

Account Troubleshooting Program

By

Ashley Monhollon

Submitted to
the Faculty of the Information Engineering Technology Program
in Partial Fulfillment of the Requirements for
the Degree of Bachelor of Science
in Information Engineering Technology

University of Cincinnati
College of Applied Science

May 2001

Account Troubleshooting Program

By

Ashley Monhollon

Submitted to
the Faculty of the Information Engineering Technology Program
in Partial Fulfillment of the Requirements for
the Degree of Bachelor of Science
in Information Engineering Technology

University of Cincinnati
OMI College of Applied Science

Copyright 2001 Ashley Monhollon

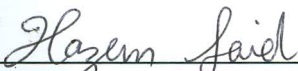
The author grants to the Information Technology Program permission to reproduce and distribute copies of this document in whole or in part.



Ashley Monhollon

5-24-01

Date



Dr. Hazem Said, Faculty Project Advisor

5/24/01

Date



Dr. Lawrence Gilligan, Department Head

5/25/01

Date

Acknowledgements

The author wishes to express her sincere gratitude to the faculty of the Information Engineering Technology Program. Without their help, the successful completion of this project would not have been possible. I would also like to express a special acknowledgement of the contribution made by Dr. Hazem Said, the project advisor, and Dr. Sam Geonetta. I appreciate the time they spent working with me and their guidance and support.

I would also like to acknowledge the help and guidance from colleagues. Valuable resources I used to help complete this project include Tony Drake, UNIX Infrastructure, Mike Schneider, UNIX Programming, Paul Tibbits, HP Instructor, and Mark Jeanmoughin, Autosecure Administrator. Their assistance helped with the completion of the project.

Table of Contents

Section	Page
Acknowledgements	i
Table of Contents	ii
List of Illustrations	iii
List of Tables	iv
Abstract	v
1. Statement of the Problem	1
1.1 Definition of the Need	2
2. Description of the Solution	4
2.1 User Profile	4
2.2 Design Protocols	4
3. Objectives of the Project (Deliverables)	8
4. Design and Development	9
4.1 Budget	9
4.2 Timeline	10
4.3 Software	14
4.4 Hardware	14
5. Proof of Design	15
5.1 Program functionality	15
5.1.1 Help	16
5.1.2 Username Not Found	17
5.1.3 Autosecure Not Operating	18
5.1.4 No Problems Noted	19
5.1.5 Account Deactivated	20
5.1.6 Account Suspended	21
5.1.7 Account Expired	22
5.1.8 Grace Logins Assigned to Zero	23
5.1.9 Account Exists Only in UNIX	24
5.1.10 UID Mismatch	25
5.1.11 Home Directory Missing	26
5.1.12 Home Directory Owned by Another ID	27
5.1.13 Account does not Exist in UNIX	28
5.1.14 Account does not Exist on Local	29
5.1.15 Account Exists at the Parent Only	30
5.1.16 Primary Group does not Exist	31
5.1.17 Account is Quite Confused	32
5.1.18 GUI Interface	33
6. Conclusion	35
7. Recommendations	36
Appendix A: /etc/passwd file	37
Appendix B: /etc/group file	38
Appendix C: /tcb/files/auth/t/<login id> file	39
Appendix D: Autosecure selang prompt output	40
Appendix E: Code	41
References	72

List of Illustrations

- Figure 1. Chart detailing incidents pre- and post-Autosecure Installation
- Figure 2. Pie chart detailing the specific incidents and volume
- Figure 3. Help output
- Figure 4. Username not found output
- Figure 5. Autosecure not running output
- Figure 6. No problems noted output
- Figure 7. Account is deactivated output
- Figure 8. Account is suspended output
- Figure 9. Account is expired output
- Figure 10. Grace logins assigned to zero output
- Figure 11. Account only exists in UNIX output
- Figure 12. UID mismatch output
- Figure 13. Home directory is missing output
- Figure 14. Home directory is owned by another ID output
- Figure 15. Account exists in Autosecure, not UNIX
- Figure 16. Account exists in UNIX and Autosecure parent, not local
- Figure 17. Account exists at the Autosecure parent only
- Figure 18. Primary group does not exist output
- Figure 19. Account information is not consistent output
- Figure 20. Connection to an NT CITRIX Server
- Figure 21. GUI Interface output
- Figure 22. Execution run (GUI Interface)
- Figure 23. Program output (GUI Interface)

List of Tables

- Table 1. Table detailing incidents monitored and tracked during six months.
Table 2. Detailed cost for functionality on one Midrange system.
Table 3. Timeline / Task List.

Abstract

System Administrators spend numerous hours detecting and correcting UNIX user account problems. The software package, Autosecure, has been installed on all the UNIX Midrange systems in attempt to increase security and manageability. With the installation of Autosecure, account problems have increased dramatically. The details and specifics are described in the *Statement of Problem* and *Definition of Need* Section.

This document discusses the aspects of design and implementation necessary in the development of an Account Troubleshooting Program. The project's purpose is to eliminate unnecessary time spent manually correcting and searching for UNIX user account problems. The program has been designed to immediately detect the problems associated with user accounts and if possible, automatically correct the problems.

The program was tested successfully and proved beneficial to correcting and eliminating problems. The structure, design, flow, and management of the UNIX Account Troubleshooting Program is explained in detail. This document includes the *Problem and Solution*, in terms of program design, as well as user and operator characteristics. The deliverables, budget, timeline, software, and hardware are discussed in the *Design and Development* Section. The *Proof of Design* section details the specifics of the program, identifies all possible problems, details an algorithm for resolution, and demonstrates execution of the program.

Account Troubleshooting Program

1. Statement of the Problem

Procter & Gamble uses over four hundred UNIX systems to provide various means of support and serve as platforms for many different applications. The company currently runs HP-UX and IBM AIX versions of UNIX. A security package, Autosecure, has been installed on all systems to provide extra security and allow greater manageability of user accounts.

UNIX security is basic on the operating system level; the Autosecure software program allows the possibility of restrictions. The restrictions include defining which users are able to access certain files during certain days and times. The package also includes better command tracking to identify which users execute which commands. The ability to switch user to a certain ID and execute a command is also possible by defining rules. With this added security, more account problems arise because of the increased complexity. System administrators spend a great deal of time determining the root cause of login problems. The details of time spent and problems created are explained in detail in the *Definition of Need* Section.

External vendors were considered to provide a possible solution to this problem, but there was not anything readily available that met all requirements. The assumption, made by the company's security team, was that all the problems with Autosecure would be resolved quickly, so there would not be a need for a program like this. It was assumed that the user account problems would decrease as Autosecure problems were solved. This assumption was incorrect; therefore, the creation of a troubleshooting program is necessary. Procter & Gamble also has a unique UNIX environment because of the

volume of servers creating complications for external vendors due to all the various Operating System versions and software packages running on the servers. Nothing was already created that was useable for all technology platforms.

1.1 Definition of the Need

Security problems in the past did not take up a majority of time spent by system administrators. With the installation of Autosecure, the number of incidents has climbed exponentially. Figure 1 details the number of incidents before and after the installation of the Autosecure security package. From the data in Figure 1, it is evident that system administrators spend a lot of time working on incidents. With automatic identification and correction of problems, valuable time will be saved.

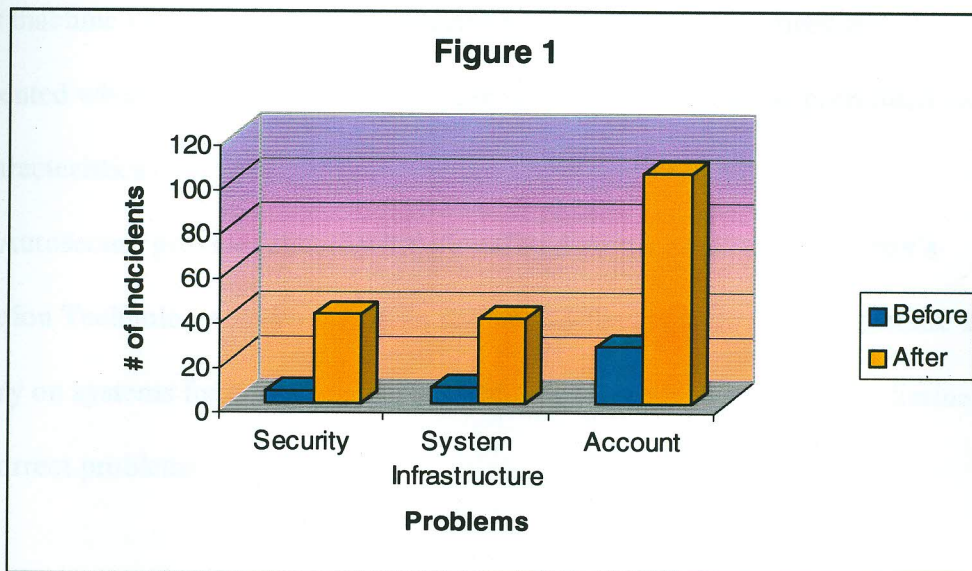


Figure 1. Chart detailing pre- and post-Autosecure installation

The reason more problems exist is because more things can go wrong with Autosecure. Autosecure offers security considerations and functionality for the UNIX platform, providing the necessary access control tools, but creating more complications when it comes to account problems. Privileges can be set based on a per administrator

basis, which can prevent or allow certain operations, including prevention of unauthorized access to files and servers, prevention of certain functions/applications being launched, automatic initiation in the event of an attempted violation, logging of activities in relation to users, central administration, delegation on authority, predefined security administration options and restrictions can be enforced based on time or time-frame, day, user ID, location, network connection type, password expiration, period between user access, and other account characteristics.

In an attempt to reduce the overhead that can potentially be incurred through the interception of all client requests, AutoSecure detects that, for example, a “file open” request has been initiated and then processes the necessary authorization procedures on the host machine via a local run-time security rules database. “Soft firewalls” can also be implemented whereby all TCP/IP requests are intercepted and can be prohibited based on host characteristics.

Autosecure provides security functionality deemed necessary for today's Information Technology environment. In reaction to the decision that Autosecure is necessary on systems for a secure environment, action needs to be taken to eliminate and easily correct problems.

2. Description of the Solution

The program provides Procter & Gamble with a UNIX User Account Troubleshooting System. This involves the configuration and creation of a UNIX shell script, the creation of test user accounts, and implementation of the functionality necessary for correcting account problems. To solve the problem discussed in the previous pages, the ATP program handles the complexity of Autosecure and UNIX.

2.1 User Profile

This program is constructed for system administrators. It is not intended for end users or users with limited knowledge of the UNIX operating system. The level of Information Technology literacy is high with regard to knowledge and training of the UNIX operating system environment (HP and IBM platforms) and the Autosecure software. Users running the program will also need to have specific security access, set up by an Autosecure rule, since the auto-correcting feature of the program allows for changes in account security and restrictions.

2.2 Design Protocols

I have gathered information on all Autosecure incidents to determine the functionality required by the Account Troubleshooting Program. Table 1 indicates the problems identified by tracking the most common re-occurring incidents. Fifteen problems were identified that the program will target and fix: Username not found / account does not exist, Autosecure is not operating or is operating improperly, the account is deactivated, the account is suspended, the account is expired, the grace logs are set to zero, the account exists only on the UNIX level, the User ID number doesn't match in the configuration files, the home directory is owned by another ID or missing,

the account does not exist in UNIX, the local Policy Model, or neither, the Primary Group doesn't exist, and the account information isn't consistent. Table 1 details the number of incidents within a six-month period.

<i>ID #</i>	<i>Problem Detected</i>	<i>Incidents (6 months)</i>
1	<i>Username not found (does not exist).</i>	40
2	<i>Autosecure not operating / problems.</i>	36
3	<i>Account is deactivated.</i>	230
4	<i>Account is suspended.</i>	1
5	<i>Account is expired.</i>	13
6	<i>Grace Logins assigned to zero.</i>	201
7	<i>Account exists only in UNIX.</i>	57
8	<i>UID Mismatch.</i>	32
9	<i>Home Directory is missing.</i>	60
10	<i>Home Directory owned by another ID.</i>	24
11	<i>Account doesn't exist in UNIX.</i>	71
12	<i>Account doesn't exist in Local Policy Model.</i>	49
13	<i>Account exists at the Parent Policy Model only.</i>	16
14	<i>Account information is not consistent.</i>	6
15	<i>Primary Group doesn't exist.</i>	198

Table 1. Table detailing incidents monitored and tracked during six months.

Figure 2 details the volume in relation to incidents based on the ID # column of Table 1.

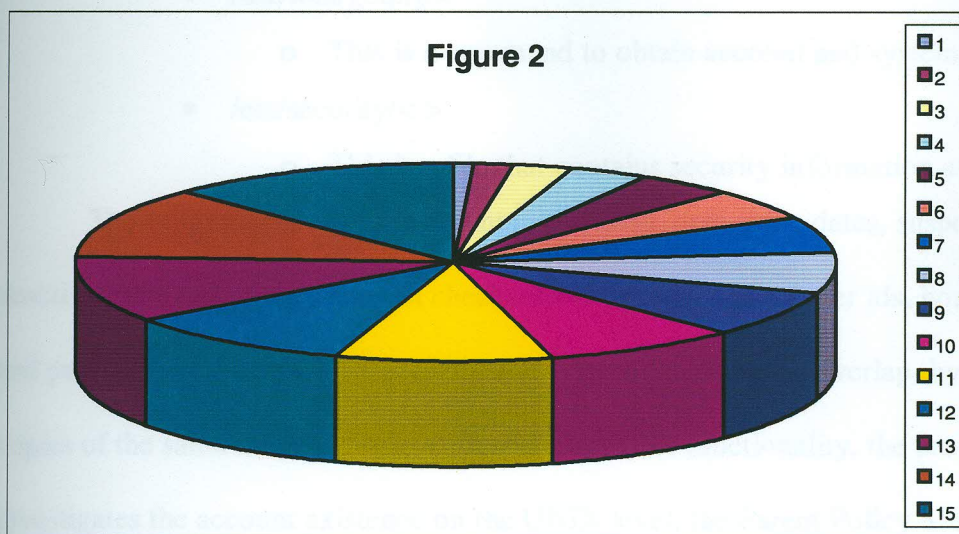


Figure 2. Pie chart detailing the specific incidents and volume

In order to identify and correct the problems in Table 1 and Figure 2, it will include accessing the UNIX files and commands:

- /usr/seos/bin/selang
 - This is a command that allows execution for Autosecure administration. (*prompt detailed in Appendix D*)
- /usr/seos/seos.ini
 - This command checks for the installation of Autosecure.
- /etc/passwd
 - This is a file that contains the user name, ID numbers, and user characteristics. (*detailed in Appendix A*)
- /etc/group
 - This is a file that contains a list of all the groups on the system, the group ID, and the login names belonging to that group. (*detailed in Appendix B*)
- /tcb/files/auth/<user id>
 - This file contains the same information as /etc/passwd, but it is a requirement for Autosecure, not UNIX, and is specific to each ID. (*detailed in Appendix C*)
- /usr/sbin/getprpw
 - This is a command to obtain account and system information.
- /etc/security/< >
 - This is a file that contains security information and restrictions.

The program checks for account restrictions, expiration dates, suspensions, deactivations, and grace logins. It checks the characteristics of user ids, home directories, and permissions. Since UNIX security and Autosecure security overlap, by needing copies of the same information in different places for functionality, the program also investigates the account existence on the UNIX level, the Parent Policy Model level (which is the high-level configuration item of the account – it identifies the nodes the

user has access to), and the Autosecure host. This is detailed in the *Proof of Design* Section. To see the details of the algorithms and code, refer to *Appendix E*.

The interface for the prototype is text based on the UNIX operating system. An option for execution is to use Exceed Windows. This is accomplished by connecting to an NT server via CITRIX and then connecting to the UNIX Server. This will allow for a visual GUI interface if the user desires. The program is executed by double-clicking on an icon titled ATP and supplying the user name as the argument. I anticipate that this option will not be utilized very often because the response time of execution is slowed down incredibly and the program only requires one argument. Also, as detailed in the *User Profile* Section, the users will have UNIX knowledge and they will be familiar with the command line operating system functionality.

3. Objectives of the Project (Deliverables)

The objective of this project is to create an Account Troubleshooting Program that identifies and corrects problems with various UNIX user accounts. The program checks for problems at the UNIX base security level, as well as the security package, Autosecure, running on the various hosts. The hosts include UNIX operating system versions, AIX and HP-UX. The associated applications running on the servers are SAP, Oracle, Netbackup, Control M, RTCIS, service guard, harvest, email, and I3, as well as other applications. The program reduces time, effort, and the volume of UNIX account problems.

The program will automate and detect as many UNIX user problems as possible. Automatic corrective actions have been created for everything that is feasible. With this functionality in place, a great deal of time will be saved.

In the concluding section of this report, I recommend the Account Troubleshooting Program be installed on all UNIX systems with user accounts.

4. Design and Development

The design and development aspect of this project has been ongoing throughout the Senior Design course sequence. The incredible volume of considerations, possible resolution steps have occupied the author's time throughout the year as well as gaining technical knowledge. For the detail of design, refer to the Timeline (Table 3), which includes the necessary algorithms for accomplishing the completion of the project.

4.1 Budget

REQUIREMENT	COST
Midrange computing system	\$389,000.00
Autosecure software license	\$3,500.00
Programming / UNIX books	\$63.50
HP Scripting Course	\$2,200.00
TOTAL:	\$394,763.50

Table 2. Detailed cost for functionality on one Midrange system

The sources of funding:

The hardware and software was previously purchased by Procter & Gamble. The books and programming course were funded by Procter & Gamble during the Senior Design sequence.

4.2 Timeline

Table 3 is a Timeline and Task List that details the task, the action taken and algorithm to solve, as well as the Target and Completion dates.

Task	Action	Target	Finish
Proposal	Create Senior Design I Proposal	SDI	Yes.
Design Freeze	Create Senior Design II Design Freeze	SDII	Yes.
Training	Attend Hewlett Packard Education Course H4322S – shell programming. (5 days)	SDII	Yes.
Program Functionality	Details Below:	SDIII	Yes.
Autosecure is not installed on system.	Output Info.	SDII	Yes.
Autosecure configuration problems.	Output Info.	SDII	Yes.
Autosecure is down.	Output Info.	SDII	Yes.
Autosecure is in maintenance mode.	Output Info.	SDII	Yes.
Account is deactivated.	Reactivate the account.	4/6/2001	Yes.
Algorithm:	Check variable _T_ALOCK. If it is not equal to “no” or “n/a”, the account is deactivated. Reactivate by calling script /usr/sbin/modprpw -k and supplying user ID.		
User only exists in UNIX – not in Autosecure parent or local.	Provide information that the account should be added in Autosecure by the security contact.	SDII	Yes.
Algorithm:	Check variable _U_UEXIST = “yes”. Check L_UEXIST = “no” and P_UEXIST = “no”. Cannot auto-correct by adding accounts in Autosecure, so provide necessary info.		
“No problems noted” analysis check.	- give info if account is OK.	SDII/III	Yes.
Algorithm:	Check _ANALYSIS variable status. If = N, then no problem found. If = Y, a problem was found and the variable was assigned to Y. Echo “No problems noted.”		
Primary group does not exist in /etc/group	Provide information of configuration error.	SDII	Yes.
Algorithm:	Check variable U_PGRP_NAME. If assigned to “Not found”, group doesn’t exist. Supply information.		
The UIDs in the /etc/passwd file and the tcb file do not match.	Provide information – cannot be auto-corrected because there is no way to know which UID is correct if they’re different.	4/2/2001	Yes.

Algorithm:	Check variables U_UID, T_UID. If both are not equal to "NONE" and U_UID is not equal to T_UID, provide info. Give what both UIDs are set to. Check: /etc/passwd & /tcdb/files/auth/t/<user ID>		
Account restrictions exist.	Provide information and request to review – may be a problem, may be correct.	4/2/2001	Yes.
Account has an administrative lock / suspended.	Provide information – cannot auto-correct, but prompt if the user wants to remove suspension.	4/9/2001	Yes.
Algorithm:	Check local suspend and policy suspend variables P_SUSPEND & L_SUSPEND. If they are not equal to "N/A", the account is suspended. Supply information & prompt to remove the suspension.		
Account is expired in Autosecure.	Cannot automatically do because sometimes accounts shouldn't be un-expired. Prompt and with a Y answer, the script will automatically un-expire the account.	4/9/2001	Yes.
Algorithm:	If P_EXPIRE or L_EXPIRE are not equal to "N/A", then the account is expired. Prompt to remove the expiration date. If yes, issue host \$PMDB and cu LOGINID expire-.		
Grace logins have reached zero.	Automatically reset the grace logins to 5.	4/9/2001	Yes.
Algorithm:	Check for L_GRACELOG –eq to zero. (only have to check local because grace logins are not a factor at the PMDB level). If they are equal to zero, issue host <node>, cu <loginID> grace(5) and provide info.		
Home directory does not exist.	Provide information and give option to create the directory.	4/16/2001	Yes.
Algorithm:	Just check if the directory /home/<login id> exists. Cannot auto-correct because sometimes it's not a problem. Shared accounts + some user accounts are not set up with home directories because they won't be used, but prompt user to create directory if desired.		
Home directory owned by an ID other than login name.	Provide info. – do not auto-correct because some accounts are purposely set up this way, but prompt if ownership change is desired.	4/16/2001	Yes.
Algorithm:	Just check the owner of the directory /home/<login id>. Cannot auto-correct because some accounts are purposely set up this way. Provide information & correct.		
Account exists in both PMDBs, but not locally	Automatically add on UNIX level.	4/16/2001	Yes.

in UNIX.			
Algorithm:	Check for U_EXIST = No, L_EXIST & P_EXIST = Yes. See if user info. Exists at parent and copy to UNIX if so. If not, check locally and get info. If info. Is not found, prompt for it. Read info and add account.		
Account only exists partially in UNIX.	Add completely.	4/16/2001	Yes.
Algorithm:	See if user info. Exists at parent and copy to UNIX if so. If not, check locally and get info. If info. Is not found, prompt for it. Read info and add account.		
Account exists in unix and at local PMDB but not at parent.	Request escalation.	5/3/2001	Yes.
Algorithm:	Check U_EXIST & L_EXIST = Yes, P_EXIST = No. Cannot add at parent. Request escalation.		
The account exists only at the local policy model and partially in UNIX.	Add the account locally automatically.	4/16/2001	Yes.
Algorithm:	Check for existence. Since it's partial, it's probably a problem. Remove and re-add.		
User only exists in unix, but with an entry in the parent PMDBs passwd file.	Request escalation.	5/3/2001	Yes.
Algorithm:	Check U_UEXIST = Yes, L_UEXIST & P_UEXIST = No. A number of different things could be wrong – cannot correct anything. Supply information to escalate problem.		
Account only exists at parent PMDB.	Add account to the local PMDB and on the UNIX level.	5/3/2001	Yes.
Algorithm:	Combine the fix for existence not on local only and not UNIX only.		
Account exists at parent and partially in UNIX, but not at local.	Add the account & correct.	4/23/2001	Yes.
Algorithm:	Host to <local host> Issue “nu <user id>” + owner + all other account variables. Mention sync_pw script.		
Account exists in parent PMDB and unix, but not locally.	Add locally.	4/23/2001	Yes.
Algorithm:	Check for U_EXIST & P_EXIST = Yes and L_EXIST = No. Host to <local host> Issue “nu <user id>” + owner + all other account variables.		

Account exists in parent PMDB and partially in unix, and not locally.	Add locally and in UNIX.	4/23/2001	Yes.
Algorithm:	Check for U_EXIST = Yes, P_EXIST not completely with partial variables, and L_EXIST = No. * Same fix as adding the account when doesn't exist in local PMDB only or UNIX only.		
Account exists everywhere except there is no entry in the passwd file of the parent PMDB.	Correct by adding entry.	5/3/2001	Yes.
Algorithm:	Check for U_EXIST, L_EXIST, & P_EXIST. Check that account exists everywhere, except there is no entry in policies dir passwd file. Add the account by issuing "host PMDB", "nu <id>" + arguments: home directory, shell, primary group, & user name. Also, check for the group list of the user and join to appropriate groups. Instruct that the password should be reset.		
GUI interface.	Exceed interface – for a GUI version of program.	5/2001	Yes.
Progress Check 1	Progress Report	4/19/2001	Yes.
Progress Check 2	Progress Report	5/3/2001	Yes.
Draft of Final Report	Draft of Final Report	5/10/2001	Yes.
Final Project	Final Project	5/24/2001	Yes.
Bound copies of Final Project	Acceptance of advisor and bound copies.	6/4/2001	Yes.
Create Presentation	Create Presentation	5/31/2001	Yes.

Table 3. Task List

4.3 Software

The software used in this project includes the following:

- UNIX operating system.

The only operating system requirement is an HP9000 or RS6000 system. The current support environment uses HP UNIX and IBM UNIX. The versions of HP UNIX are 10.20 and 11.0. The versions of AIX are 2 and 3. The program accommodates all the different environments.

- Autosecure software.

The Autosecure software needs to be installed for the script to account for all the possible problems. The current support environment uses a small percentage of HP UNIX systems that do not run Autosecure, because they have had complications with the compatibility of the software running on the system and Autosecure. The program will allow for this and it will check if Autosecure is running. The results will differ depending on the status of the software.

4.4 Hardware

The requirements for hardware include an HP or IBM midrange computer system of a current vendor supported class.

5. Proof of Design

5.1 Program Functionality

This program will generate account information about a user, identify, and correct problems. The user will enter “atp <login name>” (atp stands for Account Troubleshooting Program) and it will return information about the account. This will help isolate the root cause of an account problem because it will eliminate the need for unnecessary checking to rule out possible problem causes. It will detail the exact problem, auto-correct it, or explain exactly how to correct it.

The script will include many account details.

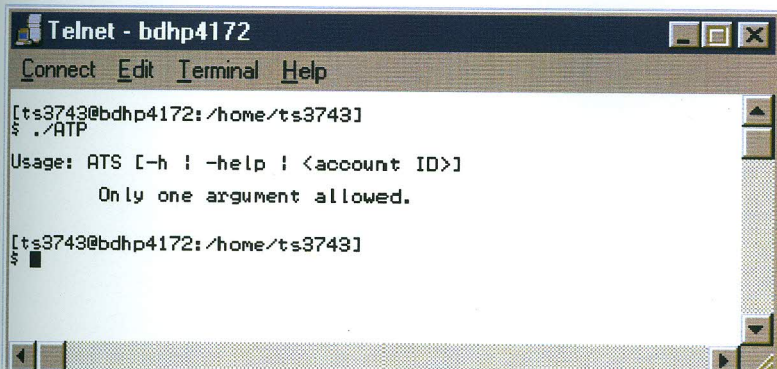
Checks / Includes the following:

1. Argument and usage
2. Prompt functions
3. Is autosecure installed?
4. Is autosecure configured?
5. parent PMDB name
6. if the user exists in unix
7. UID in /etc/password
8. GID in /etc/passwd
9. users name in /etc/passwd
10. users home directory
11. owner of users home directory
12. users default shell
13. name of users primary group
14. UID from tcb files
15. last successful password change
16. last successful login
17. last unsuccessful login
18. number of unsuccessful login attempts

19. login time/day restrictions
20. account expiration day
21. Autosecure maintenance periods
22. Autosecure existence
23. Account partial existence
24. groups
25. ownership of home directories
26. versions of Autosecure
27. grace logins
28. account disability
29. primary group
30. account expirations
31. administration locks

5.1.1 Help Output

If help is required, the administrator will just need to enter the name of the program, as shown in Figure 3. A usage statement will be returned. No other help will be available since experienced UNIX users will be using the program and they will receive training on it.

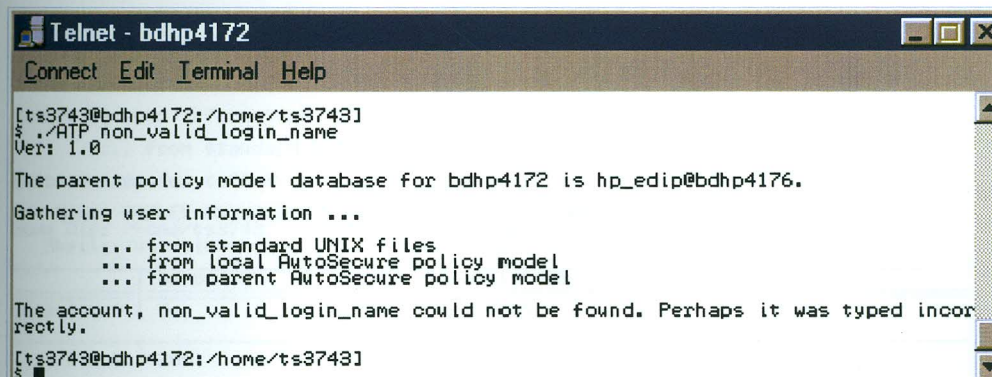


```
Telnet - bdhp4172
Connect Edit Terminal Help
[ts3743@bdhp4172: /home/ts3743]
./ATS
Usage: ATS [-h | -help | <account ID>]
    Only one argument allowed.
[ts3743@bdhp4172: /home/ts3743]
```

Figure 3. Help output

5.1.2 Username Not Found Output

When the program begins execution, one of the first checks made is to determine whether or not the user name exists on the system. If the user does not have an account, the program immediately responds with that information. Figure 4 shows the output of the program.



```
Telnet - bdhp4172
Connect Edit Terminal Help
[ts3743@bdhp4172:/home/ts3743]
$ ./ATP_non_valid_login_name
Ver: 1.0

The parent policy model database for bdhp4172 is hp_edip@bdhp4176.
Gathering user information ...
... from standard UNIX files
... from local AutoSecure policy model
... from parent AutoSecure policy model

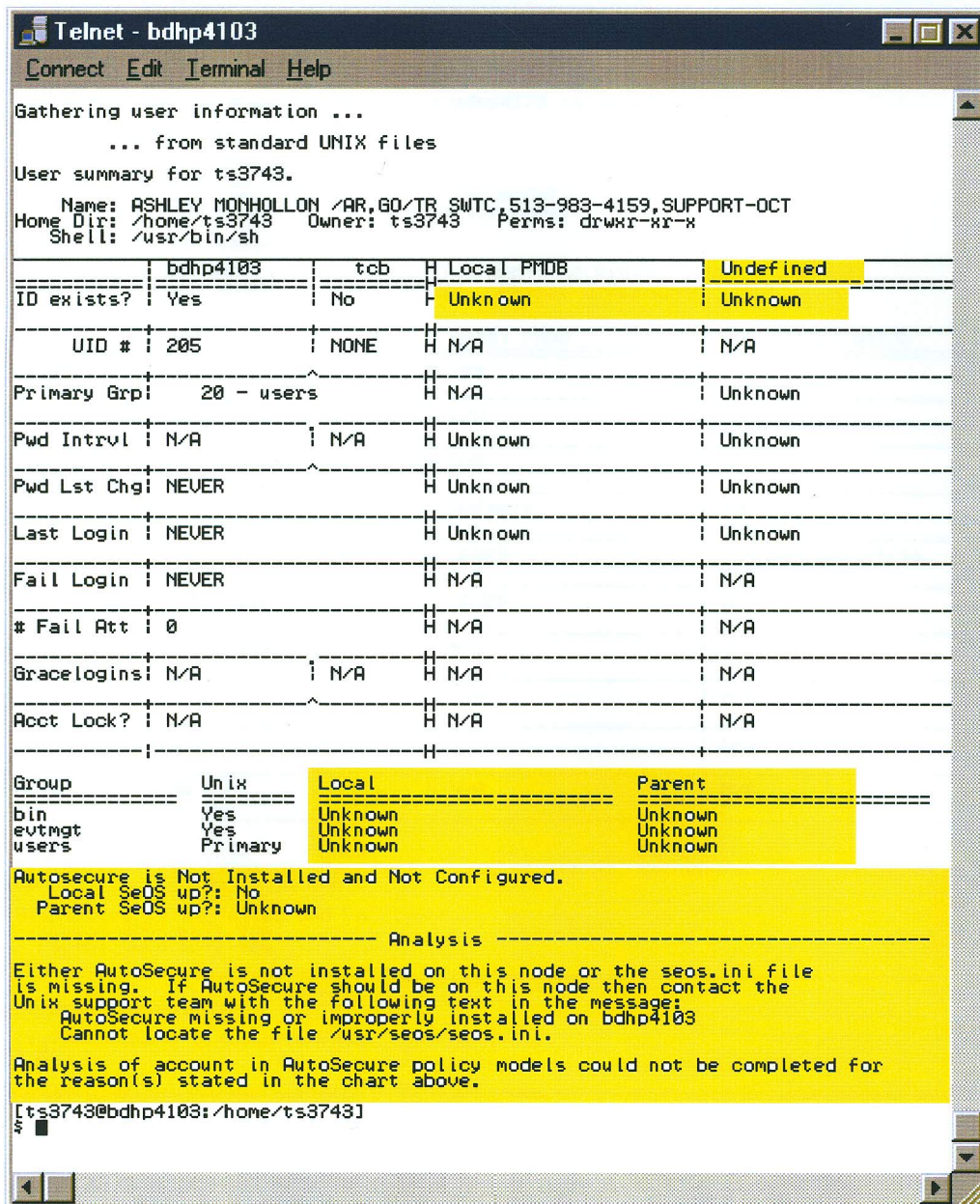
The account, non_valid_login_name could not be found. Perhaps it was typed incor
rectly.
[ts3743@bdhp4172:/home/ts3743]
$
```

Figure 4. Username not found output

5.1.3 Autosecure Not Running

Currently, Autosecure is not installed on every system because it created complications with the software or application. The program is designed to run on non-Autosecure hosts. It simply makes the check and responds that Autosecure is not running.

Figure 5 shows the output of the program.



```
Telnet - bdhp4103
Connect Edit Terminal Help

Gathering user information ...
... from standard UNIX files
User summary for ts3743.
Name: ASHLEY MONHOLLON /AR,GO/TR SWTC,513-983-4159,SUPPORT-OCT
Home Dir: /home/ts3743 Owner: ts3743 Perms: drwxr-xr-x
Shell: /usr/bin/sh

===== bdhp4103 tcb H Local PMDB Undefined
ID exists? Yes No F Unknown Unknown
UID # 205 NONE H N/A N/A
Primary Grp 20 - users H N/A Unknown
Pwd Intrvl N/A N/A H Unknown Unknown
Pwd Lst Chg NEVER H Unknown Unknown
Last Login NEVER H Unknown Unknown
Fail Login NEVER H N/A N/A
# Fail Att 0 H N/A N/A
GraceLogins N/A N/A H N/A N/A
Acct Lock? N/A H N/A N/A
=====

Group Unix Local Parent
bin Yes Unknown Unknown
evtmgt Yes Unknown Unknown
users Primary Unknown Unknown

Autosecure is Not Installed and Not Configured.
Local SeOS up?: No
Parent SeOS up?: Unknown

----- Analysis -----
Either AutoSecure is not installed on this node or the seos.ini file
is missing. If AutoSecure should be on this node then contact the
Unix support team with the following text in the message:
AutoSecure missing or improperly installed on bdhp4103
Cannot locate the file /usr/seos/seos.ini.

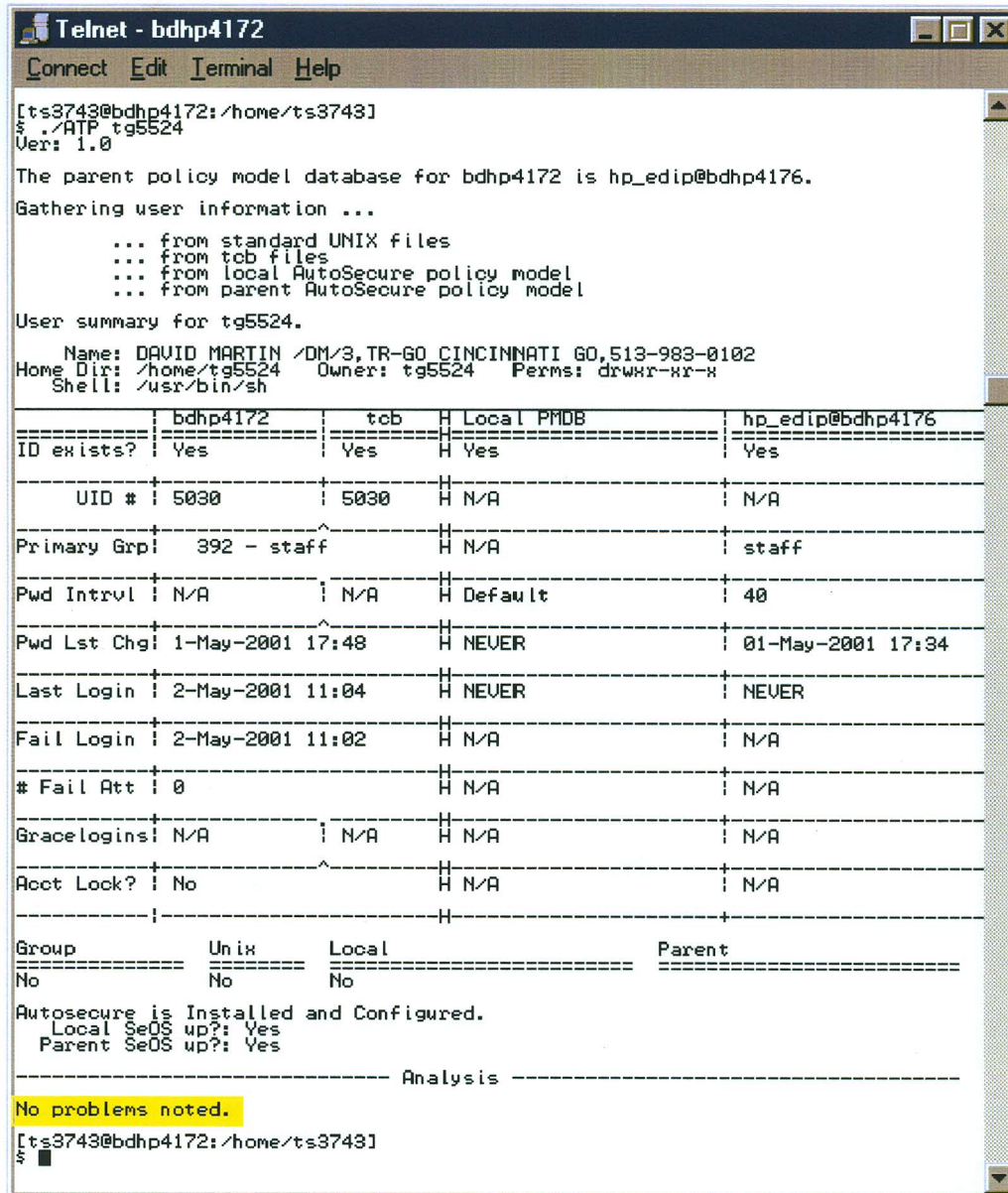
Analysis of account in AutoSecure policy models could not be completed for
the reason(s) stated in the chart above.

[ts3743@bdhp4103:/home/ts3743]
$
```

Figure 5. Autosecure not running output

5.1.4 No Problems Noted

The program will check for a number of problems and if a problem is identified, a ANALYSIS flag will be set to Yes. If the flag is assigned to No, no problems were found. Figure 6 shows the output of the program.



```
Telnet - bdhp4172
Connect Edit Terminal Help

[ts3743@bdhp4172:/home/ts3743]
$ ./ATP tg5524
Ver: 1.0

The parent policy model database for bdhp4172 is hp_edip@bdhp4176.
Gathering user information ...
    ... from standard UNIX files
    ... from tcb files
    ... from local AutoSecure policy model
    ... from parent AutoSecure policy model

User summary for tg5524.
    Name: DAVID MARTIN /DM/3,TR-GO CINCINNATI GO,513-983-0102
    Home Dir: /home/tg5524   Owner: tg5524   Perms: drwxr-xr-x
    Shell: /usr/bin/sh

===== bdhp4172      tcb      H Local PMDB      hp_edip@bdhp4176
ID exists?  Yes      Yes      H Yes      Yes
UID #      5030      5030      H N/A      N/A
Primary Grp 392 - staff      H N/A      staff
Pwd Intrvl  N/A      N/A      H Default  40
Pwd Lst Chg 1-May-2001 17:48  H NEVER    01-May-2001 17:34
Last Login  2-May-2001 11:04  H NEVER    NEVER
Fail Login  2-May-2001 11:02  H N/A      N/A
# Fail Att  0      H N/A      N/A
GraceLogins N/A      N/A      H N/A      N/A
Acct Lock?  No      H N/A      N/A
-----
Group       Unix      Local      Parent
=====
No          No          No
Autosecure is Installed and Configured.
Local SeOS up?: Yes
Parent SeOS up?: Yes

----- Analysis -----

No problems noted.

[ts3743@bdhp4172:/home/ts3743]
$
```

Figure 6. No problems noted output

5.1.5 Account is Deactivated

An account becomes deactivated when a login attempt is made and it fails five times. The program will automatically reactivate deactivated accounts. Figure 7 shows the output of the program.

```
Telnet - bdhp4172
Connect Edit Terminal Help

[ts3743@bdhp4172:/home/ts3743]
$ ./ATP tg5524
Ver: 1.0

The parent policy model database for bdhp4172 is hp_edip@bdhp4176.
Gathering user information ...
... from standard UNIX files
... from tcb files
... from local AutoSecure policy model
... from parent AutoSecure policy model

User summary for tg5524.
Name: DAVID MARTIN /DM/3,TR-GO CINCINNATI GO,513-983-0102
Home Dir: /home/tg5524 Owner: tg5524 Perms: drwxr-xr-x
Shell: /usr/bin/sh
```

	bdhp4172	tcb	Local PMDB	hp_edip@bdhp4176
ID exists?	Yes	Yes	Yes	Yes
UID #	5030	5030	N/A	N/A
Primary Grp	392 - staff		N/A	staff
Pwd Intrvl	N/A	N/A	Default	40
Pwd Lst Chg	1-May-2001 17:48		NEVER	01-May-2001 17:34
Last Login	2-May-2001 11:04		NEVER	NEVER
Fail Login	3-May-2001 13:06		N/A	N/A
# Fail Att	5		N/A	N/A
GraceLogins	N/A	N/A	N/A	N/A
Acct Lock?	Yes, too many logins.		N/A	N/A

```
Group      Unix      Local      Parent
=====
No         No         No

Autosecure is Installed and Configured.
Local SeOS up?: Yes
Parent SeOS up?: Yes

----- Analysis -----
This account was deactivated but has now been reactivated.
Do you wish to view the command log file (Yes or No) [N]? █
```

Figure 7. Account is deactivated output

5.1.6 Account is Suspended

The only time an account can be suspended is if an administrator places it under suspension. The program gives the option to remove the suspension, however, this will not be used often. Figure 8 shows the output of the program.

```
Telnet - bdhp4172
Connect Edit Terminal Help
Last Login | 28-Apr-2001 20:47      H NEVER      | NEVER
-----+-----+-----+-----+
Fail Login | NEVER                  H N/A      | N/A
-----+-----+-----+-----+
# Fail Att | 0                            H N/A      | N/A
-----+-----+-----+-----+
GraceLogins| N/A                          H N/A      | N/A
-----+-----+-----+-----+
Acct Lock? | No                          H 10-May-2001 17:00 | N/A
-----+-----+-----+-----+
Expiration | N/A                        H 10-May-2001 17:01 | N/A
-----+-----+-----+-----+

Group      Unix      Local      Parent
=====
auditors   Yes       No         No
bin        Yes       No         No
edi_usrs   Yes       No         No
staff      Primary  No         No
users      Yes       No         No

Autosecure is Installed and Configured.
  Local SeOS up?: Yes
  Parent SeOS up?: Yes

----- Analysis -----

Account restrictions exist for this account. Please review the restrictions
listed in the chart above and determine if they may be the cause of the
problem.

This account has is suspended. See chart above to determine if this
is the cause of the call. If it is then remind the user of this situation
before removing the suspension with the following commands.
NOTE: Please ensure the account should not be suspended before preceeding.
  host hp_edip@bdhp4176
  chusr t8000 suspend-

Remove the suspension (Yes or No) [N]? █
```

Figure 8. Account is suspended output

Account is Expired

An account can become expired if the password has not been changed within the specified time period or if an administrator manually expires the account. The program will prompt to remove the expiration date or not. Figure 9 shows the output.

```

Telnet - bdhp4172
Connect Edit Terminal Help

The parent policy model database for bdhp4172 is hp_edip@bdhp4176.
Gathering user information ...
    ... from standard UNIX files
    ... from tcb files
    ... from local AutoSecure policy model
    ... from parent AutoSecure policy model

User summary for tg5524.
  Name: DAVID MARTIN /DM/3,TR-60 CINCINNATI 60,513-983-0102
  Home Dir: /home/tg5524 Owner: tg5524 Perms: drwxr-xr-x
  Shell: /usr/bin/sh

=====
| bdhp4172 | tcb | H Local PMDB | hp_edip@bdhp4176 | | |
| ID exists? | Yes | Yes | H Yes | Yes |
| UID # | 5030 | 5030 | H N/A | N/A |
| Primary Grp | 392 - staff | ^ | H N/A | staff |
| Pwd Intrvl | N/A | N/A | H Default | 40 |
| Pwd Lst Chg | 1-May-2001 17:48 | ^ | H NEVER | 01-May-2001 17:34 |
| Last Login | 2-May-2001 11:04 | H | H NEVER | NEVER |
| Fail Login | 3-May-2001 13:06 | H | H N/A | N/A |
| # Fail Att | 0 | H | H N/A | N/A |
| GraceLogins | N/A | N/A | H | H N/A | N/A |
| Acct Lock? | No | ^ | H | H N/A | N/A |
| Expiration | N/A | H | H 03-May-2001 16:12 | N/A |
=====
Group      Unix      Local      Parent
=====
No         No         No         =====
Autosecure is Installed and Configured.
  Local SeOS up?: Yes
  Parent SeOS up?: Yes

----- Analysis -----
Account restrictions exist for this account. Please review the restrictions
listed in the chart above and determine if they may be the cause of the
problem.

This account has an expiration date. See chart above to determine if this
is the cause of the call. If it is then remind the user of this situation
before removing the account expiration date with the following commands.
Notice that this command will be done at the parent and will propagate to
all subscribed nodes.
  host hp_edip@bdhp4176
  chusr tg5524 expire-

Remove the expiration date (Yes or No) [N]? y
  
```

Figure 9. Account is expired output

5.1.7 Grace Logins Assigned to Zero

Grace logins can reach zero if the password was reset and the user failed to manually change the password. The program will automatically reset the grace logins to five. Figure 10 shows the output of the program.

```

Telnet - bdhp4172
Connect Edit Terminal Help

User summary for ty8000.
  Name: MARK PANZECA /M.,GO/TR SWTC,513-983-6182
Home Dir: /home/ty8000 Owner: ty8000 Perms: drwxr-xr-x
Shell: /usr/bin/ksh

=====
| bdhp4172 | tcb | Local PMDB | hp_edip@bdhp4176 |
=====
ID exists? | Yes | Yes | H Yes | Yes |
=====
UID # | 4755 | 4755 | H N/A | N/A |
=====
Primary Grp | 392 - staff | | H N/A | staff |
=====
Pwd Intrvl | N/A | N/A | H 40 | 40 |
=====
Pwd Lst Chg | 3-Apr-2001 10:36 | | H 03-Apr-2001 10:36 | 03-Apr-2001 10:23 |
=====
Last Login | NEVER | | H NEVER | NEVER |
=====
Fail Login | 8-Mar-2001 16:23 | | H N/A | N/A |
=====
# Fail Att | 1 | | H N/A | N/A |
=====
GraceLogins | N/A | N/A | H 0 | N/A |
=====
Acct Lock? | No | | H N/A | N/A |
=====

Group      Unix      Local      Parent
=====
MONITORING No      Regular    Regular
accadmin   No      Regular    Regular
bin         Yes     Regular    Regular
ecs4       Yes     Regular    Regular
evtnmgt    Yes     Regular    Regular
grpadmin   No      No         Regular
mpcm       Yes     No         No
notes      Yes     Regular    Regular
staff      Primary No         No
users      Yes     Regular    Regular

Autosecure is Installed and Configured.
  Local SeOS up?: Yes
  Parent SeOS up?: Yes

----- Analysis -----
Users grace login count has reached zero and the account is disabled.
The grace login count has been reset to 5. Please instruct the user to login
directly with this ID on bdhp4172 and issue the command 'passwd' to change
the password. The script has already issued the following AutoSecure command
host localhost;chusr ty8000 grace(5)

Do you wish to view the command log file (Yes or No) [N]? █

```

Figure 10. Grace logins assigned to zero output

5.1.8 Account Only Exists in UNIX

If the account only exists in UNIX, it was incorrectly added on the system. Autosecure needs pertinent information; therefore, this cannot be automatically corrected, but it will provide the necessary information. Figure 11 shows the output of the program.

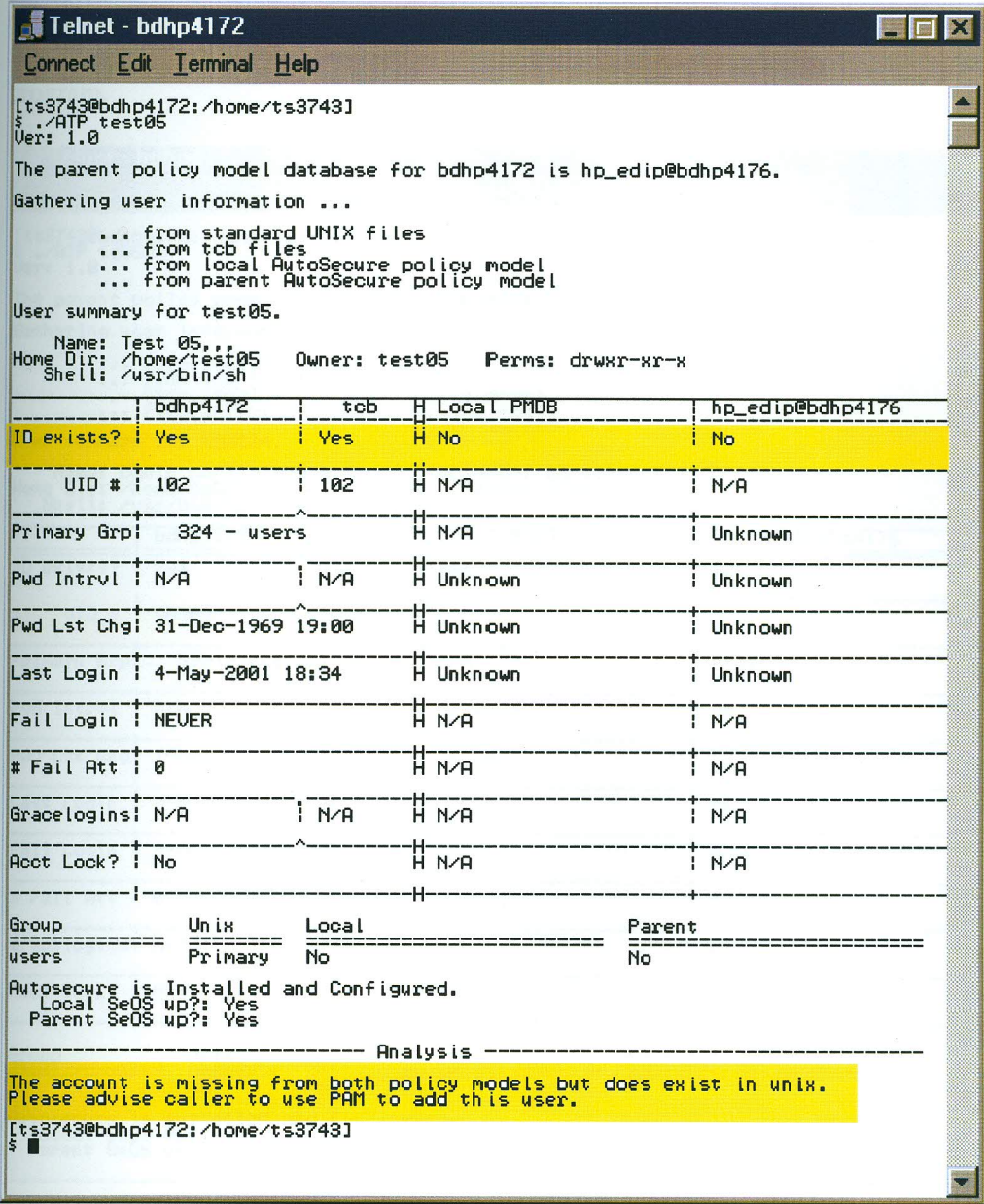
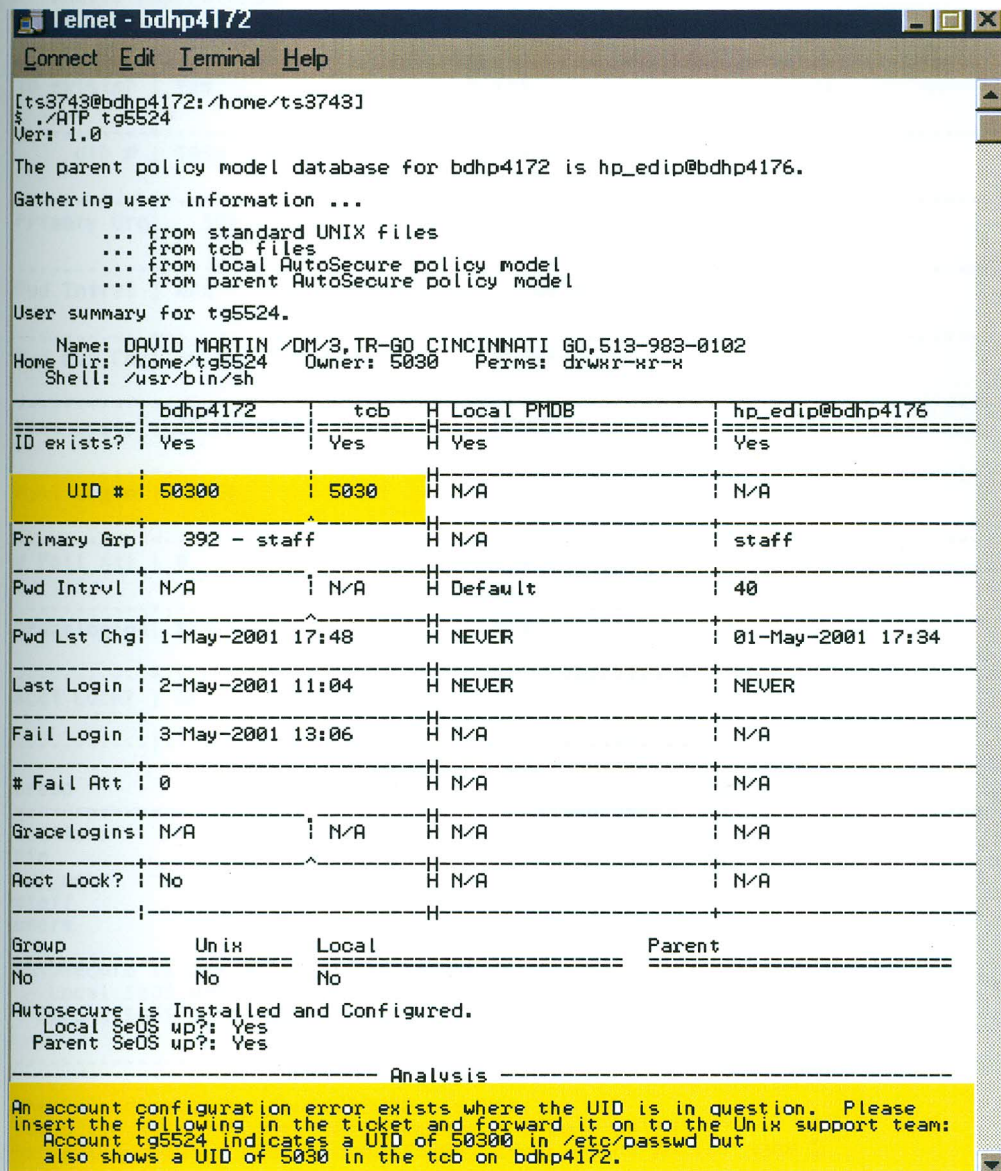


Figure 11. Account only exists in UNIX output

5.1.9 UID Mismatch

The UID mismatch problem arises because user ids are assigned to the user in two files: `/etc/passwd` and `/tcb/files/auth/t/<login id>`. (see *Appendix A & C* for file details).

One of the numbers is correct, but there is no way to know which one, so it cannot be auto-corrected, but the information will be provided. Figure 12 shows the output of the program.



```
Telnet - bdhp4172
Connect Edit Terminal Help

[ts3743@bdhp4172:/home/ts3743]
$ ./ATP tg5524
Ver: 1.0

The parent policy model database for bdhp4172 is hp_edip@bdhp4176.
Gathering user information ...
    ... from standard UNIX files
    ... from tcb files
    ... from local AutoSecure policy model
    ... from parent AutoSecure policy model

User summary for tg5524.
Name: DAVID MARTIN /DM/3,TR-GO CINCINNATI GO,513-983-0102
Home Dir: /home/tg5524 Owner: 5030 Perms: drwxr-xr-x
Shell: /usr/bin/sh

=====
| bdhp4172 | tcb | Local PMDB | hp_edip@bdhp4176 | |
| ID exists? | Yes | Yes | Yes | Yes |
| UID # | 50300 | 5030 | N/A | N/A |
| Primary Grp | 392 - staff | N/A | N/A | staff |
| Pwd Intrvl | N/A | N/A | Default | 40 |
| Pwd Lst Chg | 1-May-2001 17:48 | NEVER | 01-May-2001 17:34 |
| Last Login | 2-May-2001 11:04 | NEVER | NEVER |
| Fail Login | 3-May-2001 13:06 | N/A | N/A |
| # Fail Att | 0 | N/A | N/A |
| GraceLogins | N/A | N/A | N/A | N/A |
| Root Lock? | No | N/A | N/A |
=====
Group      Unix      Local      Parent
=====
No         No         No
Autosecure is Installed and Configured.
Local SeOS up?: Yes
Parent SeOS up?: Yes

----- Analysis -----
An account configuration error exists where the UID is in question. Please
insert the following in the ticket and forward it on to the Unix support team:
Account tg5524 indicates a UID of 50300 in /etc/passwd but
also shows a UID of 5030 in the tcb on bdhp4172.
```

Figure 12. UID mismatch output

5.1.10 Home Directory is Missing

The directory /home/<login id> does not exist. The program gives you the option to create the directory. Figure 13 shows the output of the program.

```
Telnet - bdhp4172
Connect Edit Terminal Help

User summary for t8000.
Name: STEPHEN PETERSON /SJ.F2S16 WHTC.513-634-5724
Home Dir: /home/t8000 - NOT FOUND Owner: Unknown Perms: Unknown
Shell: /usr/bin/sh

=====
ID exists? | Yes | Yes | H Yes | Yes
-----+-----+-----+-----+-----
UID # | 5091 | 5091 | H N/A | N/A
-----+-----+-----+-----+-----
Primary Grp | 392 - staff | H N/A | staff
-----+-----+-----+-----+-----
Pwd Intrvl | N/A | N/A | H Default | Default
-----+-----+-----+-----+-----
Pwd Lst Chg | 28-Apr-2001 20:47 | H NEVER | NEVER
-----+-----+-----+-----+-----
Last Login | 28-Apr-2001 20:47 | H NEVER | NEVER
-----+-----+-----+-----+-----
Fail Login | NEVER | H N/A | N/A
-----+-----+-----+-----+-----
# Fail Att | 0 | H N/A | N/A
-----+-----+-----+-----+-----
Gracelogins | N/A | N/A | H N/A | N/A
-----+-----+-----+-----+-----
Acct Lock? | No | H N/A | N/A
-----+-----+-----+-----+-----

Group      Unix      Local      Parent
=====
auditors   Yes       No         No
bin        Yes       No         No
edi_usrs   Yes       No         No
staff      Primary   No         No
users      Yes       No         No

Autosecure is Installed and Configured.
Local SeOS up?: Yes
Parent SeOS up?: Yes

----- Analysis -----

The home directory, /home/t8000, is missing.
Would you like for the home directory to be created...
Using the command mkdir /home/t8000, chown t8000 /home/t8000
```

Figure 13. Home directory is missing output

5.1.11 Home Directory is Owned by Another ID

The /home/<login id> directory is owned by another ID other than <login id>.

The program gives you the option to change the owner. Figure 14 shows the output.

```
Telnet - bdhp4172
Connect Edit Terminal Help

User summary for t8000.

Name: STEPHEN PETERSON /SJ,F2S16 WHTC,513-634-5724
Home Dir: /home/t8000 Owner: root Perms: drwxr-xr-x
Shell: /usr/bin/sh

=====
ID exists? | Yes | Yes | H Yes | Yes
=====
UID # | 5091 | 5091 | H N/A | N/A
=====
Primary Grp | 392 - staff | 392 - staff | H N/A | staff
=====
Pwd Intrvl | N/A | N/A | H Default | Default
=====
Pwd Lst Chg | 28-Apr-2001 20:47 | 28-Apr-2001 20:47 | H NEVER | NEVER
=====
Last Login | 28-Apr-2001 20:47 | 28-Apr-2001 20:47 | H NEVER | NEVER
=====
Fail Login | NEVER | NEVER | H N/A | N/A
=====
# Fail Att | 0 | 0 | H N/A | N/A
=====
Gracelogins | N/A | N/A | H N/A | N/A
=====
Acct Lock? | No | No | H N/A | N/A
=====

Group      Unix      Local      Parent
=====
auditors   Yes       No         No
bin        Yes       No         No
edi_usrs   Yes       No         No
staff      Primary   No         No
users      Yes       No         No

Autosecure is Installed and Configured.
Local SeOS up?: Yes
Parent SeOS up?: Yes

----- Analysis -----

The home directory, /home/t8000, is owned by root
instead of t8000. The ownership can be changed by issuing the command
chown t8000 /home/t8000. Would you like to change the ownership? [N]
```

Figure 14. Home directory is owned by another ID output

Account Exists in Autosecure, not UNIX

The account does not exist in UNIX. It will be prompted to automatically add.

Figure 15 shows the output of the program.

```
Telnet - bdhp4172
Connect Edit Terminal Help
[ts3743@bdhp4172:/home/ts3743]
$ ./ATP td0231
Ver: 1.0
The parent policy model database for bdhp4172 is hp_edip@bdhp4176.
Gathering user information ...
... from standard UNIX files
... from local AutoSecure policy model
... from parent AutoSecure policy model
User summary for td0231.
Name: NONE
(From information at parent PMDB)
Home Dir: /home/td0231 Owner: 7583 Perms: drwxr-xr-x
Shell: NONE
```

	bdhp4172	tcb	Local PMDB	hp_edip@bdhp4176
ID exists?	No	No	Yes	Yes
UID #	NONE	NONE	N/A	N/A
Primary Grp	NONE - NONE		N/A	staff
Pwd Intrvl	N/A	N/A	Default	40
Pwd Lst Chg	NEVER		NEVER	NEVER
Last Login	NEVER		NEVER	NEVER
Fail Login	NEVER		N/A	N/A
# Fail Att	0		N/A	N/A
GraceLogins	N/A	N/A	N/A	N/A
Acct Lock?	N/A		N/A	N/A

Group	Unix	Local	Parent
bin	No	Regular	Regular
evtmgt	No	Regular	Regular
users	No	Regular	Regular

```
Autosecure is Installed and Configured.
Local SeOS up?: Yes
Parent SeOS up?: Yes

----- Analysis -----
The account exists at both policy models but not in unix.
The following AutoSecure commands will be issued to correct this situation
by adding the account at the unix level.
host localhost
env unix
newusr td0231 homedir('/home/td0231') shellprog('/bin/sh') pgroup('staff') g
ecos('JAN DOBBENIE /J., 60-TR CINCINNATI 60,1-513-983-1992') userid(7583)
join td0231 group(bin)
join td0231 group(evtmgt)
join td0231 group(users)
Continue adding the account (Yes or No) [N]? █
```

Figure 15. Account exists in Autosecure, not UNIX

5.1.12 Account Exists in UNIX and Autosecure Parent, not Local

The account exists on the UNIX level and partially in Autosecure. It does not exist in Autosecure on the local host. The program will prompt for the addition and automatically add. Figure 16 shows the output of the program.

```

Telnet - bdhp4172
Connect Edit Terminal Help
... from standard UNIX files
... from tcb files
... from local AutoSecure policy model
... from parent AutoSecure policy model

User summary for td0231.
Name: JAN DOBBENIE /J.,GO-TR CINCINNATI GO,1-513-983-1932
Home Dir: /home/td0231 Owner: td0231 Perms: drwxr-xr-x
Shell: /bin/sh

```

	bdhp4172	tcb	Local PMDB	hp_edip@bdhp4176
ID exists?	Yes	Yes	No	Yes
UID #	7583	7583	N/A	N/A
Primary Grp	392 - staff		N/A	staff
Pwd Intrvl	N/A	N/A	Unknown	40
Pwd Lst Chg	NEVER		Unknown	NEVER
Last Login	NEVER		Unknown	NEVER
Fail Login	NEVER		N/A	N/A
# Fail Att	0		N/A	N/A
GraceLogins	N/A	N/A	N/A	N/A
Root Lock?	Yes, passwd is '*'		N/A	N/A

Group	Unix	Local	Parent
bin	Yes	No	Regular
evtmgt	Yes	No	Regular
staff	Primary	No	No
users	Yes	No	Regular

```

Autosecure is Installed and Configured.
Local SeOS up?: Yes
Parent SeOS up?: Yes

----- Analysis -----

The account exists at the parent policy model and in the unix files
but not at the local policy model. The following AutoSecure commands will
be issued to correct this situation by adding the account to the local
policy model.
host localhost
newusr td0231 owner(nobody)
chusr td0231 audit(Failure, LoginFailure)
chusr td0231 name('JAN DOBBENIE /J.,ETC-BRU-EDC,32-2-4564942,')
join td0231 group(bin)
join td0231 group(evtmgt)
join td0231 group(users)

Continue adding the account (Yes or No) [N]? yes

In order to synchronize the user's password on this node with the one
found at the parent PMDB you should login to bdhp4176 and type
sync_pw td0231 bdhp4172 hp_edip

```

Figure 16. Account exists in UNIX and Autosecure parent, not local

5.1.13 Account Exists at the Autosecure Parent Only

The account does not exist on the local host in Autosecure or UNIX. The program will prompt for automatic correction. Figure 17 shows the output of the program.

```
Telnet - bdhp4172
Connect Edit Terminal Help

... from standard UNIX files
... from local AutoSecure policy model
... from parent AutoSecure policy model

User summary for ty8000.
Name: NONE
(From information at parent PMDB)
Home Dir: /home/ty8000 Owner: 4755 Perms: drwxr-xr-x
Shell: NONE
```

	bdhp4172	tcb	Local PMDB	hp_edip@bdhp4176
ID exists?	No	No	No	Yes
UID #	NONE	NONE	N/A	N/A
Primary Grp	NONE - NONE		N/A	staff
Pwd Intrvl	N/A	N/A	Unknown	40
Pwd Lst Chg	NEVER		Unknown	03-Apr-2001 10:23
Last Login	NEVER		Unknown	NEVER
Fail Login	NEVER		N/A	N/A
# Fail Att	0		N/A	N/A
GraceLogins	N/A	N/A	N/A	N/A
Acct Lock?	N/A		N/A	N/A

```
Group      Unix      Local      Parent
=====
MONITORING No        No         Regular
accadmin   No        No         Regular
bin        No        No         Regular
ecs4       No        No         Regular
evtmgt     No        No         Regular
grpadmin   No        No         Regular
notes      No        No         Regular
users      No        No         Regular

Autosecure is Installed and Configured.
Local SeOS up?: Yes
Parent SeOS up?: Yes

----- Analysis -----

The account exists only at the parent policy model. The following AutoSecure
commands will be issued to correct this situation by adding this account to the
local policy model and at the unix level.
host localhost
newusr ty8000 owner('nobody') unix(gecos('MARK PANZECA /M.,GO/TR SWTC,513-98
3-6182') homedir(/home/ty8000) shellprog(/usr/bin/ksh) pgroup(staff) userid('475
5'))
chusr ty8000 audit(Failure, LoginFailure)
chusr ty8000 name('MARK PANZECA /M.,TR-GO,513-983-0498,')
join ty8000 group(MONITORING) unix
join ty8000 group(accadmin) unix
join ty8000 group(bin) unix
join ty8000 group(ecs4) unix
join ty8000 group(evtmgt) unix
join ty8000 group(grpadmin) unix
join ty8000 group(notes) unix
join ty8000 group(users) unix
join ty8000 group(staff) unix

Continue adding the account (Yes or No) [N]? █
```

Figure 17. Account exists at the Autosecure parent only

5.1.14 Primary Group does not Exist

The user's ID is assigned to a primary group that does not exist in the `/etc/group` file (See Appendix A for the `/etc/group` file). Figure 18 shows the output of the program.

```
Telnet - bdhp4172
Connect Edit Terminal Help

[ts3743@bdhp4172:/home/ts3743]
$ ./ATP tg5524
Ver: 1.0

The parent policy model database for bdhp4172 is hp_edip@bdhp4176.
Gathering user information ...
... from standard UNIX files
... from tcb files
... from local AutoSecure policy model
... from parent AutoSecure policy model

User summary for tg5524.
Name: DAVID MARTIN /DM/3,TR-GO CINCINNATI 60,513-983-0102
Home Dir: /home/tg5524 Owner: tg5524 Perms: drwxr-xr-x
Shell: /usr/bin/sh
```

	bdhp4172	tcb	Local PMDB	hp_edip@bdhp4176
ID exists?	Yes	Yes	H Yes	Yes
UID #	5030	5030	H N/A	N/A
Primary Grp	337 - Not found		H N/A	staff
Pwd Intrvl	N/A	N/A	H Default	40
Pwd Lst Chg	1-May-2001 17:48		H NEVER	01-May-2001 17:34
Last Login	4-May-2001 13:37		H NEVER	NEVER
Fail Login	3-May-2001 13:06		H N/A	N/A
# Fail Att	0		H N/A	N/A
Gracelogins	N/A	N/A	H N/A	N/A
Acct Lock?	No		H N/A	N/A

```
Group      Unix      Local      Parent
=====
No         No         No

Autosecure is Installed and Configured.
Local SeOS up?: Yes
Parent SeOS up?: Yes

----- Analysis -----

A group seems to be missing or there is a configuration error with this
account. Please insert the following lines and forward the ticket to the
Unix support team.
Account tg5524 indicates a primary group # of 337
which does not exist in /etc/group on bdhp4172.

[ts3743@bdhp4172:/home/ts3743]
```

Figure 18. Primary group does not exist output

5.1.15 Account Information is not Consistent

Problems appear with the account and it is partially configured. No automatic actions can be taken to correct the problem, but the program will provide the information that the account should be analyzed. Figure 19 shows the output of the program.

```
Telnet - bdhp4172
Connect Edit Terminal Help
The parent policy model database for bdhp4172 is hp_edip@bdhp4176.
Gathering user information ...
... from standard UNIX files
... from tcb files
... from local AutoSecure policy model
... from parent AutoSecure policy model
User summary for t8000.
Name: STEPHEN PETERSON /SJ,F2S16 WHTC,513-634-5724
Home Dir: /home/t8000 Owner: t8000 Perms: drwxr-xr-x
Shell: /usr/bin/sh
```

	bdhp4172	tcb	Local PMDB	hp_edip@bdhp4176
ID exists?	Yes	Yes	H No	No
UID #	5091	5091	H N/A	N/A
Primary Grp	392 - staff		H N/A	staff
Pwd Intrvl	N/A	N/A	H Unknown	Unknown
Pwd Lst Chg	28-Apr-2001 20:47		H Unknown	Unknown
Last Login	28-Apr-2001 20:47		H Unknown	Unknown
Fail Login	NEVER		H N/A	N/A
# Fail Att	0		H N/A	N/A
GraceLogins	N/A	N/A	H N/A	N/A
Acct Lock?	No		H N/A	N/A

Group	Unix	Local	Parent
auditors	Yes	No	No
bin	Yes	No	No
edi_usrs	Yes	No	No
staff	Primary	No	No
users	Yes	No	No

```
Autosecure is Installed and Configured.
Local SeOS up?: Yes
Parent SeOS up?: Yes

----- Analysis -----
This account's configuration is quite confused and it cannot be corrected with
this script. Please forward this ticket on to the Unix support team for
resolution with the following text:
Account t8000 is partially configured in unix on bdhp4172
and at the parent policy model, hp_edip@bdhp4176.

[ts3743@bdhp4172:/home/ts3743]
```

Figure 19. Account is quite confused output

5.1.16 GUI Interface

It is possible to connect to an NT server via CITRIX Client and then connect to a UNIX System using HP Openview for a GUI Interface. Figure 20 shows the connection to the NT CITRIX Server, Figure 21 shows the GUI Interface, Figure 22 shows the Execution run, and Figure 23 shows the program output.

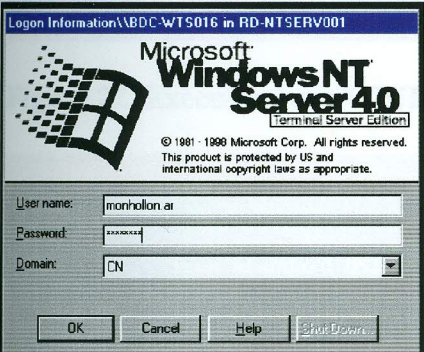


Figure 20. Connection to NT CITRIX Server

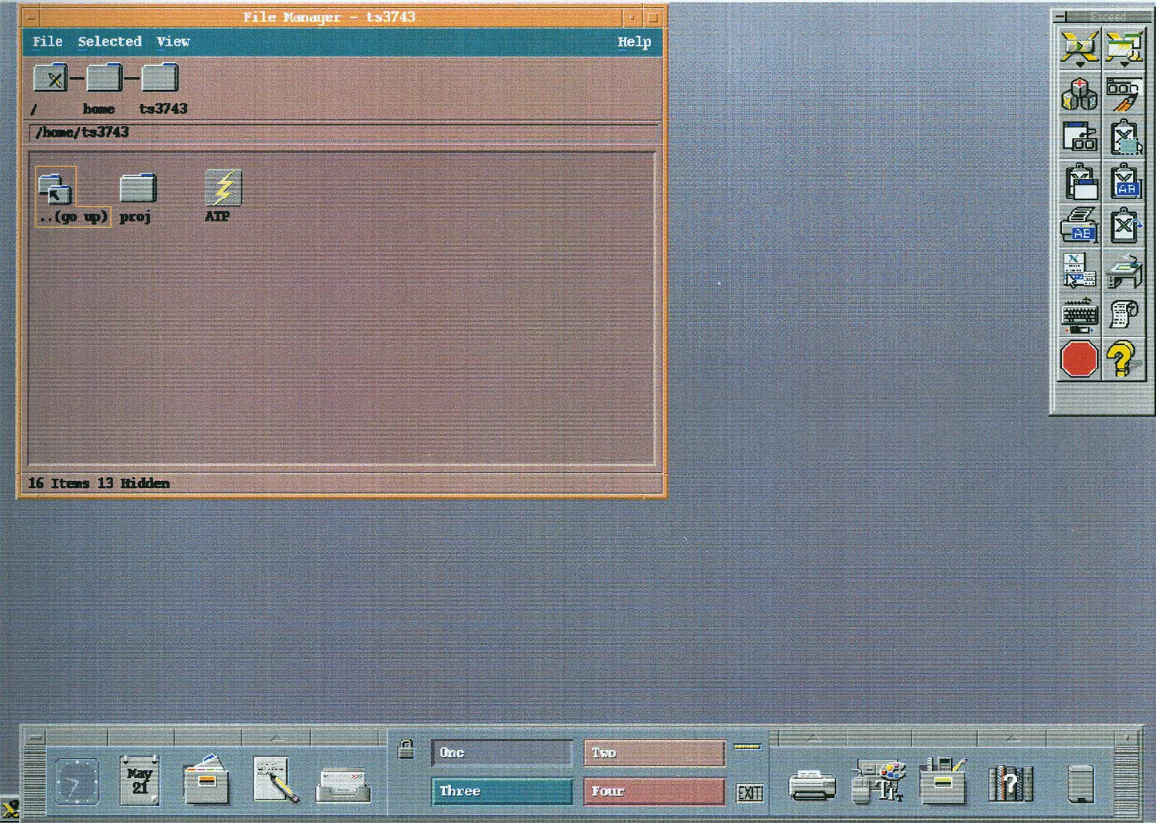


Figure 21. GUI Interface

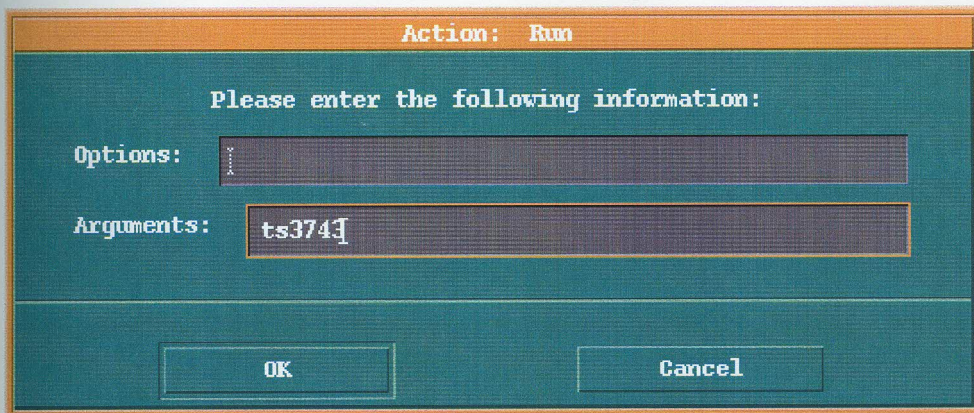


Figure 22. Execution run (GUI Interface)

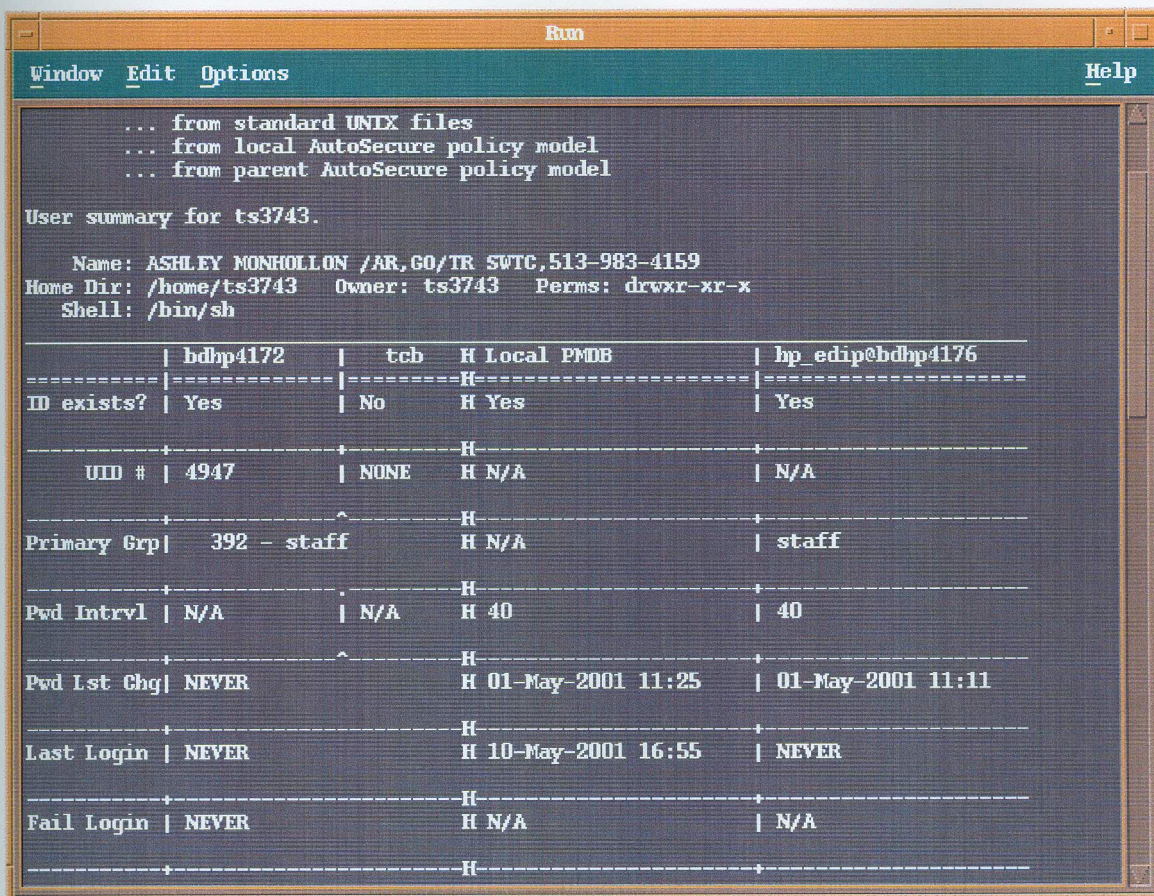


Figure 23. Program output (GUI Interface)

6. Conclusions

System Administrators spend numerous hours detecting and correcting UNIX user account problems. The installation of the software package, Autosecure, has been installed on all the UNIX Midrange systems in attempt to increase security and manageability. With the installation of Autosecure, account problems have increased dramatically. The details and specifics were described in the *Statement of Problem and Definition of Need* Section.

This document discussed the aspects of design and implementation necessary in the development of an Account Troubleshooting Program. The project's purpose is to eliminate unnecessary time spent manually correcting and searching for UNIX user account problems. The program has been designed to immediately detect the problems associated with user accounts and if possible, automatically correct the problems.

The program was tested successfully and proved beneficial to correcting and eliminating problems. The structure, design, flow, and management of the UNIX Account Troubleshooting Program was explained in detail. This document includes the *Problem and Solution*, in terms of program design, as well as user and operator characteristics. The deliverables, budget, timeline, software, and hardware were discussed in the *Design and Development* Section. The *Proof of Design* section detailed the specifics of the program, identified all possible problems, detailed an algorithm for resolution, and demonstrated execution of the program.

7. Recommendations

In the future, before implementing a new feature into production, it needs to be fully tested in attempt to identify possible problems created by the change. This was not the case with the installation of Autosecure. Too much effort and time has been wasted attempting to correct problems resulting from the change. I would have created the program sooner in attempt to save time faster.

Another recommendation is to create Validation Scripts to identify configuration problems as a whole. I am currently in the process of writing a script to look at all the home directories on the system, permissions, and ownerships. These problems will be corrected one by one so they do not appear in daily troubleshooting. This is an attempt to be more proactive with resolution.

Another possibility and recommendation is to incorporate a JAVA GUI interface and possibly allow execution from the Intranet. This will take time and energy, but is a long-term goal for the project.


```

root::0:3::/root:/sbin/sh
daemon:*:1:5:::/sbin/sh
bin:*:2:2::/usr/bin:/sbin/sh
sys:*:3:3::/
adm:*:4:4::/var/adm:/sbin/sh
uucp:*:5:3::/var/spool/uucppublic:/usr/lbin/uucp/uucico
lp:*:9:7::/var/spool/lp:/sbin/sh
nucp:*:11:11::/var/spool/uucppublic:/usr/lbin/uucp/uucico
hpldb:*:27:1:ALLBASE:/sbin/sh
nobody:*:-2:-2::/
www:*:30:368::/
tb0815:*:194:392:FREDERIC GOUSSAULT /F., ETC H 102 ETC 32-2-456-2138:/home/tb0815:/bin/ksh
tr5305:*:4750:392:ALISSA COLVIN /AL, GO IN-10 CINCINNATI GO, /home/tr5305:/usr/bin/ksh
tl3835:*:4753:392:GREG ROESL /GB, GO TR SWTC, 513-626-1557:/home/tl3835:/usr/bin/ksh
tl5567:*:4754:392:HERBERT CARRERA /HJ, GO-TR CINCINNATI GO, 513-983-8594:/home/tl5567:/usr/bin/ksh
tr5304:*:4756:392:TONYA JENKINS /TM, GO-TR CINCINNATI GO, /home/tr5304:/usr/bin/ksh
oi3:*:4758:326:oi3 USER - EMERGENCY C/O Alissa Lane:/home/oi3:/usr/bin/ksh
tl3869:*:4759:392:TOM BORTOLOTTO /TJ, TR-60 CINCINNATI GO, 513-983-9418:/home/tl3869:/usr/bin/ksh
tu4860:*:4761:392:TOM BORCHER /TA/2 KEANE, SB1-3J4 HCRC MASON, C/O COFFEY/PM 513-622-0000:/home/tu4860:/usr/bin/ksh
t4096:*:4766:392:CHERRIE WAMPLER /CS, GO-TR SWTC, 513-983-2917:/home/t4096:/usr/bin/ksh
tr5303:*:4769:392:GREG BEYZ /GB, CEC-9 CINCINNATI GO, 513-945-8987:/home/tr5303:/usr/bin/ksh
tu2404:*:4770:392:R ROBBINS /RR/2, GO CINCINNATI GO, 513-983-6211:/home/tu2404:/bin/sh
t0107:*:4773:341:DALE TRONE /DA, GO-TERRACE CINCINNATI GO, 513-983-8514:/home/t0107:/bin/sh
t0115:*:4774:392:BILL TELFORD /WJ, GO-TR CINCINNATI GO, 513-983-0245:/home/t0115:/bin/sh
tl283:*:4775:392:NANCY REDWINE /NL, TC0C-TC2020 SWTC, 513-626-8253:/home/tl283:/bin/sh
tl664:*:4776:392:WAYNE FISCHER /WA, GO TR CINCINNATI GO, 513-945-7266:/home/tl664:/bin/sh
t3103:*:4777:392:DARLA LEARY /DG, GO-TR CINCINNATI GO, 513-983-3480:/home/t3103:/bin/sh
th1176:*:4779:392:JOHAN DEBORGER /JT, ETC H 2 ETC 32-2-456-2553:/home/th1176:/bin/sh
tk7597:*:4782:392:DAVID TAYLOR /TB, GO TR CINCINNATI GO, 513-983-5512:/home/tk7597:/bin/sh
tn0289:*:4786:392:JOEL CLARK /JA ORIGIN, C-09 CINCINNATI GO, C/O GENBAUFFE/MB 513-983-0498:/home/tn0289:/bin/sh
tn9685:*:4788:392:SUE YU /S./4 DVL-156 HCRC MASON, 513-622-0029:/home/tn9685:/bin/sh
tp5682:*:4789:392:LARRY MARTINI /LW, GO/TR CINCINNATI GO, 513-983-6204:/home/tp5682:/bin/sh
tu5524:*:4795:392:STEPHEN TURCOTTE /S./GO/TR CINCINNATI GO, 513-983-6217:/home/tu5524:/bin/sh
tu9933:*:4796:392:ROBERT MCFARLAND /RS, GO-TR CINCINNATI GO, 513-983-8593:/home/tu9933:/bin/sh
ty6748:*:4798:392:ANTONIO MERCADO /GA, GO-TR CINCINNATI GO, 513-983-6205:/home/ty6748:/bin/sh
ty6749:*:4799:392:NIKOLAUS DILGER /N./GO CINCINNATI GO, 513-983-6888:/home/ty6749:/bin/sh
ti0224:*:4803:392:STEFAN FORCEVILLE /S./ETC H 2 ETC 32-2-456-2779:/home/ti0224:/bin/sh
tr3117:*:4804:392:HELENA YIN /YH, SINGAPORE SINGAPORE GO, /home/tr3117:/bin/sh
ts4179:*:4807:392:JOANNEY YAO /JO/2, HUANGPU PLANT, X-922-2273:/home/ts4179:/bin/sh
ts4200:*:4809:392:NAUREEN SID /NM./2 ORIGIN, SINGAPORE GO, C/O PUAY/S./:/home/ts4200:/bin/sh
ts4166:*:4811:392:DAMIEN KHOO /D./ORIGIN, SINGAPORE GO, C/O PUAY/S./:/home/ts4166:/bin/sh
ts4167:*:4815:392:SINGHAR GAN /SH ORIGIN, SINGAPORE GO, C/O PUAY/S./:/home/ts4167:/bin/sh
t5706:*:4818:392:ROSE WEIL /RM, TR-60 CINCINNATI GO, 513-983-8456:/home/t5706:/bin/sh
th7716:*:4819:392:ROB WOLFE /RB, GO-TR CINCINNATI GO, 513-983-7803:/home/th7716:/bin/sh
tn3254:*:4820:392:RON BROOKS /RL, TR-60 CINCINNATI GO, 513-983-0498:/home/tn3254:/bin/sh
ti0625:*:4821:392:MARC COP /MC./GO-TR CINCINNATI GO, 513-983-2016:/home/ti0625:/bin/sh
tx0118:*:4823:392:PATRICK VERBRUGEN /P./COMPR, ETC H 2 ETC, C/O DEBORGER/JT 32-2-456-2469:/home/tx0118:/bin/sh

```



```

Window Edit Options Terminal Help

root::0:root
other::1:root,hpdd, tr3118, ti6045, tm1057, ilbnce, ti6488, ti4385, filter, tk0000, ab0975, ts5103, tp9058, ty2256, tg9852, t3632, tr8105, te0716, tg9124,
tj4453, harvest, tj1357, te8726, te7517, te0910, tr7823, adm, alprod, alitest, tq8254, tv5752, tn2777, ti4377, pamadm, tm0185, tw8722, ti2497, t4264, aa2972
, ab6800, aa9229

bin::2:root,bin, th0815, tr5305, tv3606, tl3835, ae4196, tr5304, oi3, tl3869, ac1416, tu4860, aa0968, ac4207, tf1143, t4096, ab9249, tr5303, tu2404, ac158
6, t0107, tl1664, th1176, tm0289, tn9685, tp5682, tx5013, tu5524, tn9933, tt4040, tr3329, ti0224, tx3117, t3103, tn3254, tx0118, aa0190, tq30
38, controlm, tl3490, tl172, tx0181, tx4197, tx0120, tc3241, td0088, ti0246, tx0123, tx0132, tx0183, ossgd, tl4172, filemgr, ti0631, u0972, entsys,
wpcw, tp6143, ae1918, tv4040, tl2926, ab0975, ts8856, tn9760, tk7597, ecsop, ts3743, tj1696, tm4619, tr9498, tq2649, tr3118, tj3691, tq4097, u2568, tj5908,
tx0224, tf5407, tf5409, ctms, t0557, tx0180, tv0565, ab2554, tm3879, tj19672, tn9672, ac0924, tx0230, tx0924, tx7839, qnc, op, u2551, tj1749, tq8254, tm0823, tm0151,
aa2972, tj5462, tj7921, tj3287, tv7921, u7565, tr7823, hpre, tv7328, t8000, tu2303, tx0924, tx7839, qnc, op, u2551, tj1749, tq8254, tm0823, tm0151,
u2571, tv5752, tl3880, tv2777, pamadm, perf, ab6115, ae4317, harvest, tv5297, tf8403, ti4385, tp3844, tk5027, tk1444, th7716, tx0238, aa2566, tf0451, ab611
9, ts5103, tr2561, tp4768, tm0185, tv1787, tm2295, tv9964, ad4027, PERFI0A, ab6800, ac2056, t1894, tq5009, aa9288, ab8655, ae7047, th3725, ty8000

sys::3:root,wcp, bin, sys, rootswp
adm::4:root, adm, bin

daemon::5:root, daemon
mail::6:root
lp::7:root, lp
nsgroup:*:-2:
audit::10:root

secdm::204:root, tf5544, ac3784, aa9229, tr3117, ti0882, tf5407, adm, aa7683, t4096
auditors::305:root, te0716, tr5303, th1176, ti0224, ti0625, tx0118, t8000, ti0882, tx0120

SUPERGR::306:

XEHARGE::307:tg7992, ts9802, tx0224, th0038, ac5003, perfwork
CONTROL::310:ad3151, tu5524, ts4200, ts4166, ab3324, ts4390, ts4167, aa4687, tn3254, tx0004, tx0208, tx0229, EDC0P1, ac1415, tx0017, tq4097, tx0079, tx01
12, tx0117, tx0138, tx0189, tx0193, tx0202, tx0207, tv3606, tx0230, tx0237, tx0241, tj6284, ts3743, ae1918, tv2881, tf6137, tr7995, tf6136, tf6138, ae1917,
ac3807, ac1511, tj5462, tg5524, tq8228, tf7997, ad3474, ts2159, tj4453, adm, ti3523, ti6045, ti6488, ti8982, ae7047, ae1916, tj7480, aal439, ac0525, aa2566
, u2571, ac1512, ac1510, aa5114, ac1513, tx0238, ae4317, ad3486, tf0451, tf6212, ts5103, tx2561, tp4768, tm0185, tv1787, tm2295, aa9655, tm4619, tk7597, ab2
635, aa0127, tt4166

acctadm::312:tl3835, tr5304, tl3869, tu4860, ab6115, tq8228, aal809, t4096, ac3110, tr5303, tn9685, tr3117, ts4200, ts4166, ab3324, ac1512, ts4167, aa46
87, tl3490, tx0017, tx0117, ae7047, tq4097, tq5143, ac5354, tj5908, tx0224, tt4166, ad3486, t0557, tg5524, tf9109, tq4509, ac4253, tl8835, tc9497, ti6488, a
d3474, ad3151, ti4385, ti8982, tj6284, tx5947, ac3807, tj7480, aal439, ts4390, ac1415, u2571, tx0229, ac1513, aa5114, ac1586, ac1511, ac0525, tz8920, ac151
0, tf6212, ac3536, tn9964, aa9655, tn4619, tx0208, tz3727, ab2635, ts2159, tx0189, tv3606, ae1917, ae1916, aa3208, ty8000

nolopin::313:controlm, ecs0, EGS010A, ecs3, EGS310A, trng, TRNG10A, mpcm, ecs4, ecs8, ubkp, EGS810A, harvest, ecsop, perfwork, slos, SI0S10A, ctm
s, cTma, PERFI0A, itsv, ITSV10A, perf, UBXPI0A, oi3, secu, filemgr, tv3606
admin::315:tt2540, tc9497, ti0327

controlm::316:tl0107, ac4253, t5706, aa2972, tk1444, controlm, tl172, ab8655, ti0327, EGS010A, EGS310A, tx0138, tm0823, MPCMI0A, tx0123, u2567, ab0720, ec
s4, GATIEWAY, aa9288, ab0975, t0718, ecs8, EGS410A, EGS810A, ecsop, th9150, tj3691, aa0968, ctms, tq8254, ab6800
dba::200:tx0004, tx4127, tg3038, tx0211, tx0208, ac7762

extwgt::319:root, th0815, tr5305, tj5462, tl3835, ae4196, tr5304, tl3869, tu4860, ab3329, tr8403, tf1143, t4096, ab2554, tr5303, tm2404, pamadm, t0107, t1
664, t3103, th1176, tm0289, tn9685, tp5682, tq4509, tm5524, tn9933, tv6749, ti0224, tr3117, tk1444, th7716, tx3254, tx0118, tv3606, tg3038, control
m, tl3490, tl172, tx0181, tx0138, tx0120, tc3241, td0088, ti0246, tx0123, tx0132, EDC0P1, tx0183, ossgd, tl4172, aa2566, ab9249, u2567, tg5143, ab61
19, tv4040, entsys, ts8856, tn9760, tk7597, ecsop, ts3743, tj1696, tm4619, th6963, tr9498, tr3118, tj3691, tq4097, tj5908, tx0224, tf5407, t0557, tx
0180, aa2972, t0718, tm3879, tl9672, tn9964, tk0780, ty6923, td0231, tg5524, tf9109, tv9830, td772, ab6800, tj3287, tg9124, u7565, bin, hpre, tv7328, tv0924
, tr7839, tj1749, tm0823, tm0151, u2571, tl3880, tm2777, th9150, ti2497, harvest, tv5297, tj4385, tx0238, tf0451, ac1416, ts5103, tx2561, tp4768, tm0185, tv
1787, tm2295, aal809, t1894, tq5009, aa9288, ab8655, aa0190, aa0968, ab0975, tx5013, ae7047, aa9649, ty8000
tty::322:

ubkp::323:tl0107, ti0224, t5706, ti0625, tg3038, tl172, tx0181, aa9288, tc3241, ti0246, ti0615, tx0104, tx0123, tx0132, ab8655, tv4040, tv9760, ubkp, tk144
4

```



```

Window Edit Options Terminal Help
[ root@bdhp4172: /tcb/files/auth ]
# cd t
[ root@bdhp4172: /tcb/files/auth/t ]
# more tg5524
tg5524:u_name=tg5524:u_id#5030:\
:u_pwd=QMbT/iK50Xn/U:\
:u_auditid#231:\
:u_auditflag#0:\
:u_suclog#988753731:u_suclog#988815847:u_suctty=pts/tb:u_umsuclog#988909618:\
:u_umsuctty=pts/tb:u_lock@:chkent:

[ root@bdhp4172: /tcb/files/auth/t ]
# more ts3743
ts3743:u_name=ts3743:u_id#4947:\
:u_pwd=N7tro9XYzr8hg:\
:u_auditid#172:\
:u_auditflag#0:\
:u_suclog#988730752:u_suclog#988908949:u_suctty=pts/ta:u_umsuclog#988908940:\
:u_umsuctty=pts/ta:u_lock@:chkent:

[ root@bdhp4172: /tcb/files/auth/t ]
# more ty8000
ty8000:u_name=ty8000:u_id#4755:\
:u_pwd=*\
:u_auditid#583:\
:u_auditflag#0:\
:u_lock@:chkent:

[ root@bdhp4172: /tcb/files/auth/t ]
# more tn3254
tn3254:u_name=tn3254:u_id#4820:\
:u_pwd=ye0k3nZ/slJy6:\
:u_auditid#68:\
:u_auditflag#0:\
:u_suclog#978624154:u_lock@:chkent:

[ root@bdhp4172: /tcb/files/auth/t ]
# more t8000
t8000:u_name=t8000:u_id#5091:\
:u_pwd=37NV020LRtroA:\
:u_auditid#279:\
:u_auditflag#0:\
:u_suclog#988505279:u_suclog#988505256:u_suctty=pts/tb:u_lock@:\
:chkent:

[ root@bdhp4172: /tcb/files/auth/t ]
#

```



```

Window Edit Options Terminal Help

Updated by : ts3743
Comment   : ASHLEY NONHOLLON /AR, 60/TR SWTC, 513-983-4159
Phone     : 513-983-4159
Location  : 60/TR SWTC

Se0S> su ts3743 unix
(Localhost)
Data for USER 'ts3743'

-----
Audit mode : Failure, Login-Failure
Group connections:
Group      Owner      Date      Time      Type
CONTROL    tr5305    21-Oct-1999 20:02 Regular
OCT_root   tx0224    28-Sep-2000 11:45 Regular
accadmin   bin       21-Oct-1999 20:02 Regular
bin        tr5305    21-Oct-1999 20:02 Regular
ecs4       21-Oct-1999 20:02 Regular
evtmgt     21-Oct-1999 20:18 Regular
gpadmin    21-Oct-1999 20:02 Regular
mpcm       21-Oct-1999 20:02 Regular
notes      21-Oct-1999 20:02 Regular
users      tr5305    21-Oct-1999 20:02 Regular

Owner      : tr5305
Pwd last change : 01-May-2001 11:25
Password interval : 40
Full name    : ASHLEY NONHOLLON /AR
Last accessed : 155.118.61.142
Last access time : 04-May-2001 15:21
Create time   : 21-Oct-1999 17:59
Update time   : 01-May-2001 11:25
Updated by    : ts3743
Comment       : ASHLEY NONHOLLON /AR, 60/TR SWTC, 513-983-4159
Phone        : 513-983-4159
Location     : 60/TR SWTC

(Localhost)
Unix :
=====
Data for USER 'ts3743'
-----
User id      : 4947
Primary group : staff
Group id     : 392
Shell program : /bin/sh
Home directory : /home/ts3743
Gecos       : ASHLEY NONHOLLON /AR, 60/TR SWTC, 513-983-4159

Se0S>

```


References

Books

Stevens, Richard. *Advanced Programming in the UNIX Environment*. Chicago, Illinois: Academic Press, 1996.

Montgomery, John. *The Underground Guide to UNIX*. Reading, Massachusetts: Addison-Wesley Publishing, 1995.

Holsberg, Pete and Armstrong, James C. *UNIX Unleashed*. New York: SAMS Publishing, 1994.

Web Page

Author unknown. "Free Country Web Page".

[Http://www.thefreecountry.com/developercity/unixbook.html](http://www.thefreecountry.com/developercity/unixbook.html). October 4, 2000.

Other

Hewlett Packard Education Course H4322S, Shell Programming.

- 5 day course covering advanced shell programming for technical users and system administrators. Teaches the tools necessary to automate complex tasks and increase productivity.

Project Expert Resources

Dr. Sam Geonetta

Dr. Hazem Said