	Printer group
users	20	bee lewis peggy root	bee lewis lewis1 peggy	Application group

5 records listed.

Figure 38 - *This is an example of the Groups Report.*

The following paragraphs describe the fields displayed on the example report.

Group Name - The leftmost column on this report displays the name of the group. These group names are defined in the UNIX group file. The list is presented in alphabetical order.

GID - This is the number associated with the group name as defined in the group file.

Supplementary for Users - This field reports a multi-valued alphabetical list of users who have this group as a supplementary group.

GID for Users - The users listed in this field are assigned this group in the passwd file. It is commonly referred to as their GID group or primary group.

Description - This is a free form text field to be used by the System Administrator to document the usage of groups on your UNIX system.

This report is produced by the database reporting language on your system. The paragraph can be found in VOCLIB/SENTRY.GROUPS.REPORT. The database file is SENTRY.GROUPS.

3.4 ACCOUNT PROTECTION REPORT

This is a report of all protected commands on your system. It is sorted by account such that there is one page per account printed. Note that the account pathname appears in the title of the report.

SENTRY.ACCOUNTS.REPORT Commands Protected in Account /users/jeff as of 12:16:19 08-08-00

Commands: Verbs, Sent, Menu, PA or PQ	Type	Description	Group Name & Rights	User Name & Rights	Other Rights
DELETE	V	Verb to DELETE records from a FILE	users : U adm : ALL piadm : ALL	peggy : ALL root : ALL lewis : U lewis1 : U	NONE
ED	V	Verb to invoke the Pi/open editor	users : U adm : ALL piadm : ALL	peggy : ALL root : ALL lewis : U lewis1 : U	NONE
MODIFY	V	Verb to invoke the cursor control-dependent data entry processor	piadm : ALL	peggy : ALL root : ALL	NONE

3 records listed.

Figure 39 - *This is an example of the Account Protection Report. Each account is listed on a separate page. All protected commands for an account are presented in alphabetical order.*

The following paragraphs describe the fields presented on the report and shown in Figure 39.

Commands - This is the name of the command as it appears in the VOC of the account. It may be the name of a verb, sentence, paragraph, PROC, or menu.

Type - This field indicates if the command is a (V)erb, (S)entence, (P)aragraph, (PQ) PROC, or (M)enu. Note that the examples presented in our report are verbs and one PROC.

Description - The description field is used for documentation and may be entered through the Database Maintenance program for Database Commands.

Group Name & Rights - This field displays the names of groups (if any) used to define the access to this command and the rights given to these groups. The names of the groups MUST be registered UNIX group names. This field may be multi-valued.

User Name & Rights - Displayed in this field is a list of all users who have rights to this command. Their rights are listed to the right of the user ID. This may be a multi-valued field.

Other Rights - Should a user NOT be mentioned by name and NOT be a member of one of the groups assigned rights to this command, the user's rights default to those displayed in this field. NONE is the system default but may be changed by the System Administrator in the data entry screen for Command Maintenance.

This report is written in the database reporting language used by your system. The paragraph which generates this report is VOCLIB/SENTRY.ACCOUNTS.REPORT. The database file is SENTRY.COMMANDS.

3.5 COMMAND PROTECTION REPORT

The SENTRY Command Protection Report presents an alphabetical listing of all commands protected through SENTRY's Database Commands program.

SENTRY.COMMANDS.REPORT Command Protection as of 12:16:37 08-08-00

Commands: Verbs, Sent, Menu, PA or PQ	Type	Description	Pathname	Group Name & Rights	User Name & Rights	Other Rights
DELETE	V	Verb to DELETE records from a FILE	/usr/sentry.practice	users : U adm : ALL piadm : ALL	peggy : ALL root : ALL lewis : U lewis1 : U	NONE
**						
ED	V	Verb to invoke the Pi/open editor	/usr/sentry.practice	users : U adm : ALL piadm : ALL	peggy : ALL root : ALL lewis : U lewis1 : U	NONE
**						
MODIFY	V	Verb to invoke the cursor control-dependent data entry processor	/usr/sentry.practice	piadm : ALL	peggy : ALL root : ALL	NONE
**						

3 records listed.

Figure 40 - *This is an example of the Command Protection Report displaying protected commands.*

The following paragraphs describe the seven fields displayed on this report. Please refer to the sample report for an example of each field.

Commands - This is the name of the command as it appears in the VOC of the account. It may be the name of a verb, sentence, paragraph, PROC, or menu.

Type - This field indicates if the command is a (V)erb, (S)entence, (P)aragraph, (PQ) PROC, or (M)enu. Note that the examples presented in our report are verbs.

Description - The description field is used for documentation and may be entered through the **Database Maintenance** program for **Database** Commands.

Pathname - This is the pathname of the accounts in which the Command Protection is used.

Group Name & Rights - This field displays the names of groups (if any) used to define the access to this command and the rights given to these groups. The names of the groups MUST be registered UNIX group names. This field may be multi-valued.

User Name & Rights - Displayed in this field is a list of all users who have rights to this command. Their rights are listed to the right of the user ID. This may be a multi-valued field.

Other Rights - Should a user NOT be mentioned by name and NOT be a member of one of the groups assigned rights to this command, the user's rights default to those displayed in this field. NONE is the system default but may be changed by the System Administrator in the data entry screen for Command Maintenance.

This report is written in the database reporting language used by your system. The paragraph which generates this report is sentry/VOCLIB/SENTRY.COMMANDS.REPORT. The database file is SENTRY.COMMANDS.

There are no prompts for this report.

3.6 ACCESS VIOLATIONS REPORT

The SENTRY Access Violations Report is an audit report of violations logged by SENTRY for Database Commands and for User Defined Items. Each attempt to use a restricted command by an unauthorized user is reported here.

SENTRY.VIOLATION.REPORT **SENTRY Access Violations** **12:16:56 08-08-00**

Key#	Date	Time	tty	Login Id	Pathname	Violation Item
V27	08/04/95	01:55PM	/dev/pty/ttyp2	peggy	/usr/sentry.dev	Command Executed - DELETE VOC RTP3

One record listed.

Figure 41 - *This is a sample report of the SENTRY Violations Log. Each attempt to use a restricted command by an unauthorized user is reported.*

Each attempt to use a restricted command is logged in SENTRY's violation log and may also be displayed at the system console if desired. The report of security violations show the date and time of occurrence, the port, the user ID, the specific account where the violation occurred and the full command which was attempted. Applications using SENTRY's User Defined Items may also create violation records which will contain the user item being protected and a user specified comment, in addition to the standard information. The System Administrator should print and review the Violations Report frequently in order to monitor user actions. SENTRY allows the violation log to be purged selectively or in whole after the report has been printed.

The following paragraphs describe the fields on this report.

Key# - This is the record ID generated by SENTRY as a key to that specific violation entry.

Date/Time - This is the date and time on which the violation occurred.

tty - This field is the device to which the user was connected when the violation occurred.

Login ID - This is the User ID in effect when the violation occurred.

Pathname - This is the pathname to the account containing the protected VOC item which was used by an unauthorized user.

Violation Item - This field provides documentation on which Command was used. Messages beginning with "Command Executed" indicate that the command was used within a paragraph, sentence or program. Messages beginning with "PERFORM Command" indicate that use of the Protected Command occurred at the database prompt.

In addition to the standard SENTRY reports, we encourage you to use the database reporting language to create custom reports or to perform inquiries (e.g. LIST SENTRY.VIOLATIONS WITH DATE AFTER "01/01/95" AND WITH COMMAND LIKE "...PAYROLL..." to show all violations related to the PAYROLL file). Because all of the data is stored in an integrated database, there is great flexibility and power available for reporting and research.

4. INTRODUCING THE UTILITIES MENU

The Utilities Menu is executed through selection four on the SENTRY **Main Menu**. The programs provided in this selection are ancillary to the job of providing sound, well documented system security. These utility programs offer conveniences such as duplicating the protection from one account to another, purging the Violations Log, and generating new passwords.

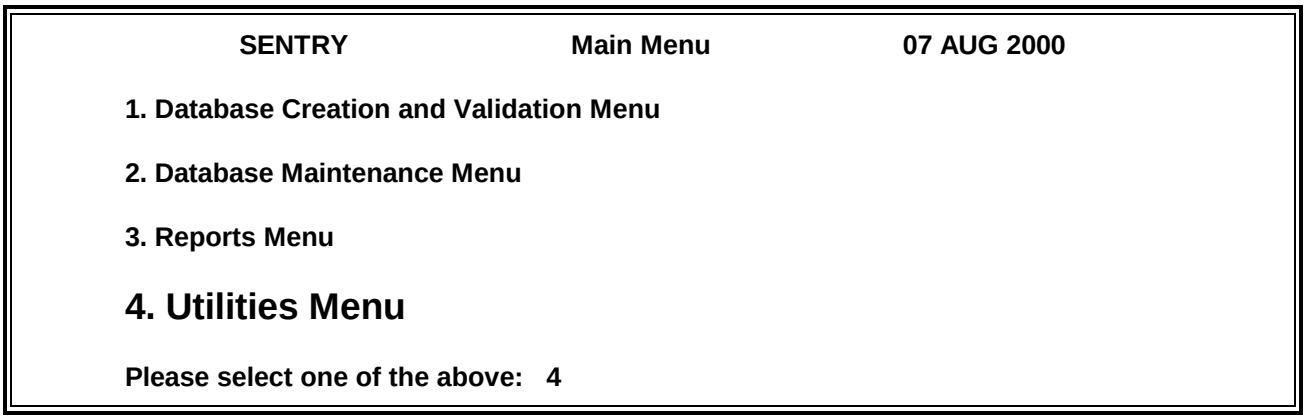

Figure 42 - *Using the fourth selection on the Main Menu, you may invoke the Utilities Menu.*

Through the five utility programs offered in the **Utilities Menu** you may make a number of "global" changes with little effort. These programs are provided as a convenience for the System Administrator who frequently needs to perform certain tasks on a system-wide basis.

One program provides you with the convenience of duplicating all of the Database Command security from one account to another, saving data entry time.

You may use our utility program to purge the Violations Log on a selective basis. Our password generation program will generate new passwords for all users using the standard specified in the System Profile for length and format. A special report is available to assist the System Administrator in notifying users of the changes.

Should SENTRY's cross reference files become damaged, you can easily rebuild them through this menu. Additionally, we have provided a utility to "re-install" SENTRY's command protection on an account.

4.0 UTILITIES MENU

This menu provides access to five utility programs designed to save the System Administrator data entry effort and time in performing global tasks such as generating and protecting an account "like" another account, purging the Violations Log on a selective basis, and changing passwords in SENTRY's database.

```
SENTRY              Utilities Menu              16 AUG 2000

    1. Protect a Database Account Like an Account Already Protected

    2. Purge the Violation Log

    3. Generate New Passwords for Users

    4. Rebuild SENTRY Cross Reference Files

    5. Update Protected Commands to Account VOC Files.


    "<RETURN>" to return to previous menu

    Please select one of the above:
```

Figure 43 - *This is the Utilities Menu which offers access to five utility programs for performing global changes quickly.*

Each menu selection is described briefly in the following paragraphs for quick reference. Greater details are provided in the following sections for each program.

Selection one, **Protect a Database Account Like an Account Already Protected**, is a time saving utility if you wish to copy the Command Protection of one account to another. Frequently this is the case. A great deal of data entry may be skipped through the use of this program.

Selection two, **Purge the Violations Log**, allows you to delete entries from the Violations Log on a selective basis, by user ID, date, port, etc.

Selection three, **Generate New Passwords for Users**, will generate and change all passwords on the system if you would like. For the System Administrator who wishes to change all passwords frequently, this is a real time saver. A report is also generated which may be used to notify each user of his new password.

Selection four, **Rebuild SENTRY Cross Reference Files**. Sentry maintains a number of traditional inverted lists which are used for cross referencing. When you use the "@" function you are accessing one of these lists. Should you encounter a list where an item appears as "NOT FOUND" or isn't shown when it should be, you should rebuild these lists through this program.

Selection five, **Update Protected Commands to Account VOC Files**. It is possible that through the use of the editor or upgrading to a new release that Sentry's Command Protection could be overwritten. To re-install the Command Protection into the VOC of an account, use this program.

In the following pages, complete descriptions of each program are provided.

4.1 VOC PROTECTION SETUP

This program provides the convenience of being able to copy the protection set on VOC items in one account to a second account. For a system with numerous accounts needing the same or similar protection, this program provides an automated process of creating VOC protection without the necessity of entering each item in a number of accounts.

To invoke this program enter **4, Utilities Menu**, from the SENTRY Main Menu; then, select **1, Protect a Database Account Like an Account Already Protected**.

On entering this program, you will be prompted:

ACCOUNT CONTAINING PROTECTION:

Enter the absolute pathname of the account from which you wish to copy the VOC item protection. This account must be a valid account using SENTRY's VOC protection.

ACCOUNT TO BE PROTECTED:

This is the second prompt. Enter the absolute pathname of a valid database account which you want to have identical VOC protection to the first account.. For convenience, a list of the protected verbs which will be copied may be reviewed by entering "@" at this prompt. This is a display only. No selection or modifications may be performed to this list. Entering <RETURN> will return you to the previous prompt.

ENTER 'OK' TO BEGIN PROCESSING

Entering "OK" at this prompt starts the copying process. If SENTRY encounters the same VOC item name already protected in the target VOC, you will be asked if you wish to overwrite it. If you respond with "Y" it will be overwritten, and a response of "N" will cause the item to be skipped.

4.2 PUGING THE VIOLATIONS LOG

This program provides a convenient method of selectively purging the SENTRY Violations Log. You may purge by record key, dates, ports, USER ID, or account name. To invoke this program enter **4, Utilities Menu**, from the SENTRY **Main Menu**; then select **3, Purge the Violations Log**.

On entering this program, you will be prompted:

1. Violation Keys
2. Beginning Date
3. Ending Date
4. Computer Port
5. user IDs
6. Account Pathname

1. **VIOLATION KEYS** - To select specific Violations records to be purged, enter the exact key (record ID) for field **1, Violation Keys**. Separate multiple keys with spaces. You may not use this selection criteria in conjunction with any other criteria. Enter <RETURN> to proceed to prompt 2 if you are not using this selection.

2. **BEGINNING DATE** - This selection allows you to set a beginning date from which to select entries. This date must be earlier than the ending date. The format is MM/DD/YY.

3. **ENDING DATE** - This date is the last date for which records should be purged. Using BEGINNING DATE and ENDING DATE you may specify a range to purge from one date to another date. This date must be after the BEGINNING DATE. The format is MM/DD/YY.

4. **COMPUTER PORTS** - If you would like to purge the violations which occurred on specific ports, enter the ports separated by spaces.

5. **USER IDS** - You may purge the violation entries for specific User IDs by entering the IDs separated by spaces.

6. **ACCOUNT PATHNAME** - To purge by specific pathnames, enter the absolute pathname in which the violations occurred.

ENTER FIELD NUMBER OR "OK" TO BEGIN THE PURGE PROCESS. - You may change any entry by referencing the field number associated with the prompt. When you are ready to begin the purge enter "**OK**". If you have entered NO selection criteria, all violations records will be purged.

This program is constructing a query sentence to SELECT the items to be purged. When entering your criteria, think of it as though you were completing the phrase "WITH field.name EQ (or LT, GT)" to the items you enter.

4.3 PASSWORD CREATION

This program provides a convenient utility to assist you in creating new passwords for a number of users. You may select users to be changed based upon IDs, department, project, group, and user name. Through this utility you may change all passwords on a regular basis if needed. To invoke this program enter **4, Utilities Menu**, from the SENTRY **Main Menu**; then, select **3, Password Creation**.

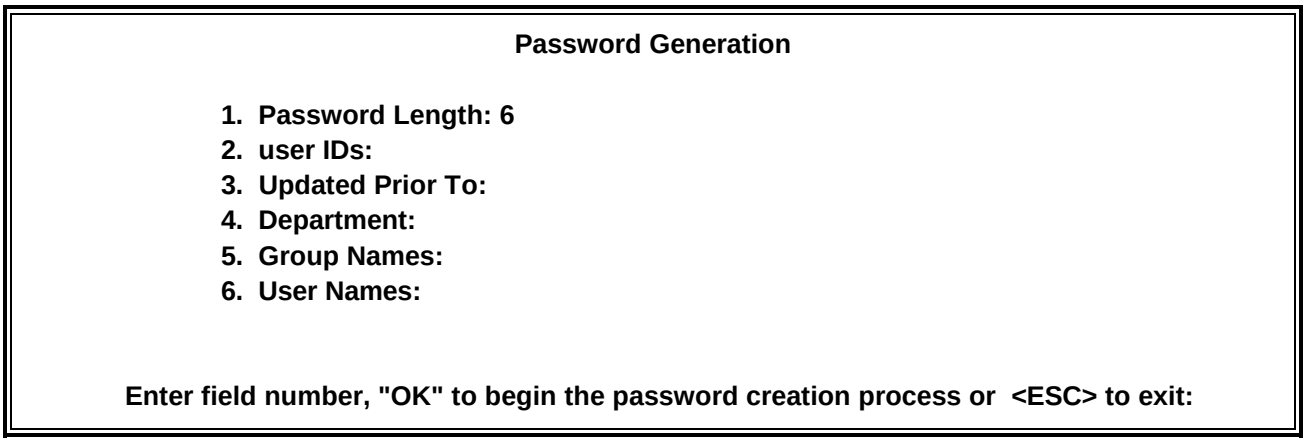

Figure 44 - *This is the Password Generation data entry screen.*

You may select a list of users for whom you wish to change passwords by any of the six criteria displayed. User IDs, department, groups, and user names may be used. Separate multiple names with spaces. There is no validation for existence of your selection criteria.

1. **Password Length** - The generated passwords will be no less than the minimum number of characters specified in the System Profile and at least four characters. If the number specified here is larger than that in the system profile, it will be used instead. Each generated password will begin with a consonant and alternate with a vowel, consonant, vowel pattern to fill the required length. This technique produces pronounceable words which aids in remembering them. User should be reminded NOT to write down their passwords. Therefore, it is important that the password to easy to remember.

This program will conform to the ALPHA or ALPHANUM mask set in the System Profile as well as the case set for generated passwords.

2. **user IDs** - Enter a list of user IDs separated by spaces for which you would like to generate new passwords. The new passwords are written into the SENTRY.USERS file in an encrypted format. The System Administrator may access these passwords through the Sentry Users Maintenance screen.

3. **Updated Prior To** - Sentry writes a time/date stamp to the database when the password is modified. You may select users for password change by this date field. Enter the date in the format

MM/DD/YY. Sentry will select all users whose password update date is earlier than this date. If there is no date in this field, the record will not be selected.

4. **Department** - If you have entered data into the "department" field of the SENTRY.USERS file, you may use this field in your selection criteria for generating new passwords. Enter the department names separated by spaces. There is no validation on this field. Please check your entries against the Sentry Users Report to insure that your selection criteria are spelled correctly.

5. **Groups** - You may select users by their group membership for password change. Enter the group names separated by spaces. Be sure to use the appropriate case when entering the names. This program does not validate this entry against the SENTRY.GROUPS file.

6. **User Names** - Sentry maintains a cross reference list by the user's name as entered into the Sentry Users data entry program. If you have used this field in your data entry, you may use it in this program to select by user name instead of by user ID (selection criteria 2). Enter the names separated by spaces. This program does not validate this entry against the Users file. Take care that you enter the case and spelling just as it appears in the SENTRY.USERS file.

"Enter field number, "OK" to begin ..." - To enter your selection criteria, enter the field number which appears to the left of the item. When more than one entry is desired, such as several departments, use spaces to separate the entries. No validation is performed on your selection criteria.

The passwords will be encrypted and written to the SENTRY database. This program produces the same style passwords as the password generator in the **User Profiles** program. The value of this utility is that a number of passwords may be changed quickly.

Do you wish to update passwords immediately? The prompt asks if you want the new passwords written to the UNIX passwd file as they are generated, or written to a work file for later update. If you update immediately, the users affected will be unable to login until notified of their new passwords. If you choose "N", the passwords will be stored in a work file. When you enter SENTRY, you have the option to place the changes stored in the work file into effect. Alternatively, you may run the SENTRY.UPDATE.USERS command.

You will next be prompted for whether you wish to print a report of user IDs and their new passwords. Answer "Y" to print. SENTRY prints to the default printer. If you wish to direct your output to another printer be sure to set your printer destination BEFORE entering SENTRY.

Enter "OK" when you are ready to begin generating new passwords.

A report is produced which includes the User ID and the new password. The format of the report is such that it can be cut into mailable strips with which to notify users of their new passwords. If you have entered the user's name and department in the SENTRY Users screen, the report will use this information also.

4.4 REBUILD CROSS REFERENCE FILES

SENTRY maintains a number of traditional inverted lists which are used for cross referencing. When you use the "@" function you are accessing one of these lists. Should you encounter a list where an item appears as "NOT FOUND" or an item doesn't appear which should, you should rebuild these lists through this program. This message indicates that a reference to an item exists but the item itself is missing. When a process is interrupted through a program error, machine failure or "killing" the process, the result may be that the cross reference files are not updated properly. Therefore, we have provided this "cleanup" program just in case one of these events should occur.

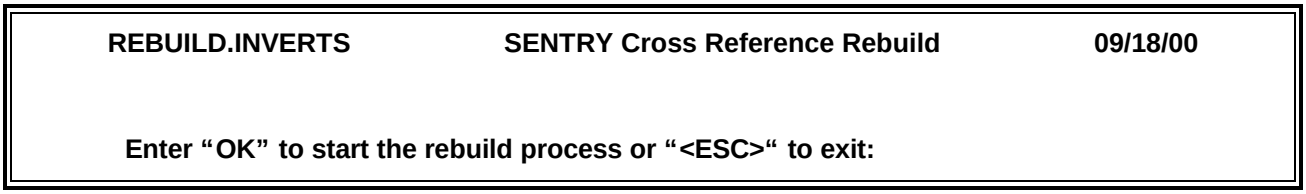

Figure 45 - *This is an example of the "Cross Reference Rebuild" screen.*

Enter "**OK**" when you wish to start the rebuild process. Enter <ESC> to exit this screen.

4.5 UPDATE PROTECTED COMMANDS

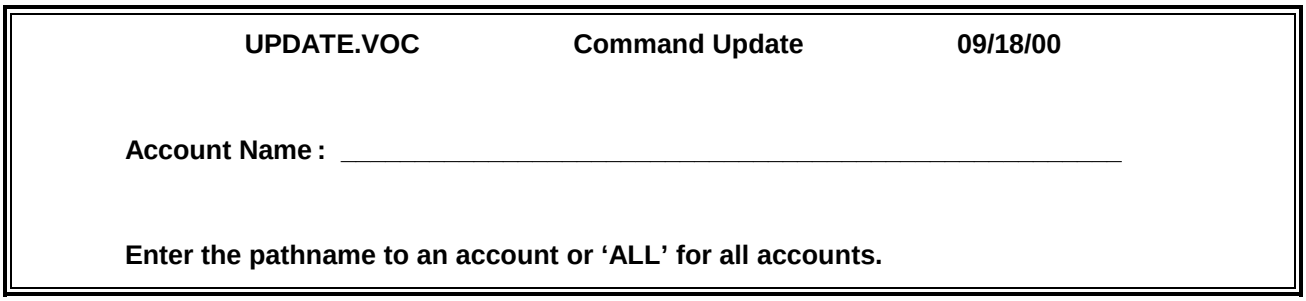

Figure 46 - *This is an example of the screen used to re-load the VOC protection for one or more accounts.*

SENTRY command protection uses the database file SENTRY.COMMANDS to store data about protected commands. The protected commands actually reside in the VOC file of the account where they are used. It is possible through the use of the editor or upgrading to a new release that the protected VOC records could be overwritten. This program will re-load the VOC protection from the SENTRY.COMMAND file. To re-install the command protection into the VOC of an account enter the account name at this prompt. You must use the fully qualified UNIX pathname here. To re-load all protected accounts enter ALL. SENTRY will report the number of items to be updated in each account. We suggest you use the Commands Report to review the contents of the SENTRY.COMMANDS file before proceeding with this program.

Once you have entered the pathname to the account SENTRY will validate the pathname and ask if you are ready to continue with the updates. To continue with the updates enter "**OK**". Enter <ESC> to abort this program.

APPENDIX 1

SENTRY INTERNAL SUBROUTINES

NOTICE

The subroutines documented in this appendix are provided as a convenience to the user on a "USE AT YOUR OWN RISK" basis. If you wish to use these programs and need assistance we are willing to help. However, because we cannot prevent misuse or "accidents" which might cause data corruption we must remind you that you are fully responsible!

Be careful . . . . practice safe computing.

All subroutines are catalogued globally as "*SENTRY...". We recommend the following example of BASIC syntax as the preferred technique for calling the SENTRY Subroutines

```
SENTRY.USER.ITEM.CONTROL="*SENTRY.USER.ITEM.CONTROL"
CALL @SENTRY.USER.ITEM.CONTROL
```

Subroutine: SENTRY.ENCRYPT

This subroutine is used to encrypt and decrypt data strings based on a user defined encryption key.

Sample: **CALL @SENTRY.ENCRYPT(DATA.STRING, RETURN.STRING, ENCRYPTION.KEY)**

Parameters:

DATA.STRING (Input)

This can be any data string of any length including already encrypted data.

RETURN.STRING (Output)

This is the result of the encryption. If the data string is already encrypted and the encryption key is the same as was used to encrypt the data, the result will be the decrypted data.

ENCRYPTION.KEY (Input)

This is a character string between 10 and 100 characters long that is to be used as the seed for the encryption routine. Do not use a variable key. Use only a constant, hard coded in your program.

DATA ENCRYPTION

One of the ultimate means of securing sensitive data is to encrypt it. Encryption is simply transforming the data according to some code so that it is not intelligible. For example, an encryption technique might be to assign each letter of the alphabet a number according to its position (A = 1, B = 2, C = 3, etc.). Then to encrypt the word "INFORMATION" we transform it to "9 14 6 15 18 13 1 20 9 15 14". Someone who knows the code can decrypt the series of numbers and retrieve the original data.

There are an almost infinite number of encryption techniques. SENTRY uses a method which can be classified as "private key encryption". The encryption subroutine is SENTRY.ENCRYPT. The subroutine has three arguments -- DATA.STRING, RETURN.STRING and ENCRYPTION.KEY. The ENCRYPTION.KEY may be any string between 10 and 100 characters long. The key is used to uniquely "muddle up" the bits in DATA.STRING. The result is placed into RETURN.STRING. As an example, suppose the key is "OLDSMOBILE" and the input data in DATA.STRING is "SENTRY works great!" The encrypted string in RETURN.STRING might look like "zt>a[H =~3A7|-gyI^003W". To decipher the encrypted data, someone would have to know both the encryption algorithm and the key used.

Decryption works like encryption. If we call SENTRY.ENCRYPT with an encrypted string in the argument DATA.STRING and with the same key in ENCRYPTION.KEY that was used to encrypt the data originally, the string returned in RETURN.STRING will be the original, intelligible data.

SENTRY.ENCRYPT will not change any database delimiters (i.e. record mark, text mark, field marks, value marks, subvalue marks) and will not encrypt other characters into delimiters. Hence, it is perfectly safe to write encrypted data into data files.

Examples of BASIC code to store encrypted data and display decrypted data are shown below:

```
STORE.ENCRYPTED
        SENTRY.ENCRYPT = "*SENTRY.ENCRYPT"
        INPUT THE.DATA
        THE.KEY - "Fudge Tastes Good!"
        CALL @SENTRY.ENCRYPT(THE.DATA,
                CRYPT.DATA,THE.KEY)
```

```
        WRITE CRYPT.DATA ON
              FILE.VAR, REC.KEY

DISPLAY.DECRYPTED
        SENTRY.ENCRYPT = "*SENTRY.ENCRYPT"
        READ THE.RECORD FROM FILE.VAR,
              REC.KEY ELSE ...
        THE.KEY = "Fudge Tastes Good!"
        CALL @SENTRY.ENCRYPT(THE.RECORD,
              OUT.DATA, THE.KEY)
        PRINT OUT.DATA
```

It is critical that the encryption key be a constant. Without the key, decryption of encrypted data is not possible. If an incorrect key is used with encrypted data, the data is re-encrypted and will now require two decryptions to be made readable. For example, suppose that data were encrypted three times with different keys as follows:

```
CALL @SENTRY.ENCRYPT(ORIG.DATA, ENCRYPT.DATA, KEYA)

CALL @SENTRY.ENCRYPT(ENCRYPT.DATA, MUDDLED.DATA, KEYB)

CALL @SENTRY.ENCRYPT(MUDDLED.DATA, GARBLED.DATA, KEYC)
```

To decrypt GARBLED.DATA we'd have to call SENTRY.ENCRYPT three times as follows:

```
CALL @SENTRY.ENCRYPT(GARBLED.DATA, TEMP.DATA, KEYC)
CALL @SENTRY.ENCRYPT(TEMP.DATA, TEMP.DATA2, KEYB)
CALL @SENTRY.ENCRYPT(TEMP.DATA2, ORIG.DATA, KEYA)
```

NOTICE: Be extremely careful when you use encryption. Test thoroughly and on a comprehensive set of data. Once data are encrypted using your own private encryption key, we know of NO technique to decrypt the data should you overwrite, forget, lose, or destroy the original key. You are completely responsible for your use of this subroutine. It's POWERFUL and potentially dangerous.

Subroutine: SENTRY.USER.ITEM.CONTROL

SENTRY.USER.ITEM.CONTROL is a subroutine used to determine access rights of a user ID to items defined by the user with the SENTRY User Item Maintenance Screen (Section 2-6).

Sample:

```
SENTRY.USER.ITEM.CONTROL = "*SENTRY.USER.ITEM.CONTROL"
```

ERROR.TEXT = “””“

CALL @SENTRY.USER.ITEM.CONTROL(USER.ITEM, ITEM. FOUND, ACCESS.RIGHTS, ERROR.TEXT)

Parameters:

USER.ITEM (Input)

This is the name of the item that was defined with the SENTRY User Item Maintenance screen.

ITEM.FOUND (Output)

The item requested is searched for in two steps.

STEP 1: The SENTRY.USER.ITEMS file is searched in the current account for the item. If the local SENTRY.USER.ITEMS file cannot be accessed or the item is not found, the subroutine will then continue with step 2.

STEP 2: The SENTRY.USER.ITEMS file in the SENTRY account is searched for the item. A file pointer in the local VOC should be called SENTRY.GLOBAL.USER.ITEMS. It should look like this:

F
sentry/SENTRY.USER.ITEMS
sentry/D_SENTRY.USER.ITEMS

Where “sentry” is replaced by the absolute pathname to the “sentry” directory. On our machine, the path is /usr/sentry/SENTRY.USER.ITEMS.

If the item is found in either step 1 or 2, the value will be 1. If the SENTRY.USER.ITEMS file in the SENTRY account cannot be accessed or the item is not found in either step 1 or step 2, the value returned will be 0.

ACCESS.RIGHTS (Output)

If the user item was found, the current user's rights to the item are returned.

ERROR.TEXT (Output)

If an error was encountered by the subroutine, an error message will be returned. If no error occurred ERROR.TEXT will be null.

Subroutine: SENTRY.VIOLATION.STAMP

SENTRY.VIOLATION.STAMP is used to log access violations of user items.

Sample :

```
SENTRY.VIOLATION.STAMP = "*SENTRY.VIOLATION.STAMP"

CALL @SENTRY.VIOLATION.STAMP(USER.ITEM, COMMENT)
```

Parameters:

USER.ITEM (Input)

The user-defined item for which the violation occurred. This reference was created through the SENTRY User Item Maintenance screen.

COMMENT (Input)

Free format text description of the violation.

This is a routine similar to the one which logs violations to the SENTRY Violations Log when a user with insufficient rights attempts to use a SENTRY protected command. It will create a new entry in the SENTRY.VIOLATIONS.LOG file. The entry will then appear in the SENTRY violations report.

APPENDIX 2

SENTRY KEY BINDINGS

A record called "KEY.BINDINGS" in the SENTRY.CONTROL file is used to control the keystrokes used to activate special functions within the SENTRY data entry screens. For example, the "normal" way to exit from a data entry screen is by entering the <escape> character followed by <return>. This may create a conflict for sites using certain communications packages. By modifying the KEY.BINDINGS record, the user may customize his version of SENTRY to use whatever series of keystrokes is desired for each of the functions.

The record contains three multi-valued fields. Field one is the name of the function to be controlled -- the names should not be changed, as SENTRY depends upon them appearing as expected. Field two is the series of characters to be entered to activate the corresponding function -- note that it is assumed that a <RETURN> will be entered and the <RETURN> does not have to appear within the series of characters. Field three of the record contains the text which is used to describe the keystrokes (e.g. <ESC> for the escape key).

The default KEY.BINDINGS record is shown below:

FUNCTION NAME	KEYSTROKES	DESCRIPTION
XREF.OPTION	"@"	"@"
PREV.FIELD	"^"	"^"
DEL.FIELD	SPACE	<SPACE>
REPAINT	"^^"	"^^"
CANCEL	ESC	<ESC>
HELP	"HELP"	"HELP"

Note that under KEYSTROKES, the words SPACE and ESC are meant to represent the simple characters produced by pressing the space bar and the escape key.

To modify the set of keystrokes used for any of the functions, simply modify the appropriate value in field two of the record, using the database editor. Place the description of the keystrokes into the corresponding value of field three. After modifying the record the user must quit to UNIX, reenter the database

environment and reenter SENTRY in order for the changes to take effect because these variables are read into named COMMON. **NOTE: DO NOT** enter the quote marks.