BoKS Administration

Version 4.0

Dynamic Software AB

Trademarks UNIX® is a registered trademark of AT&T
DEC® is a registered trademark of Digital Equipment Corporation.
VT100™ is a trademark of Digital Equipment Corporation.
WYSE® is a registered trademark of Wyse Technology.

Revision number for chapter files

Table of contents :	1.4
Before You Use BoKS :	1.7
Welcome to BoKS :	1.7
User Administration :	1.12
Password Administration :	1.10
User Authentication :	1.10
Menu Configuration :	1.10
Parameter Configuration :	1.9
Backup Administration :	1.11
Log Administration :	1.9
Reports :	1.9
Background Monitoring :	1.11
Integrity Check :	1.9
Host Administration :	1.7
Password Generator Administration :	1.6
BoKS Configuration :	1.11
Troubleshooting :	1.11
Reference Pages :	1.4
Index :	1.4

BoKS Administration

Dynamic Software AB
Hammarby Fabriksväg 13
Box 92058
120 06 STOCKHOLM
SWEDEN

T

Table of contents

This page is intentionally left blank.

I

Before You Use BoKS

I.1 Outlook

This guide provides the information that system administrators need to use BoKS effectively.

I.2 Prerequisite Knowledge

Those using this guide should have an understanding of the essential UNIX concepts. As a system administrator, you should be able to use the UNIX commands which are necessary for the daily running of the system.

We recommend also that in addition to reading this chapter, you read the chapter entitled *Welcome to BoKS* before you begin to use this product. This applies particularly to those who have either not used a security product before or who have not implemented a computer security policy before.

I.3 Structure

This guide is divided into three parts which comprise:

- twelve core chapters
- up to three add-on module chapters
- index

The guide outline is as follows:

Part One **Introduction**

Chapter 1 *Welcome to BoKS*

Provides an overview of the features in BoKS and explains the background concepts.

Part Two **Functionality**

Chapter 2 *User Administration*

Describes how to create and modify users in the BoKS database. Explains how to control system access on a per-user basis.

Chapter 3 *Password Administration*

Describes how to alter password parameters and how to ban particular passwords. Explains how to change system and user passwords.

Chapter 4 *User Authentication*

Describes how to grant and deny various types of system access to the user community in general and to individual users.

Chapter 5 *Menu Configuration*

Describes how to alter the BoKSADM (BoKS Administration) menu tree for individual system administrators by blocking certain key menu choices.

Chapter 6 *Parameter Configuration*

Describes how to alter the default parameters used by BoKS so that the product is adapted to suit your needs.

Chapter 7 *Backup Administration*

Describes how to backup and restore the BoKS database and other essential files.

Chapter 8 *Log Administration*

Describes the system and user activity reports produced by BoKS. Explains how to restore archived reports.

Chapter 9 *Reports*

Describes the BoKS system reports and explains how to query them.

Chapter 10 *Background Monitoring*

Describes how to enable and disable the background monitoring facility. This facility enables the monitoring of certain key system activities; for example, the editing of the BoKS database and other important files.

Chapter 11 *Integrity Check*

Describes how to enable the system integrity checker which reports on system vulnerability. The chapter also explains how to use the system integrity reports.

Chapter 12 *Host Administration*

This chapter describes how to add hosts to the BoKS database and how to simplify network administration.

Chapter 13 *One-Time Password Administration*

Add-on module chapter for those who have configured the one-time password module into the standard configuration of BoKS. It describes how to use the BoKS one-time password generator in conjunction with BoKS and how to maintain the password generator.

Chapter 14 *PC-UNIX Integration*

Add-on module chapter module for those who have configured the PC-Guard integration module into the standard configuration of BoKS. It describes how to administer a BoKS domain containing both DOS and UNIX machines. Users on the DOS client are controlled from a UNIX Master.

Part Three **Reference**

Chapter 15 *Configuration*

Explains the principles behind BoKS and describes the technical landscape of the product.

Chapter 16 *Troubleshooting*

Describes common problems that can occur in conjunction with BoKS and gives advice on how to fix the problem.

Chapter 17 *Reference*

Provides reference pages for the most common BoKS commands.

I.4 Related Documentation

We suggest that you have access to the following documentation:

- *BoKS - Getting Started*

  The *BoKS - Getting Started* guide accompanies this guide and explains how to install and initially setup BoKS. It also contains release notes associated with your particular version of the product.

- *BoKS - Reference Manual*

  Those who wish to extensively configure BoKS or need to supply technical support for the product should have access to the *BoKS - Reference Manual* which provides an entry for each of the BoKS utilities with a syntax listing and description.

- UNIX reference material

  A reference book on the particular UNIX variant that you are running. At points through the manual you are referred, to a UNIX reference manual so that you can check which particular circumstances apply to your operating system.

- *PC Guard Administrator Reference Manual*

  PC Guard User Guide

  These reference manuals are applicable to those administering the PC-Guard integration add-on module.

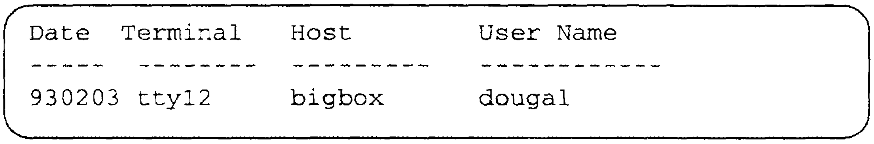
I.4.1 Font and Style Guide

This manual uses the following style and font conventions:

Screen Representations

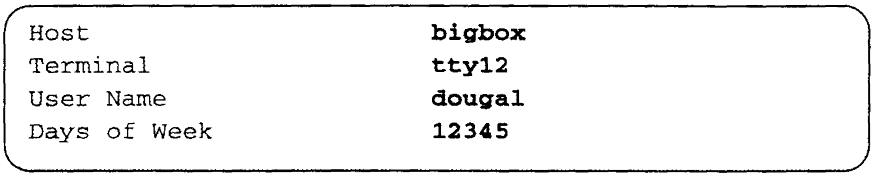
The `courier` font is used when when displaying the output of a screen. The text is displayed on a grey background in a rounded rectangle. Data to be entered into the screen is displayed in **`bold courier`**.

An example of data-display screen-shot is as follows:



```
Date   Terminal    Host         User Name
-----  --------    ---------    ------------
930203 tty12       bigbox       dougal
```

An example of a data-entry screen-shot is as follows:



```
Host                         bigbox
Terminal                     tty12
User Name                    dougal
Days of Week                 12345
```

Referring to Parts of a Screen

When parts of a screen are referred to in the text, the `courier` font is always used. When data entered into the screen is referred to the **`bold courier`** font is used. In some cases the grey background is also displayed.

For Example:

Dougal can be restricted to accessing the system to a certain number of days. This is done using the field `Days of Week`.

For Example:

Enter **`12345`** in the field `Days of Week` if you want to enable the user to log every week day.

Alternatively:

Enter the following to enable users to log in every week day:

```
Days of Week     12345
```

Pressing a Key

When referring to a particular key on the keyboard, the key is surrounded by a box.

For Example:

Use the `Space Bar` to select your choice and then press `Return` to go back.

Parts of the System

When referring to parts of the system within text the `courier` font is used. System objects include hostmachine names, terminals, users and hostgroups. There is a convention of putting the names of hostgroups in upper case. This is so that hostmachine names and hostgroup names are not confused.

For example:

The new Director of Northern Europe Sales, Simon Sharpe, has the account name `simon`. He is able to log in on the machine `littlebox` from the terminal `tty08`. He might need access to the marketing machine `colourbox` at some point in the future. The simplest way of enabling access to both machines is to assign the user `simon` to the hostgroup `SALES` which comprises both `littlebox` and `colourbox`.

Chapter and Manual References

References to other chapters in the manual and to other manuals in general are made in *italic* script.

For Example:

For further information please refer to the *Parameter Configuration* chapter in this manual. If you require further technical information, please refer to the *BoKS Reference Manual*.

Files and Directories

References to files and directories are made in *italic* script.

For Example:

These programs are usually located in the directory */usr/bin*.

Program

References to programs are made in *italic* script followed by a reference to the chapter in brackets.

For Example:

/bin/getty(1) - UNIX reference manual chapter 1.
/etc/passwd(4) - UNIX reference manual chapter 4.
su(1B) - BoKS reference manual chapter 1.
user_profiles(4B) - BoKS reference manual chapter 4.

I.4.2 Icons

The following icons are used:

✍

This is an example of an example. The text is in italics and there is a vertical line in the margin.

The explanation of the example starts here.

Information on the *BoKS Screen Lock* function is flagged by this icon in the margin. Text which belongs to this module is marked by the vertical line in the margin.

Information specific to the *BoKS Network Licence* is flagged by this icon in the margin. Text which belongs to the network description is marked by a vertical line in the margin.

Information on the *BoKS Password Generator - S220* module is flagged by this icon in the margin. Text which belongs to this module is marked by a vertical line in the margin.

I.5 Repeated Constructions

Certain keys are used repeatedly to simplify carrying out tasks in BoKS. These keys are:

- `Return` key, used to proceed to the next field in a screen.
- `Return` key, used to execute a menu choice.
- `Execute` key, used to execute a menu choice.
- `Go Back` key, used to quit from a screen with out executing the menu choice.
- `Menu Help` key, for background menu help. This provides you with background help to the data-entry screen or menu, depending on what is appropriate for your current location in the BoKSADM menu.
- `Help` key, for context sensitive help which often provides a list of values to choose from. `Help` provides context sensitive help for the field you are currently at or the menu choice that your cursor is placed on.
- `Space Bar` key, used to clear a field.
- `Ctrl` `U` key sequence, used to change output device so that the result of a menu choice can be sent to a printer or a file.

These actions are not specified in this guide unless there is a particular significance attached to using one of these keys in a certain situation.

1

Welcome to BoKS

1.1 BoKS - Practical Security for Open Systems

In many computer environments today there is a need to secure data from unauthorised access. The level of security required varies from establishment to establishment. In general terms you can say that a secure system is one that can differentiate between authorised and unauthorised users for both system and data access.

A UNIX system has two main mechanisms for differentiating between authorised and unauthorised users:

- Login procedure
- Data access control

It is users with system administration privilege (system administrators) who control these features, using the facilities that UNIX provides. BoKS enhances the UNIX security mechanisms, providing system administrators with more flexibility and functionality when securing a system. BoKS regards users with a user identity number of 0 (UID 0) as being system administrators. The default system administrator is the user `root`. It is possible to create other UID `0` accounts, the merits of this action are discussed later in this chapter, and throughout this guide in general.

1.1.1 The Login Procedure

Users accessing a UNIX system must enter their account name to identify themselves to the system. In addition users often, but not always, are required to enter a password. It is the password that secures the login procedure as the account name is public information, whereas the password is encrypted. If there is no password to an account, or the password is poor, the ability of UNIX to differentiate between authorised and unauthorised users is compromised. Users' passwords are, unfortunately, often easy to guess and often not changed on a regular basis.

BoKS Response to the Login Procedure

In response to inherent weaknesses in the UNIX login procedure, BoKS forces all users to:

- Set a password
- Change the password on a regular basis
- Set reasonably complex passwords

In addition BoKS enables you to:

- Ban certain passwords which are easily guessed
- Block the reuse of passwords
- Enforce two levels of passwords
- Restrict where and when users can log in from and log in to

The parameters and restrictions that BoKS places on the login procedure significantly develop and strengthen the features in UNIX which differentiate between authorised and unauthorised users.

1.1.2 Data Access Control

A UNIX system stores data in files. The files themselves are stored inside directories. UNIX controls access to both directories and files by enabling the system administrator to set and manipulate access permissions.

The access permissions are two dimensional and structured in the following matrix: The permissions

- Read (r)
- Write (w)
- Execute (x)

are assigned to a file.

Access to a file is qualified by restricting who has access and the extent of access for each type of user. Who has access can be one or a combination of three types of users:

- Owner of the file (user)
- System group (group)
- Rest of the user community not included in the system group (others)

Each type of user can be assigned any or a combination of the three types of permissions. It is therefore essential that users are carefully grouped together so that *system group* and *rest of the user community* do not become synonymous.

The access that each user has to files and directories is based on their UID (user identity number) which determines which user type they are and therefore which permissions they are to have.

BoKS Response to Data Access Control

To strengthen this mechanism, BoKS enables system administrators to:

- Set a *umask* value for each user. A *umask* value is the setting of the default file permissions for all files subsequently created by users.
- Control use of the substitute user facility, the *su*(1B) program, so that users are restricted to which user IDs they are able to adopt.
- Actively consider the system group that users should belong to.

In addition BoKS enables the administrator to:

- Monitor permission changes on selected files.
- Audit alterations to selected files.
- Enables the division of system administration tasks between several users with system administrator privilege. This means that the scope of system administrator authority can be limited and controlled.

1.1.3 Five Key Security Features

BoKS offers five main security features:

- Control of who can log in and where they can log in from.
- Password format control and the ability to alter formats on a per access route basis.
- Restriction of the use of the *su*(1B) program.

NOTE *You can set BoKS up in such a way that certain users are blocked from logging in but are able to be accessed through su(1B). In this way you can control and monitor system activity more effectively. Users who adopt another user ID after logging in have their activities audited under their ID at login and not the ID they have adopted.*

- Configure the BoKSADM menu system so that the menu choices for administering and securing the system are divided between several system administrators, thus limiting the activities of each system administrator.
- System administrator access control. By default BoKS does not allow system administrators to log in anywhere other than the console. To alter this you must use a specific command from the command line (see the *Configuration* chapter for further information).

NOTE *This means that even if users know the root password it is of no use to them unless they can access the console.*

In the networking version of BoKS root access is restricted to the console of the master-server.

1.2 At the Heart of BoKS

All features in BoKS centre around the security database. When BoKS is installed onto a system only the user `root` is created in the BoKS database with the same attributes that it has in the */etc/passwd*(4) file.

NOTE *If root does not have a password, BoKS aborts installation.*

When you have installed BoKS, there are two types of users:

- Users which existed before BoKS was installed.
- Users which do not exist and have to be created through BoKS.

Existing users, which were created on the system, before BoKS was installed can be loaded into the BoKS database, retaining their attributes as they are specified in the local password file. Alternatively users can be created from scratch and are assigned attributes through BoKS.

Once users have been created, additional means of system access can be granted to each user by the system administrator.

To control system access, BoKS replaces the following programs:

- */bin/login (1) (login program)*
- */bin/su (1) (substitute user)*
- *xdm (1) (X Display Manager)*

The following daemons have also been rewritten :

- *pcnfsd (1) (personal computer network file system daemon)*
  Controls access to *pcnfs (1) (personal computer network file system).*
- *rshd (1) (remote shell daemon)* Controls access to programs which use *rcmd (3) (remote command),* for example *rsh (1) (remote shell), rcp (remote copy).*
- *rexecd (1) (remote execution daemon)*
  Controls access to programs using *rexecd*(1), for example *rmt (1) (remote tape).*
- *ftpd (1) (file transfer program daemon)*
  Controls access to the file transfer program *ftp*(1).

The way these re-written programs are manipulated is explained in the next section (please refer to the sub section entitled *System Access*).

1.3 The Tool BoKS

BoKS is more than an access control suite, it is an entire security concept. Typically to secure a UNIX system, requires:

- good working habits

- detailed system monitoring
- simple and comprehensive user administration
- effective backup routines

To meet these requirements, BoKS provides the core functionality outlined in the following sections.

1.3.1 User Administration

BoKS enables you to set up user defaults. This means that when you create a user almost all the fields are filled out with a default value, thus minimising the chance of input error and enabling you to maintain a uniform user community.

1.3.2 Password Administration

BoKS enables you to set password format parameters which enforce combinations of letters and numbers. This ensures that the passwords users create are difficult to guess. This feature is further strengthened by the ability to create a list of passwords which are banned from being used and blocking passwords from being reused.

1.3.3 System Access

BoKS enables you to control system access on many levels. BoKS controls system access through *access routes.* An access route is comprised of the three **W** s.

1. **W** hich access command (`access_method`)
2. **W** here the command is used from (`from_location`)
3. **W** here the command is to gain access to (`to_location`)

Each access route has an authentication method. The authentication method defines the way in which users using the access routes are to authenticate themselves to the BoKS database so that access can be granted. The default is to specify the user password

In addition the following parameters can also be specified:

- time of day - period of the day during which the access route is available
- days of the week - days of the week that the access route is available

Particular access routes can be assigned by default to all new users. Additional access routes can be assigned to individual users, as necessary.

Blocking System Access

Users can be blocked from accessing the system by:

- system administrator
- too many failed login attempts

- expired passwords
- attempting system access from an unauthorised location
- attempting system access during an unauthorised time

1.3.4 Menu Access

If you have several system administrators, you can divide access to the BoKSADM menu choices between them. This results in system administration functionality being divided between several administrators, limiting the overall power of each administrator - a "divide and rule" type policy. In this way more control can be exercised over system administrators and the consequences of any UID 0 security breaches, either accidental or intended, are limited.

1.3.5 Background and Integrity Monitoring and Reports

BoKS offers two major types of system monitoring:

- Background Monitoring.. Monitors user activity, controls the timeout feature and monitors file access.
- Integrity Checking. Monitors the level of vulnerability that a system is exposed to, reports on potential security problems, suggests potential patches to the most serious security holes.

The results of both types of system monitoring are presented in comprehensive, easy-to-read and easy-to-analyse reports.

To make full use of the integrity checker feature, integrity checking should take place regularly, so that the security implications of system changes can be monitored effectively.

1.3.6 Backups

BoKS comes complete with a backup facility so that you can backup user data and the system setup on a regular basis.

1.4 Add-on Modules

BoKS is a modular product which has a series of core modules outlined above. In addition it is possible to install a number of add-on modules which are configured into the core structure. The main add-on modules are:

- network support
- one-time password generator support
- PC - Unix integration

1.4.1 Network Support

The BoKS network module enables users to control a network of machines. The BoKS network is termed the BoKS domain. The domain is made up of a master-server, a number of slave-servers and clients.

Master-Server

The master-server holds the original copy of the security database. The security of the BoKS domain is controlled from this central point. `root` by default can only log into the master-server. BoKS administration facilities through BoKSADM can only be executed on the master-server. This means that all BoKS configuration of slave-servers and clients is carried out from the master-server.

Slave-servers

The slave-servers contain read-only copies of the database which are updated or replaced (depending on the extent of the changes) with copies of the master-database when the master-database changes. Any server, either master or slave, may respond to a client request, for example a request to log in or a request to change user ID. As long as at least one server is up and running, users can access the system. This means that if the master-server goes down, one of the slave-servers can still ensure system access.

Clients

The client does not have a copy of the security database but instead validates user access requests by requesting information from one of the server databases via the network. There is a local daemon running on the clients to update the local */bin/passwd (4)* file.

Host Administration

Most of the network administration is carried out through the *Host Admin* menu which enables you to:

- Add hosts to the BoKS database
- Group hosts together into host groups so that a user can have access to more than one machine using the same account.

When adding new machines to the network and to the security database, user data can be loaded from both *YP/NIS* files and the regular password files.

1.4.2 One-time Password Module

BoKS has a one-time password module which enables users to use a one-time password generator. The passwords produced by the password generator are only valid for one system access session. The implications of an unauthorised user gaining to access to a session password are significantly less than an unauthorised user gaining access to a regular UNIX password.

1.4.3 PC-Unix Integration Module

In a network scenario BoKS enables you to have DOS clients which are running PC-Guard as the security package. This module enables you to load PC-Guard users into the BoKS database and can control them from the BoKS master-database.

1.5 Starting BoKS for the First Time

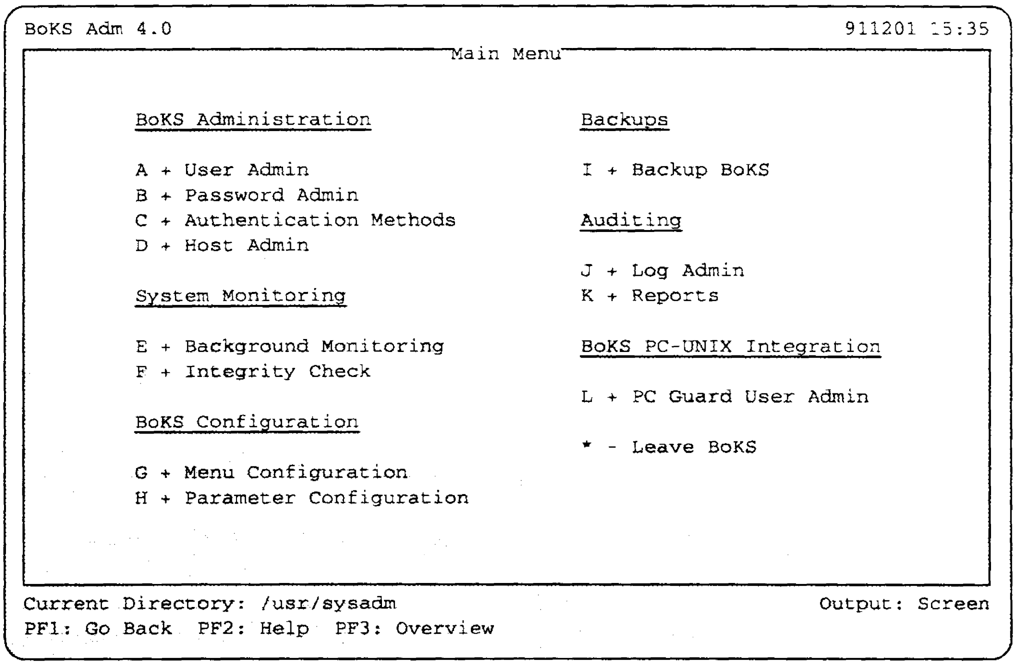
Having installed BoKS, you invoke the BoKSADM menu system by entering **boksadm** at the system prompt. In the network version of BoKS *boksadm* can only be run from the master-server. All slave-server and client configuration takes place from the BoKSADM menu on the master-server.

The first time you invoke the BoKSADM menu system, you are presented with the *Parameter Configuration* menu. We advise you to fill out the system parameters and defaults as new users assume these parameters. See the *BoKS - Getting Started* guide and the *Parameter Configuration* chapter in this guide for further details.

The process of loading existing users into the BoKS database and creating new users is explained in the in the *BoKS - Getting Started* guide and in the *User Administration* chapter in this guide.

1.6 The Main Menu

The BoKSADM menu system has the main menu illustrated in figure *1.1*.



```
BoKS Adm 4.0                                                        911201 15:35
                                  Main Menu

        BoKS Administration                        Backups

        A + User Admin                             I + Backup BoKS
        B + Password Admin
        C + Authentication Methods                 Auditing
        D + Host Admin
                                                   J + Log Admin
        System Monitoring                          K + Reports

        E + Background Monitoring                  BoKS PC-UNIX Integration
        F + Integrity Check
                                                   L + PC Guard User Admin
        BoKS Configuration
                                                   * - Leave BoKS
        G + Menu Configuration
        H + Parameter Configuration

Current Directory: /usr/sysadm                                    Output: Screen
PF1: Go Back  PF2: Help  PF3: Overview
```

Figure 1.1 - Main Menu

1.6.1 Using the BoKSADM (BoKS Administration) Menu System

The BokSADM menu system is composed of a series of sub menus. Each sub menu can contain both a further sub menu and menu choices. Each menu choice enables you to perform a system administration task.

The menu system is intuitive and has a consistent format, making it easy to navigate and quick to learn.

Selecting a Menu Choice

One of the following two signs is placed before each menu choice, on every menu:

- "+" sign before a menu choice means that the menu choice calls a sub-menu.
- "-" sign before a menu choice means that the menu choice executes a particular task.

The menu choices can be executed either by moving the cursor key to the menu choice and pressing `Return` or by pressing the letter in front of the menu choice. This letter is referred to as the *direct choice.* The action of pressing the direct choice letter to execute a menu choice is referred to as *pick and point.*

Menu Help

Each menu choice has both background help and context sensitive help. To call-up the background help for both menus and data-entry screens, press the function key illustrated with the label *Menu Help* at the bottom of the screen on BoKSADM menu.

To call-up context sensitive help for the data-entry field or menu choice, press the function key illustrated with the label *Help* at the bottom of the screen on the BoKSADM menu.

In most cases you are able to call-up a popup box at each input field. This popup box provides a list of alternatives that can be entered into this field. To call-up the popup box:

- Move to the relevant field
- Press the `Help` function key
- Move the highlight bar down to the appropriate alternative
- Press `Return`

This action is referred to as *pick and point.*

Function Keys

Throughout the BoKSADM menu system the same four function keys are used to carry out actions. These actions are:

Go Back — Quits you from your current screen without executing the command and takes you back to the previous screen/menu.

Help — Displays the context sensitive help for the current field or menu choice.

Menu Help — Displays the general, background menu help for the current menu or data entry screen.

Execute — Executes the current menu choice.

NOTE *On some terminals the function keys used are slightly different but the actions are always the same.*

Direct commands are also available. Direct commands are Ctrl sequences which can be executed from any keyboard to carry out certain functions. (Please refer to the chapter entitled *Before You Use BoKS).*

Pick and Point

Pick and point is the term for making a direct choice either from the menu or from a `Help` popup box.

To make a direct choice from the menu:

- Press the letter before the "+" or "-" signs which are in front of the menu choice.

To pick and point from a `Help` popup box:

- Move to the relevant data-entry field
- Press the `Help` function key
- Enter the first letter or first group of letters of the appropriate alternative in the list
- Press `Return` at the option you require.

This selects the alternative you require and places it in the data-entry field.

Using the Mouse

If you are running BoKS in an X-Windows environment, you are able to use the mouse to pick and point menu choices in the BoKSADM menu.

Selecting a Menu Choice with a Mouse

To select a menu choice with a mouse:

- Move the marker over the desired menu choice
- Click mouse button *1*

Using a Function Key with a Mouse

To use the function keys with a mouse that are listed at the bottom of the BoKSADM menu:

- Move the marker to the function key label on the screen
- Click mouse button *1*

Changing Directory and Output Device with a Mouse

To change current directory and the output device when in the BoKSADM menu:

- Move the marker over the desired function key label at the bottom of the screen
- Click mouse button *1*
- The screen prompts either:
  - for the name of the directory you wish to change to or
  - for the name of the output device if you have requested a change in output device

- Enter the name of the directory or the output device and press `Return`

If you wish to quit from either of these tasks and retain the old values, click on the function key on the bottom of the BoKSADM screen, labelled *Go Back.*

Go Back from a Menu Using a Mouse

To go back a menu using a mouse:

- Click mouse button *3* from anywhere within the menu

Multi-Pick

Multi-pick is a feature used for selecting several items as opposed to pick and pointing one item. It is similar to using pick-and-point in a popup box. Move to the relevant field and press the `Help` function key. If the data-entry field supports the multi-pick feature, a popup box appears on the screen with a list of alternatives. The difference between a multi-pick popup box and a pick-and-point popup box is that multi-pick enables you to select more than one alternative.

To select several items from the popup box, carry out the following:

- Move to the item with a cursor key
- Press the space bar
- A plus sign appears to the left of the item
- Move the cursor key to the next appropriate item and repeat the process

If you make a mistake and select an item by accident, move to the selected item and press the space bar again. This de-selects the item and the plus sign disappears.

When you have finished selecting the items press `Return` and the popup box disappears and the items have been selected.

The data-entry fields that support the multi-pick feature are specified in the relevant functionality descriptions in the following chapters in this guide.

1.6.2 Direct Commands for Administering the Menu System

Generate a List of Direct Commands

`Ctrl` `G` enables you to generate a list of direct commands and each command has a brief description.

Redraw the Screen

`Ctrl` `L` enables you to redraw the screen if for some reason the output display has become corrupted.

Go Back

`Ctrl` `Z` or `Ctrl` `A` `1` both enable you to go back a menu/screen.

Help

`Ctrl` `A` `2` enables you to call up on-line help if you are in a field, even if your function keys do not work.

Menu Help

`Ctrl` `A` `3` enables you to call up menu help even if your function keys do not work.

Execute

`CTRL` `A` `4` enables you to execute a menu choice or command even if your function keys do not work.

Screen Dump

To save an image of the current screen in a file or send it to a printer first use `Ctrl` `U` to change output to the desired device and then press `Ctrl` `P` to dump the contents of the screen to that device.

Exit from BoKSADM

`Ctrl` `C` `Ctrl` `C` enables you to quit from the menu tree altogether, regardless of where you are in the menu tree.

1.6.3 Direct Commands to Move within a Screen/Menu

Move to Previous field/menu choice

`Ctrl` `F` `U` enables you to move to the previous field if in a data entry screen or to the previous menu choice if in a menu.

Move to Next Field/menu choice

`Ctrl` `F` `D` enables you to move to the next field if in a data entry screen or to the next menu choice if in a menu.

Move to First Menu Choice

`Ctrl` `F` `H` enables you to move to the first field if in a data entry screen or to the next menu choice if in a menu.

Go to End of Line

`Ctrl` `E` enables you to go to the end of the data in a data entry field.

1.6.4 Direct Command to Edit Field Contents

Erase Input Field

`Ctrl` `K` enables you to erase a line of data in an input field.

Erase Character Forward

`Ctrl` `D` enables you to erase the next character in an input field.

Erase Character Backwards

This enables you to erase the previous character in an input field.

Erase Character Backward

This enables you to erase the previous character in an input field.

1.6.5 Direct Command to Change a Factor Outside the Menu System

Change Current Directory

`Ctrl` `B` enables you to change your current directory just as you would at the system prompt. Both relative and absolute directory names are permissible.

Change Output Device

`Ctrl` `U` enables you to change where the output of a command is sent to. Normally the output is sent to the screen but it can be redirected to a printer or a file. The current output device is displayed at the bottom right hand corner of the screen.

View the Contents of a Directory

Ctrl V enables you to view a list of files and subdirectories in the current directory. A "*" beside a file indicates that it is executable and a / after the name indicates that it is a directory.

Execute a Shell Command

Ctrl X enables you to execute a shell command from within the BoKSADM menu system.

This page is intentionally left blank.

2

User Administration

2.1 Outline

The following chapter explains how to use the *User Admin* menu. From this extremely central part of BoKS you can administer users in a BoKS domain. This chapter explains how to carry out the following:

- Create new users
- Load existing users into the BoKS database from the password file
- Specify the life span of a user account
- Specify the password life span
- Specify the automatic timeout parameter
- Assign ways of accessing the system to users
- Modify users system setup
- List user parameters

The *User Admin* menu is both comprehensive and complex. As it is central to the functionality of BoKS, we recommend that you plan how to manage your user community before creating users through BoKS.

2.2 Outlook

Once you have installed BoKS, one of your first tasks is to set up your users. To make this process easier, you can create default values prior to setting up your user community. Set these parameters by selecting the *Parameter Configuration* menu from the main menu. Select the menu choice *User Admin Defaults.* (See the *Parameter Configuration* chapter for further details.) A user is composed of the following attributes:

- User Security Profile

- Access Route
- Administration Parameters

User Security Profile

Setting up default values for BoKS parameters removes a considerable amount of data input work, thus reducing the likelihood of errors and ensuring a more cohesive user community.

When a user is created through BoKS a security profile is created which is stored in the BoKS database. The profile defines the limits of system activity that have been setup for each user. The profile consists of:

- access route specifications
- user administration specifications
- login start up details

Access Routes

Access routes defines the means by which users can access the system. An access route comprises three **W** s:

- **W**hich method a user is able to access the system with, for example *LOGIN, TELNET,* and *XDM.*
- **W**here a user can access the system from. This can be a terminal or, in the case of a network, a remote machine.
- **W**here a user is granted access to.

The system administrator can specify default access routes for the user community as a whole and can also tailor access routes for individual users and groups of users.

There are three different types of access routes:

- LOGIN
- SU
- Miscellaneous

1. LOGIN access route

   Controls:

   - **W**ho can use the *login*(1B) program
   - **W**here the user can use the *LOGIN* access method from
   - **W**here the user can gain access to via the *LOGIN* access method

   In this example the first **W**here specifies which terminal the user can log in to the system from. The second **W**here specifies which machine in the BoKS domain the user can access via *LOGIN.*

2. SU access route

   Controls:

   - **W**ho can use the *su*(1B) program to temporarily adopt another user's ID number

- Where the user may use the *SU* access method from
- Which user ID may be adopted

In this example the Where specifies from which terminal *SU* may be used from.

3. FTP, PCNFS, REXEC, TELNET, RSH, XDM, RLOGIN

Miscellaneous access methods which are controlled control three Ws:

- Which miscellaneous access method is available to the specified user
- Where the user can use the access method from
- Where in the BoKS domain the user can reach with the access method

In this case the first Where is either a terminal, or more commonly, a machine in the BoKS domain.

The second Where is a machine in the BoKS domain.

User Administration Parameters

The following user parameters can be altered for individual users from the *User Admin* menu:

- automatic timeout
- password lifespan
- dates for user last login
- access control based on days of the week
- times of the day when users can access the system

The use of these parameters reduces bad habits, from the point of view of system security. This helps to ensure that your user community behaves in a controlled manner.

All the above features are in addition to the following settings:

- user's command search path (PATH setting)
- user's default file permissions
- user's home directory

These parameters can be altered for individual users.

If the options on the *User Admin* menu are used correctly, the system administrator can create both flexible and secure user environment.

Startup File

The users' system environment that they first log into is largely controlled by the login startup file. As a default the UNIX startup files *.login* (C-shell), *.profile* (Bourne shell), and *.cshrc* (C-shell) are copied into the users' home directories when the users are created. The startup file used when the user logs in, depends on the shell that the user accesses. The startup file determines the commands that are carried out once users have been accepted for system access.

It is configurable which files are copied into a new user's home directory. The procedure for defining which files are copied into the new home directory is explained in the *Configuration* chapter.

2.3 Important Terms

The following is a list of terms that you encounter in this chapter:

Access Route

Specification of the route that a user utilises to access a particular system.

BoKS Domain

One or several machines controlled by one BoKS database. In the standalone version of BoKS the domain only consists of the standalone machine. In the network version of BoKS it consists of a number of machines with the database on the designated master-server machine.

CPU

CPU is an acronym for the term *central processing unit*. This is the area of the computer where a program is executed. It is the area that is often referred to as the "processor."

CPU time

Amount of time that a program is running in the CPU.

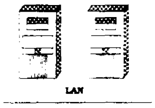
Direct Entry Format

An access route may be entered in a direct format. This means that all the components of an access route are entered in one field. The advantage of the direct format is that it is quicker to enter.

Home Directory

Users' own directory where they may create files and directories.

Host



The host is a machine in the BoKS domain. In the standalone version of BoKS, the domain only consists of one host. In the network version of BoKS a host can be master-server, slave-server and client. All machines regardless of what role the play, are regarded as hosts.

Host group

Host group is a collection of hosts which have been grouped together in the BoKS database and can be administered as one entity. This feature is only available on the network version of BoKS.

Screen Entry Format

An access route can also be entered in screen entry format. Here the system administrator creates the access route by entering the access route components field by field. The advantage with the screen entry format is that you do not have to know the syntax of the access route and the menu offers you online-help at each field.

Shell

The shell is a program whose main property is its ability to execute other programs.

Su

The *su* (substitute user) UNIX program. This allows users to temporarily adopt another user ID. The system is aware of the original user ID which is registered when the user logs in. The system audits all auditable system activity by the user to the ID at login and not the adopted one.

NOTE *When using the /bin/su(1B) program the following terms should also be understood:*

- *Target user - user whose ID is being adopted.*
- *UID User's identity number when logging in.*

Umask

Umask defines a user's default file permissions settings on all new files that the user creates. Permission settings in UNIX are two dimensional.

The user community is divided into three types of user:

- owner of the file
- group of users needing special access to the file
- the rest of the user community not included in the previous groups

To each of these groups can be assigned all or some of the following three types of permissions:

- read
- write
- execute

The following is a table of *umask* values which manipulate the above permission settings:

		Permissions		
Umask	**Setting**	**User Access**	**Group Access**	**Other**
000	`-rwxrwxrwx`	all	all	all
002	`-rwxrwxr-x`	all	all	read,execute
007	`-rwxrwx---`	all	all	none
022	`-rwxr-xr-x`	all	read,execute	read,execute
027	`rwxr-x---`	all	read,execute	none
077	`-rwx------`	all	none	none

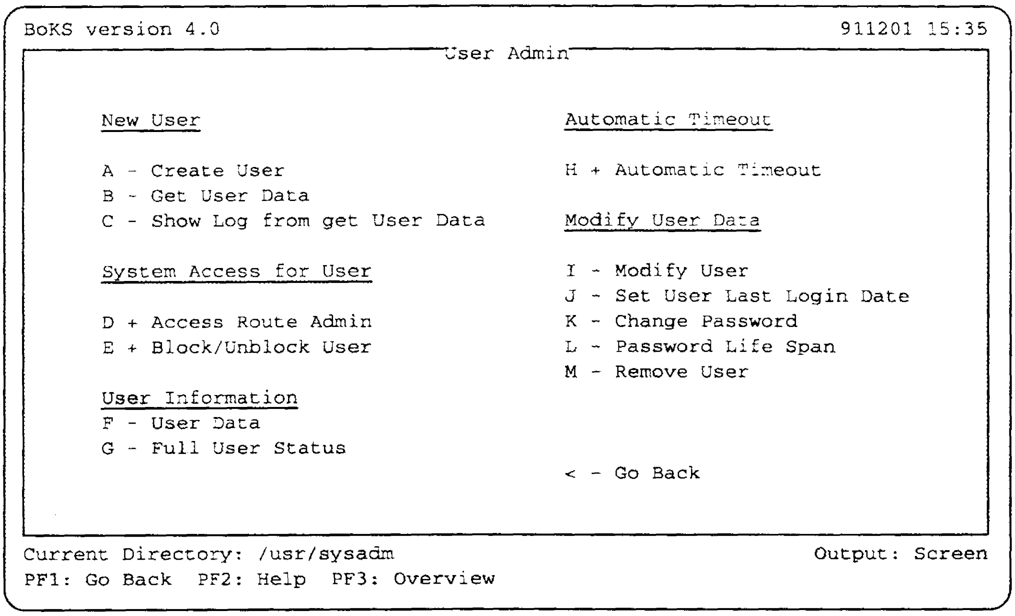
YP/NIS

YP/NIS (Yellow Pages/Network Information Service) is a distributed database which enables several machines to share the password and group files. User administration in a network is centralised with this functionality.

2.4 The User Admin Menu

The *User Admin* menu appears on the screen as shown in figure *2.1*.

NOTE *The functionality of the menu choice "Change Password" is available both from the User Admin and from the Password Admin menus. In the "Password Admin" menu this functionality is available with the "User Password" menu choice.*



```
BoKS version 4.0                                              911201 15:35
                                 User Admin

    New User                                Automatic Timeout

    A - Create User                         H + Automatic Timeout
    B - Get User Data
    C - Show Log from get User Data         Modify User Data

    System Access for User                  I - Modify User
                                            J - Set User Last Login Date
    D + Access Route Admin                  K - Change Password
    E + Block/Unblock User                  L - Password Life Span
                                            M - Remove User
    User Information
    F - User Data
    G - Full User Status
                                            < - Go Back

Current Directory: /usr/sysadm                                Output: Screen
PF1: Go Back  PF2: Help  PF3: Overview
```

Figure 2.1 Sub menu, User Admin

2.5 Functionality

The following section explains how to use the functionality provided in the *User Admin* menu. To access this menu, select the *User Admin* menu from the main menu. All the menu choices explained in this section are found on the *User Admin* menu or in one of the two sub menus leading from the *User Admin* menu.

2.5.1 Creating Users

When you install BoKS only `root` is created as a user. After installation there are two possible types of users:

- Users which existed on the system before BoKS was installed.
- Completely new users which have to be created through the BoKS database.

Existing users can be loaded into the BoKS database from the relevant data file (usually */etc/passwd*(4)) using the *Get User Data* menu choice.

New users are created one at a time using the *Create User* option on the *User Admin* menu.

Loading Existing Users

The *Get User Data* option enables you to load existing users (those users who existed before BoKS was installed) from the system's user data file into the BoKS database. The data file is typically the */etc/passwd*(4) file or a YP/NIS map.

Before using this option consider the following:

Pre-set Parameters

The users are created with predefined parameters. These parameters define:

- access routes
- access times

The parameters can be altered on the *Get User Data* screen before the menu choice is executed.

The parameter definitions are made when BoKS is installed and through the *Parameter Configuration* menu. Please refer to the *BoKS - Getting Started* guide and the *Parameter Configuration* chapter in this guide for further information.

If you are using the network version of BoKS and are using the *Get User Data* option to set up users from more than one machine, make sure that all the user identity numbers which are greater than 99 are unique. The reason for this as as follows:

If you, for example, load a user from a local password file with a user ID of 100 on one machine and then load a user from a second machine with a user ID of 100, the second user is not created as the user ID 100 is already occupied in the BoKS database.

Reading Users in

Having considered the previous points, you are ready to load existing users into the database. Select the *Get User Data* menu choice from the *User Admin* menu and enter:

NOTE *If the parameters have already been set, and you want to retain them, press* `Return` *after each field.*

`Host to Load Users from`

The name of the machine that users are resident on. In the case of the standalone version of BoKS, the host name is automatically entered.

`Local or Remote Users`

Specify whether you are:

- Loading the users from a local password file, if this is the case, enter **`Local`**.
- Loading users from a YP/NIS map, if this is the case, enter **`Remote`**.
- Loading from both the local password file and a YP map to load users from, enter **`Both`**.

`Type of Users`

Specify which type of users you wish to load into the database. Enter:

- **`System`** for system administration users (users with user IDs less than 100).
- **`Users`** for regular system users (users with IDs greater than and equal 100).
- **`All`** for all users.

`Host(Group) to Create As`

Machine users are to be coupled with. In the standalone version of BoKS this field is already completed with the name of the standalone machine. In the network version of BoKS this can be any host or host group in the BoKS domain. See the *Host Administration* chapter for further details.

`Access Route`

Access routes that are to be available to the new users by default. Access routes are specified in the following format:
*access_method***:***from_location***->***to_location*

The LOGIN access route is normally required. A sample entry is as follows:

```
LOGIN:tty*->bigbox
```

This example enables users to log in to the machine `bigbox` from any terminal connected to the machine `bigbox`.

Other access route examples are:

```
SU:tty*->tracey
```

This example enables the user to use the *su*(1B) command from all terminals to adopt the user ID of the user `tracey`.

```
XDM:xterml->littlebox
```

This example enables use of the *xdm*(1B) (X Display Manager) program. Access to this command is available on the machine `littlebox` from the X-terminal `xterml`.

NOTE

When defining the use of the XDM access method the from_location is always an X-terminal and not a host machine.

In the network version of BoKS, the following access routes can also be set:

```
RLOGIN, TELNET:*->bigbox
```

This example enables users to access the machine bigbox from any machine in the BoKS domain via the access methods `RLOGIN` and `TELNET`.

```
RSH:littlebox->bigbox
```

This example enables users to use the *rsh*(1) command to execute commands on the remote machine `bigbox` from the machine `littlebox`. This specification applies to all programs which are authenticated on `bigbox` using the daemon *rshd*(1B). Thus the same applies to the command *rcp*(1) as this uses the *rshd*(1B) for authentication.

NOTE

Multiple access routes can be entered provided that they are separated by commas. Please refer to the RLOGIN, TELNET example above. An asterisk entered into the access method field denotes that all access methods are to be authorised. A star in the from_location field denotes that the access method is available from any where on the system.

A typical multiple access route setting is as follows:
LOGIN:*->bigbox, SU:* ->otto

The above example enables users to log in from any terminal line into the machine bigbox. The second access route after the command enables you to use the su(1B) command from from any terminal to adopt the user ID of the user `otto`.

A typical global access method and from_location setting is as follows: **`*:*->littlebox`**
The above example enables users to access the machine littlebox, using any method from any location.

`Start Time`
Time in hours and minutes after which users are able to access the system. Entering 0 means that users may access the system from 00:00. The time of day is specified using the 24 hour clock.

`Stop Time`
Time in hours and minutes after which the user is no longer able to access the system. Entering 0 means that logout time is set to 24:00. The time of day is specified using the 24 hour clock.

`Days of Week`
Days of the week that users are to be able to access the system. Monday is denoted by a "1" , Tuesday is denoted by a "2," Wednesday is denoted by a "3" , and so on. If users were to use the system Monday->Thursday, enter "1234."

Get User Data in the Two Versions of BoKS

In the standalone version of BoKS, the hostname in first and fourth fields is typically the same. In the second and third fields the entries are typically **`local`** and **`all`** respectively.

In the network version of BoKS the menu choice is usually executed twice for each machine the users are to be read in from. First the system users are created from the local source file. Secondly the other users are created from the local source file. When the other users are created the `Host(Group) to Create As` is typically specified as the local host name or an appropriate host group.

Show Log from Get User Data

After the *Get User Data* option has been used, you must select the *Show Log from Get User Data* to check for users that have not been created when the user data was loaded from the local password file or NIS map. The most common reason for users not being created is that they have a user ID number which is already in use in the BoKS database. If this is the case you must change the user ID number of the user in the local password file and change the permissions on their files and directories accordingly. When you have altered the user's ID to one that is not already used in the BoKS database, select the *Get User Data* option from the *User Admin* menu. The second time it reports that the users, already created in the first run, have not been created this time. See the *Troubleshooting* chapter for further details.

Sample Output

Sample output from this report is as follows:

```
Reading user data from bigbox at 930426 09:12:04
Homedirs will be stored with full path on host bigbox
Adding Access Routes: xdm,rlogin,telnet:*-> bigbox
                  Time:08.00-17.00, 12345

USER                COMMENT                          CREATED
bigbox:root         already exists                   **NO
bigbox:nobody       No password - login              yes
                    disallowed
bigbox:tracey                                        yes
bigbox:abcd                                          yes
```

Creating New Users

To create new users from scratch once BoKS has been installed, use the *Create User* option on the *User Admin* menu.

NOTE *The first time a user logs in they must change their password. After changing their password, they are logged out and have to log in again using the new password.*

If all parameters have been preset, the standalone version of BoKS requires that only the `User Name` field is filled out.

In the case of the network version of BoKS the *Host* field also needs entering.

If the pre-set values are inappropriate, alter the values to the ones you require.

The *Create User* option contains two screens. To access the second screen press `Return` or the cursor key to key down through the fields on screen one to reach screen two. Use the up arrow to key up through the fields on screen two to return to screen one.

To create a user, select the *Create User* option and enter:

`Host(group)`

Host (or hostgroup) to which the new user is to belong.

`User Name`

User's system account name.

`Comment`

More details about the user to give the system administrator a reminder about the user name.

`Access Route`

One or several access routes that the new user can access the system with. The format of an access route is:

access_method **:** *from_location* **->** *to_location.*

Typically a LOGIN access route is specified using the following type of format:

```
LOGIN:tty*->bigbox
```

This example enables users to log in to the machine `bigbox` from any terminal connected to the machine `bigbox`.

Other access route examples are:

```
SU:tty*->tracey
```

This example enables the user to use the *su*(1B) command from all terminals to adopt the user ID of the user `Tracey`.

```
XDM:xterm1->littlebox
```

This example enables use of the *xdm*(1B) (X Display Manager) command so that the X-terminal, `xterm1`, can be used to access the machine `littlebox`.

In the network version of BoKS, the following access routes can also be entered:

```
RLOGIN, TELNET:*->bigbox
```

This example enables users to access the remote machine `bigbox` from any machine in the BoKS domain, using *rlogin*(1) and *telnet*(1).

```
RSH:littlebox->bigbox
```

This example enables users to use the *rsh*(1) command so that they can execute commands on the machine `bigbox` from the machine `littlebox`. The example above involves authentication by the daemon *rshd*(1B) on the machine `bigbox`. This also applies to the command *rcp*(1) which uses the *rshd*(1B) daemon for authentication.

NOTE

Multiple access methods and access routes can be entered provided that they are separated by commas. Refer to the RLOGIN, TELNET example above. Access commands can be combined provided that they have the from_location and to_location in common. The asterisk wild card entered into the access method field denotes that all access methods are to be authorised. An asterisk in the from_location field *denotes that the access method is available from any where on the system.*

Multiple access routes may be specified at any one time. For example: LOGIN:*->bigbox, LOGIN:* ->otto

The above example enables users to log in from any terminal line into the machine bigbox *and to log in from any terminal line into the machine* otto.

Start Time

Time after which a user may log in Format HHMM. Entering 0 means that users may access the system from 00:00. The time is specified using the 24 hour clock.

Stop Time

Time after which users can not access the system. Format HHMM. Entering 0 means logout time is set to 24:00. The time is specified using the 24 hour clock.

Days of Week

Days of the week that users are to be able to access the system. Monday is denoted by a "1" , Tuesday is denoted by a "2" , Wednesday is denoted by a "3" , etc. If users are to use the system Monday->Thursday, you enter "1234."

Group

Name of the group to which the user is to belong. The group must already exist. Please refer to your UNIX reference manual for details on creating system groups.

Home Directory

User's home directory, for example the user fred might have the following home directory: *fred.* This home directory is created as *parent_home_directory/* fred, where *parent_home_directory* is the directory specified under which home directories on that machine are created.

NOTE ***In the standalone version of BoKS the parent home directory is set in the "User Admin Defaults" menu choice on the "Parameter Configuration" menu.***

In the network version of BoKS the parent home directory is set in the *Host Admin* menu.

Alternatively you can specify both the parent home directory and the home directory by entering an absolute path name, thus: */home/fred.* This means that regardless of the machine's parent home directory setting the account is setup as */home/fred.*

`Shell`

Shell the user starts upon logging in. The default is the system shell. Typically the system shell is the Bourne shell.

`User ID`

User identity number. This number is generated automatically. Therefore unless you have a particular reason for setting the identity, for example creating a superuser (UID 0), use the unique number generated.

`Start Program`

The command to be executed as soon as the user logs in. If the user is to access the shell on log in, leave this field blank.

`Path`

The command search path for the user. The full pathname must be specified. For example if you want to specify a directory called *cmds* in the directory */usr/local/bin* you must enter: **`/usr/local/bin/cmds.`** Enter the path in the following format: *full_pathname:full_pathname:full_pathname.*

NOTE *The default path is over written when a path is specified. To append new directories to the path list enter $PATH into the list in the following way:*

$PATH:full_pathname:full_pathname:full_pathname.

For example:

$PATH:/usr/local/bin/cmds

`Umask`

The *umask* for the user.

Modify User

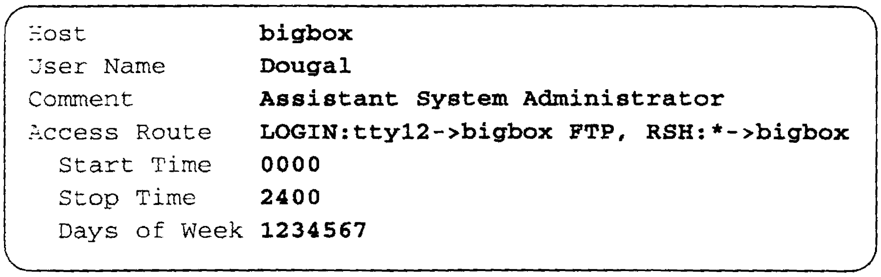
To alter a user's setup take the *Modify User* menu choice from the *User Admin* menu. The screen is the same as for the *Create User* menu choice.

NOTE *You are unable to modify a user's access route setting from this menu choice. Access routes can not be modified. They must be closed using the "Access Route Admin" sub menu on the "User Admin" menu. Open a new, more appropriate access route instead (using the "Access Route Admin" sub menu).*

Enter the name of the user and press **`Return`** and the rest of the user's details appear on the screen . To alter any of the parameters cursor down to the relevant field and enter in the appropriate value.

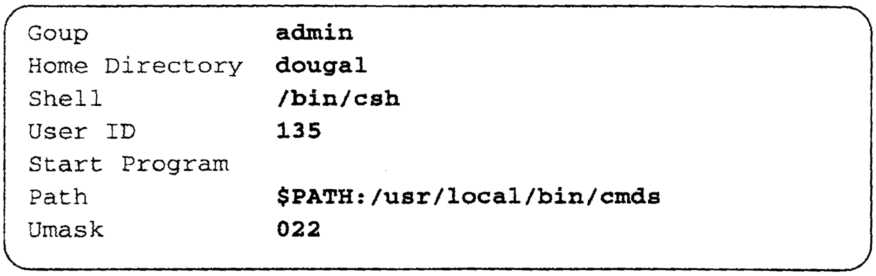
Tracey is snowed under with work and is fed up with working twelve hour days so she asks Mr. Hackit - her manager - to sign off an assistant. After a series of interviews she gives the job to a candidate called Dougal. She decides that Dougal is to have access to all the hosts on the system via the *following access routes: login, ftp and rsh from all hosts to all hosts. He is to execute the C shell when he logs in and is to be able to access the system all hours during all the days of the week.*

To carry this out, she selects the Create User menu choice and enters:



```
Host            bigbox
User Name       Dougal
Comment         Assistant System Administrator
Access Route    LOGIN:tty12->bigbox FTP, RSH:*->bigbox
  Start Time    0000
  Stop Time     2400
  Days of Week  1234567
```

The second screen looks as follows:



```
Goup              admin
Home Directory    dougal
Shell             /bin/csh
User ID           135
Start Program
Path              $PATH:/usr/local/bin/cmds
Umask             022
```

Tracey is then prompted for a password for Dougal. Having re-entered the password, Dougal is created as a user in the BoKS database and is able to log in.

Dougal is keen to log in and have a look around the system. He logs in and enters his name and the password Tracey has given him at the login prompt on terminal `tty12`. BoKS prompts him to enter his old password and then a new password. He tries entering his old password as his new password and is told that this password has already been used. He enters a completely new password. He is prompted to re-enter the new password so that it can be verified. After the password has been successfully changed BoKS logs Dougal out. He is then required to log in using the new password.

2.5.2 Constraining the User

Having created a user, there are further security features that you can take advantage of to contain the user and encourage good security habits.

When creating a user, BoKS automatically sets the following parameters:

- user last login date

- password lifespan
- automatic timeout

The above parameters enable you to constrain the user as follows.

2.5.3 Altering the User Parameters

The global default settings for these parameters can be altered using the *Parameter Configuration* menu which is accessed from the main menu. Alter the parameters in the following way:

Set User Last Login Date

A user account in BoKS must have a finite lifespan. The default period is 365 days.

The date of the last login attempt can subsequently be modified as necessary using the *Set User Last Login Date* menu choice on the *User Admin* menu. Providing user accounts with a finite lifespan means that dormant accounts can only exist on the system for a maximum of one year.

To alter the last login date for a user, take the *Set User Last Login Date* option and enter:

`User`

Name of the host coupled with the name of the user for whom the period is to be changed in the format *host(group)name : username.*

`Last Login Date YYMMDD`

The date when the account is to expire in the format YYMMDD.

Password Life Span

The longer the user uses the same password, the more likely it is that it becomes the knowledge of someone else. To reduce this threat, BoKS enforces a lifespan on passwords so that one password is valid for a particular number of days only. Once a user's password has expired, the user is forced to change it and is not permitted to use the old password. The default lifespan is 30 days.

To alter the lifespan of a password for a particular user, select the *Password Life Span* option from the *User Admin* menu and enter the following:

`User`

Name of the host coupled with the name of the user, using the the format *host(group)name : username.*

`Life Span in Days`

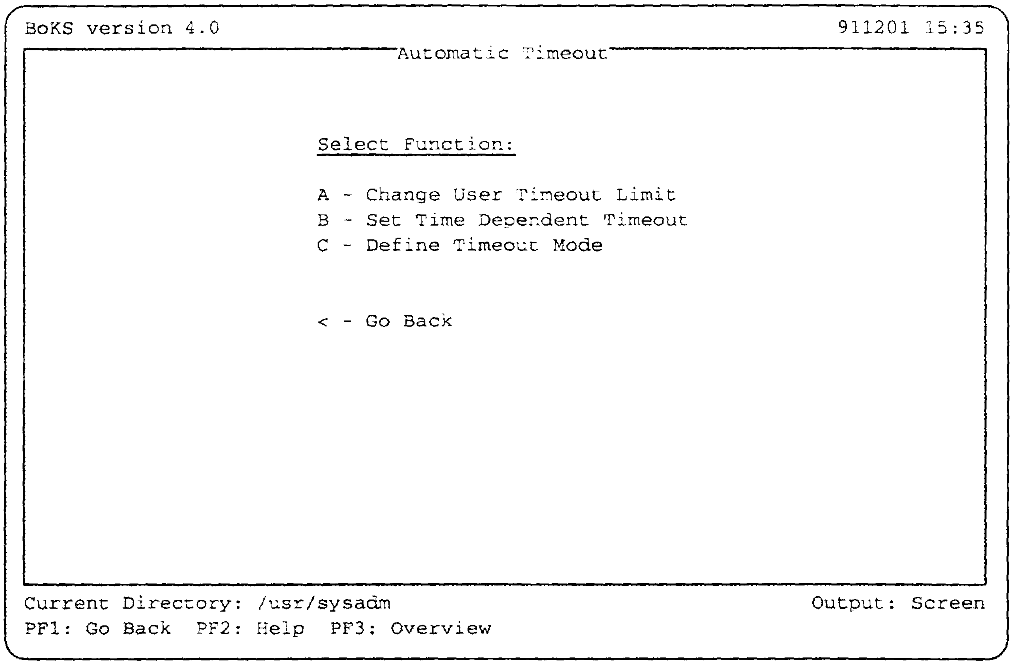
Password lifespan period in days (any number between 1 and 365).

Automatic Timeout

Users often have to leave their terminals during the course of the working day but they rarely remember to log out. When this happens they are leaving an access route into the system unprotected. To remove this risk, BoKS enables you to set an automatic timeout limit which is triggered by user system inactivity.

If users are using the system in an X-environment, they are not logged out but are locked out of their display. These users have to enter their passwords to unlock their displays.

To alter the automatic timeout settings, select the *Automatic Timeout* option from the *User Admin* menu. This menu choice takes opens the *Automatic Timeout* sub menu, shown in figure 2.2.



```
BoKS version 4.0                                              911201 15:35
                          Automatic Timeout

                     Select Function:

                     A - Change User Timeout Limit
                     B - Set Time Dependent Timeout
                     C - Define Timeout Mode


                     < - Go Back









Current Directory: /usr/sysadm                               Output: Screen
PF1: Go Back  PF2: Help  PF3: Overview
```

Figure 2.2 Sub Menu, Automatic Timeout

Change User Timeout Limit

The *Change User Timeout Limit* on the *Automatic Timeout* sub menu enables you to alter the period of inactivity after which the user is logged out.

To use this menu choice, select the *Change User Timeout Limit* option and enter:

`User`
: The hostname coupled with the name of the user, using the format *host(group)name : username.*

`Timeout Limit in Minutes`
: New timeout period in minutes. Enter 0 to disable the automatic timeout feature.

For example:

```
User                          bigbox:tracey
Timeout Limit in Minutes      15
```

This means that after a period of 15 minutes inactivity, the user `tracey` on the machine `bigbox` is logged out.

Set Time Dependent Timeout

The *Set Time Dependent Timeout* option on the *Automatic Timeout* menu enables you to create a timeout limit for an individual user which is based both on the time of day and the days of the week. This means that if you consider the system to be more at risk at some times than at others, you can tighten the timeout control during the period when the system is under greater threat.

To use the *Set Time Dependent Timeout* menu choice, enter:

`User`
: Host name coupled with the username, using the format *hostname : username.*

`Start Time`
: Time from which this timeout setting is to apply. The format is HHMM. The 24 hour clock is used to specify this value.

`Stop Time`
: Time after which the setting no longer applies. The format is HHMM. The 24 hour clock is used to specify this value.

`Days of Week`
: Days of the week when the timeout limit will apply. The format is 1234567 where "1" denotes a Monday, "2" denotes a Tuesday, "3" denotes a Wednesday, and so on.

`Timeout Limit in Minutes`
: Timeout limit in minutes. Enter a value between 0 and 1440, where 1440 minutes is equal to 1 day.

Tracey learns that Brian is going to be working late for the next couple of weeks and will, as a result, be logged on to the system during the night but will not necessarily be at his terminal. It would therefore be wise to shorten the timeout period for Brian during the evening period. She takes the Automatic Timeout menu choice, followed by the Set Time Dependent Timeout menu choice and enters:

```
User                           bigbox:brian
Start Time                     1730
Stop Time                      0730
Days of Week                   1234567
Timeout Limit in Minutes       3
```

Define Timeout Mode

The *Define Timeout Mode* option enables you to specify the criteria under which system inactivity is evaluated.

In the standard configuration of BoKS, a user is considered to be active on the system if any of the following is true:

- `CPU Time`

  A process associated with the terminal that the user is logged in on is consuming CPU time.

- `Terminal Output`

  Screen update is being performed (this means an update is sent to a terminal). This criteria is particularly useful if you have users who run programs which update the screen regularly. If this criteria is observed under these circumstances the timeout daemon is not checking true user activity.

- `Data Input`

  Data input via the user's keyboard.

BoKS screen locking in an X Windows-environment does not observe CPU-time as an inactivity criteria. This means that a display may be locked even if a program is using CPU-time. This does not effect running programs.

To alter the criteria that timeout is based on for a particular user, take the *Define Timeout Mode* option and enter:

`User`

Host name coupled with the username, using the format *hostname : username.*

`CPU Time Dependent Timeout`

Specify **yes** to observe CPU activity. Specify **no** to ignore it.

`Terminal Output Dependent Timeout`

Specify **yes** to observe terminal output activity. Specify **no** to ignore it.

By ignoring any of these criteria, the automatic timeout program no longer observes the disabled criteria when evaluating timeout requirements. By observing these criteria, the automatic timeout program evaluates timeout requirements on the activity of these features. By default all criteria are observed.

You can not choose to ignore data input from the keyboard, this is always regarded as a criteria for determining if a user is active.

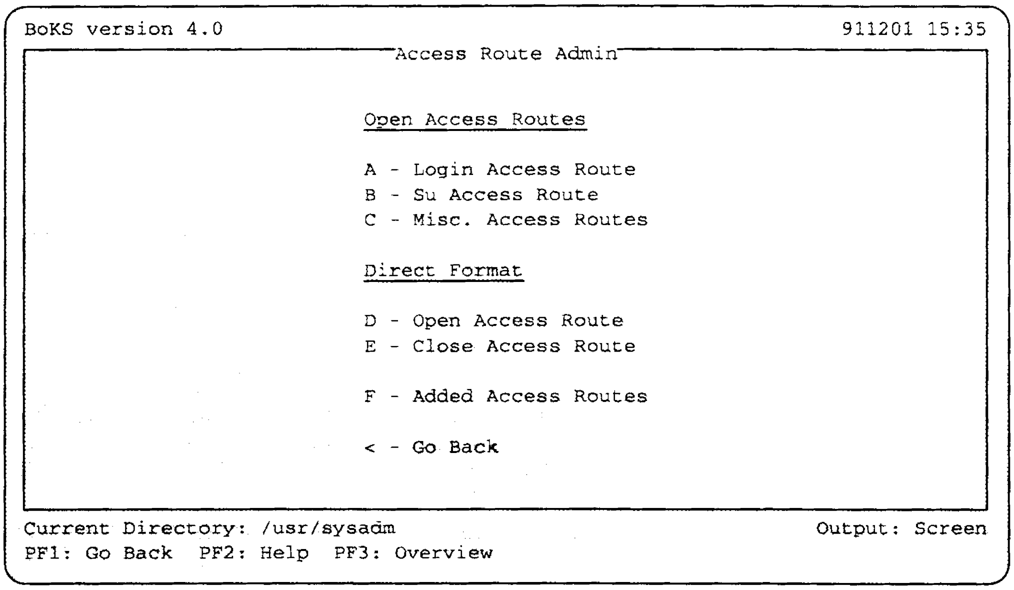
2.5.4 Controlling User Access

Access to the system is granted to users in the form of access routes. An access route enables you to specify which program/programs users can use to access the system. The definition can control system access to an even finer degree by specifying:

- Times of day the user can access the access method
- Days of the week the user when the user can access the access method

Use the *Access Route Admin* sub menu which is accessed from the *User Admin* menu, to allocate new access routes to users.

The access route is one of the corner stones of the BoKS product and the access control menu choices are designed to provide you with as much access control versatility as possible. The *Access Route Admin* menu appears on the screen as in figure *2.3*.



```
BoKS version 4.0                                              911201 15:35
                          Access Route Admin

                          Open Access Routes

                          A - Login Access Route
                          B - Su Access Route
                          C - Misc. Access Routes

                          Direct Format

                          D - Open Access Route
                          E - Close Access Route

                          F - Added Access Routes

                          < - Go Back

Current Directory: /usr/sysadm                                Output: Screen
PF1: Go Back  PF2: Help  PF3: Overview
```

Figure 2.3 Sub menu, Access Route Admin

An access route is made up of the 3 **W** s:

- **W** hich access method a user is able to gain system access with, for example *LOGIN, TELNET* and *XDM.*
- **W** here a user can access the system from. The from_location can be a

terminal line (/dev/ttyXX) or a machine name.

NOTE *The asterisk wild card can also be used to specify that the access method can be accessed from any location. Please refer to the Access Route Setup chapter for further information.*

- **W** here the user can gain system access to. The location_to can be both a host and a host group.

NOTE *Access methods are stored in the BoKS database in uppercase but can be entered through the BoKSADM menu screens in lowercase.*

The following access methods are available in BoKS:

Available Access Methods

The first component in the access route is the access method. The access methods that can be controlled in an access route are:

- LOGIN

  The *login*(1B) program which is used by users when accessing the system. *login*(1B) checks the BoKS database to see whether the user is authorised access to use *login.*

- SU (Substitute User)

  The *su*(1B) program which enables users to temporarily adopt another user ID once they have logged in. *su*(1B) program checks the database to see if the user requesting *su* is authorised to use the program. If the user is able to use *su*(1B), all activities are logged to the user ID that the user had on logging in and not the adopted one.

- FTP (File Transfer Protocol)

  The *ftp*(1) program enables the transfer of data over the network. The BoKS version of this program checks the BoKS database to see if the user requesting the use of *ftp* is authorised to do so via the *ftpd*(1B) daemon.

- RSH (Remote Shell)

  The *rsh*(1) program enables you to execute a command on a remote machine. The BoKS version of this program checks the BoKS database via the *rshd*(1B) daemon to see if the user requesting use of *rsh*(1) is allowed to use the program.

  Other programs which use *rshd*(1B) for authentication are also controlled in this manner. For example the *rcp*(1) program which enables you to copy files over the network from a remote machine.

- TELNET

  The *telnet*(1) program enables you to access a remote machine in the network. The protocol *telnet*(1) can also typically be used in environments other than the UNIX one. BoKS authenticates the user by the *telnetd*(1) which executes the *login*(1B) program on the target machine.

- RLOGIN (Remote Login)

  The *rlogin*(1) program enables you to log in to a remote machine on the network from a login session on another machine. The *rlogin*(1) program differs from the *telnet*(1) program mainly in the way that it is UNIX specific. Authentication occurs via the *rlogind*(1) daemon which uses the *login*(1B) on the target machine.

- REXEC (Remote Execute)

  The *rexec*(3) library function enables you to execute commands which use the *rexecd*(1B) deamon.

- XDM (X Display Manager)

  The *xdm*(1B) daemon is the system access program used in the X-Windows environment. *xdm*(1B) command checks in the BoKS database to see if the user is authorised to log in via an X-terminal.

- PCNFS (Personal Computer Network File Server)

  The *pcnfs*(1) service enables you to access files on a personal computer which have been mounted using the personal computer network file server. BoKS controls this via the *pcnfsd*(1B) daemon.

- *

  The asterisk wild card specifies all access methods listed above.

For more technical information on these access methods, please refer to the *Configuration* chapter and your UNIX reference material.

These access commands can be used from the following system locations:

From_Location

The second component in the access route is the *from_location*, the place from where the access method may be used. A *from_location* can be:

- `terminal`

  This setting applies to the LOGIN and SU access methods and specifies which terminal line a user may use when accessing the system with a particular access method.

- `host(group)name`

  The from_location used by all access methods other than LOGIN and SU.

- *

  If an asterisk is used then all appropriate *from_locations* are specified.

The access commands can be used to access the following locations:

To_Location

The third component in an access route is the *to_location*, specification off where the access method is able to reach. The *to_location* can be one of the following:

- `user`

  If the SU access method is specified, the *to_location,* must be a user. This is the user whose user ID may be adopted.

- `host(group)name`

  The to_location used by all access methods other than SU.

- `*`

  If an asterisk is used then all appropriate *to_locations* are specified.

Examples of Access Routes

As you are free to combine the three access route components there are many possible combinations. Typical combinations are:

```
RLOGIN,TELNET:bigbox->littlebox
```

```
SU:tty04->root
```

```
LOGIN:tty05->bigbox
```

2.5.5 Creating and Removing Access Routes

The following section explains how to create and remove access routes using the *Access Route Admin* menu. This section explains how to enter:

- access routes in screen entry format
- access routes in direct format

It also explains how to:

- remove access routes.

Login Access Route

The *Login Access Route* menu choice on the *Access Route Admin* sub menu enables you to set up a LOGIN access route for a particular user without needing to know the access route syntax.

To use this option, select the *Login Access Route* menu choice and enter:

`User`

Hostname coupled with the username, using the format *host(group)name : username.*

`From Terminal`

Terminal from where the user is to be able to log in. Wild cards can be used in this field.

`To Host`

Machine that the user is to be able to access. In the standalone version of BoKS, this field is automatically completed.

`Start Time`

Time of day after which the user is to be able to log in. Entering 0 means that the user can use the access route from 00:00. The 24 hour clock is used.

`Stop Time`

Time of day after which the user is unable to log in. Entering 0 means logout time is specified as 24:00. The 24 hour clock is used.

`Days of Week`
: Days of the week when the user is to be able to log in. The format is 1234567, where "1" denotes a Monday, "2" denotes a Tuesday, and so on.

SU Access Route

The *SU Access Route* menu choice on the *Access Route Admin* menu enables you to set up an SU access route for a particular user without needing to know the access route syntax. This means that the user is be able to adopt another user's user ID once they have logged in using the *su*(1B) program.

To setup an SU access route, select the *SU Access Route* option from the *Access Route Admin* menu and enter:

`User`
: Hostname coupled with the username in the format: *host(group)name : username.*

`From Terminal`
: Terminal from where the user is to be able to *su* from.

`To User`
: Username for the user ID which the specified user is to adopt.

`Start Time`
: Time of day after which the user is to be able to use *su*(1B) to the specified user account. Entering 0 means that the user can use the access route from 00:00. Make the entry using the 24 hour clock.

`Stop Time`
: Time of day after which the user is unable to use *su*(1B) to the specified account. Entering 0 means the access route is unavailable after 24:00. Make the entry using the 24 hour clock.

`Days of Week`
: Days of the week when the user is to be able to use *su*(1B) to this particular account. The format is 1234567, where "1" denotes a Monday, "2" denotes a Tuesday, and so on.

Misc. Access Routes

The *Misc. Access Routes* menu choice on the *Access Route Admin* menu enables you to set up access routes other than SU and LOGIN without needing to know the access route syntax. Select the *Misc. Access Routes* option from the *Access Route Admin* menu and enter:

`User`
: Hostname coupled with the username, using the format: *host(group)name : username.*

`Access Method`
: Access program the user is to access. The function key **`Help`** enables you to list all available access methods in a popup box. To select an access method from the popup box, pick and point the appropriate alternative.

`From Host`

Machine from where the user is to execute the access method.

`To Host`

Machine that the user is to be able to access. In the standalone version of BoKS this field is filled out.

`Start Time`

Time of day when the user is to be able to use the access method. Entering 0 means that the access route is available after 00:00. Make this entry using the 24 hour clock.

`Stop Time`

The time of day after which the user is unable to use the access method. Entering 0 means that the access route is unavailable after 24:00. Make this entry using the 24 hour clock.

`Days of Week`

Days of the week when the user is to be able to use the access method. The format is 1234567, where "1" denotes a Monday, "2" denotes a Tuesday, and so on.

Open Access Route

The direct format of an access route is used when you wish to specify the access route in one field and not by entering data in several fields. The advantage of doing this is that it is quicker than the screen entry format. The disadvantage is that you must know the access route syntax.

To open an access route for a specific user in direct format, select the *Open Access Route* menu choice from the *Access Route Admin* menu and enter:

`User`

Hostname coupled with the username you want to create an access route for. The format is *hostname* : *username.*

`Access Route`

Specification of the access route(s) you are creating. Access routes must be entered as follows: *access method* : *from location* -> *to location.* For example:

```
LOGIN:tty10->bigbox
```

This example means that users can log in using the *login*(1B) program on the terminal line `tty10` to access the machine `bigbox`.

```
RLOGIN:bigbox->littlebox
```

This example means that users can use the remote login facility using the *rlogin*(1) command on the the machine `bigbox` to access the machine `littlebox`.

```
FTP, RSH:bigbox->littlebox
```

This example means that users can use both the file transfer protocol and remote shell facilities from the machine `bigbox` to access files and programs on the machine `littlebox`.

`Start Time`

Time after which the access route is available. Format is HHMM. Entering 0 means that the access route is available after 00:00. Make this entry using the 24 hour clock.

`Stop Time`

Time after which the access route is no longer available. Format is HHMM. Entering 0 means that the access route is unavailable after 24:00. Make this entry using the 24 hour clock.

`Days of Week`

The days of the week when the access route is available. The format is 1234567, where "1" denotes a Monday, "2" denotes a Tuesday, and so on.

Close Access Route

Denying a user to an access route must be specified in direct format. To remove a user's ability to use an access route select the *Close Access Route* option on the *Access Route Admin* menu and enter:

`User`

Hostname coupled with the username whose access route you are deleting, using the format: *host(group)name : username.*

`Access Route`

Specification of the access route you are deleting. Enter in the format: *access method : from location -> to location.*

For example:

```
LOGIN:tty10->bigbox
```

This example means that the user can no longer use the *login*(1B) program from the terminal line `tty10` to the machine `bigbox`.

```
RLOGIN:bigbox->littlebox
```

This example means that the user can no longer use the *rlogin*(1) program from the machine `bigbox` to access the machine `littlebox`.

```
FTP, RSH:bigbox->littlebox
```

This example means that the user can no longer use both the file transfer protocol and remote shell facilities from the machine `bigbox` to access files and programs on the machine `littlebox`.

Added Access Routes

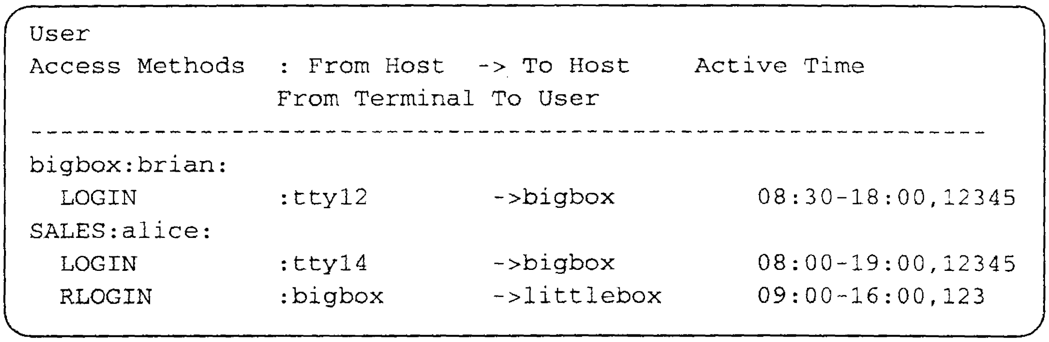
For information on the access routes assigned to each user, take the *Added Access Routes* menu choice in the *Access Route Admin* menu and enter:

`Host`

Name of machine for which you would like the access routes listed. In the standalone version of BoKS you are not required to enter the hostname, instead the menu choice displays the information as soon as it is selected.

Sample Output

Sample output is as follows:



```
User
Access Methods  : From Host   -> To Host      Active Time
                  From Terminal To User
-----------------------------------------------------------
bigbox:brian:
  LOGIN         :tty12        ->bigbox          08:30-18:00,12345
SALES:alice:
  LOGIN         :tty14        ->bigbox          08:00-19:00,12345
  RLOGIN        :bigbox       ->littlebox       09:00-16:00,123
```

NOTE *Host groups are only available in the network version of BoKS.*

This list shows that the user brian who is resident on the `bigbox` machine can access `bigbox` from the terminal line `tty12` between 8.30 in the morning and 6.00 in the evening, between Monday and Friday.

The user `alice` is resident on the machines in the hostgroup SALES. (The host group feature is only available to those running the networked version of BoKS. For those running a BoKS network, please refer to the *Host Administration* chapter for more information on hostgroups.) `alice` is able to use the access methods LOGIN and RLOGIN. She can log in to `bigbox` on the terminal line `tty14` between 8.00 in the morning and 7.00 in the evening, between Monday and Friday. `alice` can also log in remotely from the machine `bigbox` to access the machine `littlebox` between 9.00 in the morning and 4.00 in the afternoon, between Monday and Wednesday.

Explanation of Added Access Routes Report Fields

The *Added Access Routes* menu choice lists the following information:

`User`

Hostname coupled with the username for whom the listed access routes apply. The format is *Host(group)name* **:** *username.*

`Access methods`

Means of access that have been allocated to each user.

NOTE *An asterisk denotes all access methods.*

`:From Host`

`From Terminal`

Location from where each access method may be used (in the case of LOGIN and SU this is tty lines, in the case of other programs this is a host(group) name).

NOTE *An asterisk denotes that the access method is available from any where within the BoKS domain.*

```
-> To Host

   To User
```

Location which can be accessed by a particular access method. This can be a machine in the BoKS domain or in the case of SU a username whose user ID can be adopted.

`Active time`

Time of the day and days of the week when each access route is available.

This listing displays the access route information for all the users on a specified host.

2.5.6 Blocking System Access

To block and unblock system access for a specific user, select the *Block/Unblock User* option on the *User Admin* menu. This menu choice takes you into the *Block/Unblock User* sub menu.

The *Block/Unblock* sub menu enables you to deny users system access. You can also use the menu to unblock users who are already denied system access.

The *Block/Unblock User* sub menu appears as shown in figure *2.4.*

Unblock User

There are four main reasons why a user may be blocked from the system:

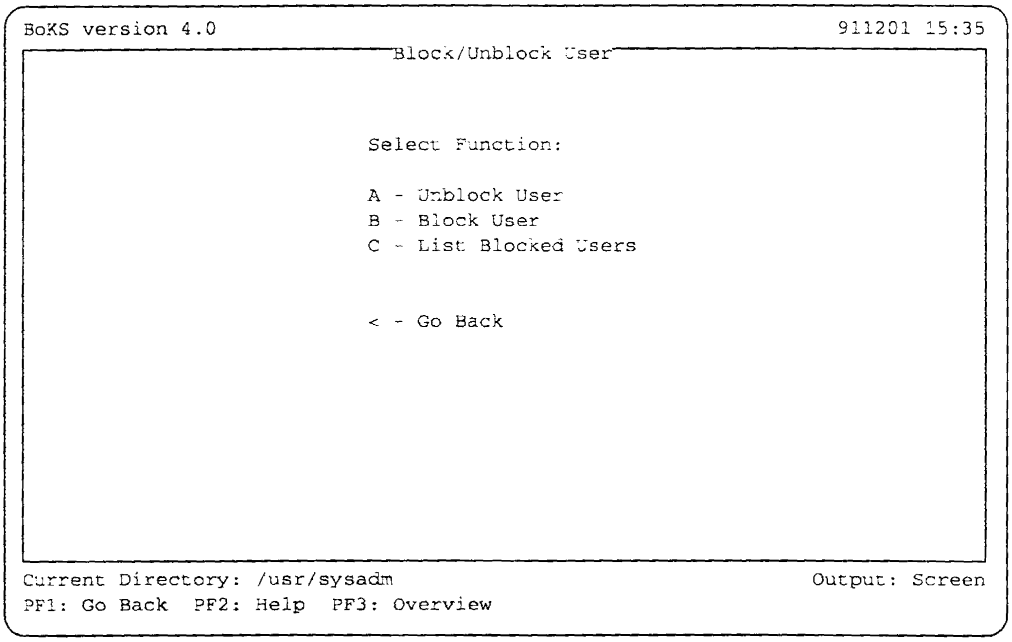
1. Blocked previously by the administrator using the *Block User* option.
2. As a result of too many consecutive failed login attempts.

NOTE *Once a user has logged in successfully the number of failed logins is reset to zero.*

3. User's password has expired or the user has no password set (in this instance once the user has been unblocked the */bin/passwd(1B)* utility is started so that the user receives a new password).
4. The user account has expired. In this instance the *Unblock User* menu choice refers you to the appropriate menu choice for extending the life span of the user's account.

The *Unblock User* menu choice enables you to unblock the following:

- Users who have been specifically blocked by the *Block User* option



```
BoKS version 4.0                                                  911201 15:35
                              Block/Unblock User

                           Select Function:

                           A - Unblock User
                           B - Block User
                           C - List Blocked Users


                           < - Go Back

Current Directory: /usr/sysadm                                  Output: Screen
PF1: Go Back  PF2: Help  PF3: Overview
```

Figure 2.4 Sub Menu, Block/Unblock User

- Users who are blocked due to too many failed login attempts
- Users whose password has expired and points you in the right direction for extending the life span of a user account

To unblock a user, select the *Unblock User* menu choice from the *Block/Unblock User* menu and enter:

`User`

Hostname coupled with the username of the user who is to be unblocked. The format is *host(group)name : username.* The function key `Help` provides a popup box with a list of blocked users. Pick and point the appropriate user.

Block User

You can specifically block a user from any system access using the *Block User* menu choice on the *Block/Unblock User* menu.

To block a user, select the *Block User* menu choice and enter:

`User`

Hostname coupled with the username of the user who is to be blocked. The format is *host(group)name : username.*

List Blocked Users

To list blocked users use the *List Blocked Users* menu choice on the *Block/Unblock Users* menu. This shows which users have been blocked from the system and the reason why they have been blocked. The headings on this report are as follows:

`User`

Hostname coupled with the username of the user who is blocked.

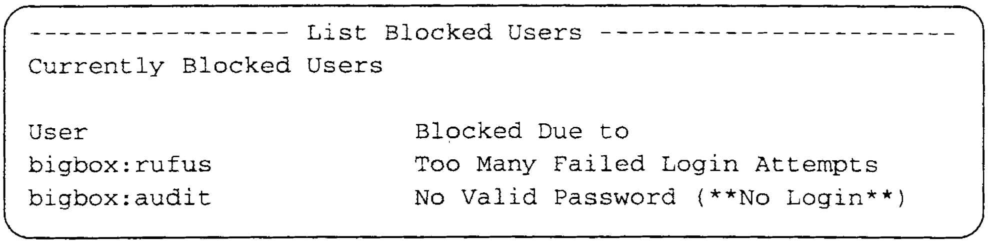
`Blocked Due to`

Reason why the user is blocked.

If for some reason a user is unable to access the system, this is a useful place to start checking. If the user is blocked and needs to access the system, take the *Unblock User* option.

Sample Output

Sample output from the *List Blocked Users* menu choice is as follows:



```
---------------- List Blocked Users ----------------------
Currently Blocked Users

User                         Blocked Due to
bigbox:rufus                 Too Many Failed Login Attempts
bigbox:audit                 No Valid Password (**No Login**)
```

This example shows that the user `rufus` who is resident on the machine `bigbox` has been blocked due to too many unsuccessful login attempts made with his account name. It also shows that the system account `audit` has been blocked as the account has no password. This happens to all accounts without a password.

Remove Users from the Database

The *Remove User* enables you to delete a user from the BoKS domain.

WARNING

Once a user has been removed the user no longer has access to the system.

To delete a user, select the *Remove User* menu choice and enter:

`User`

Name of the user to be deleted. Enter the user in the format: *hostname : username*. You are required to confirm the deletion by entering **y** when prompted or **n** to abort the deletion.

2.5.7 Displaying User Information

In BoKS it is possible to list the user current configuration through a collection of menu choices which are mainly resident under the *User Information* header on the *User Admin* menu.

For the *User Admin* menu there are three report options:

1. *User Data*

   This report is located under the *User Information* header.

2. *Full User Status*

   This report is located under the *User Information* header.

3. *Added Access Routes*

   This report is located in the *Access Route Admin* sub menu.

User Data

To list essential information about users on a particular machine, select *User Data* option from the *User Admin* menu and enter:

`Host`

Name of the host whose users are to be listed. Leave this field blank if information about all users in the BoKS domain is required.

`Sort By`

Order in which you would like the information to be listed.

There are five different types of ordering available:

0 `User Name`

Enables you to list the user records in user name (alphabetical) order.

1 `User ID`

Enables you to list the user records by user identity numbers - UID.

2 `Group ID`

Enables you to list the user records by group identity numbers - GID.

3 `Password Expire Date`

Enables you to list the user records by password expire date. It lists those users that are blocked first, followed by user records ordered in ascending order by oldest password expire dates.

4 `User Expire Date`

Enables you to list the user records in ascending order by oldest user expire date first.

Sample Output

Sample output is as follows:

```
User         UID GID   Password User    Flt Tout Comment
                       Expire   Expire
----------- ------------------- ------ --- ---- -------
SALES:alice 108 sales 930101   930201  0     5 Alice Springs
RD:buzz     109 tech  930203   930508  2    10 Buzz - prod. dev
```

This report shows the following about the user SALES:alice:

- User `alice` is resident in the hostgroup SALES.
- She has a password which expires on the 1st of January 1993.
- Her account expires on the 8th of May 1993.
- She has no failed login attempts against her (this is as her last login attempt was successful).
- She has a five minute timeout limit.

For a general explanation about these fields, please refer to the following section.

Field Description for the User Data Report

The following explains in detail the fields listed in the *User Data* report output.

`User`
: Username coupled with the hostname.

`UID` User identity number.

`GID` Group identity number.

`Password Expire`
: Date each user's password is set to expire.

`User Expire`
: Date each user's accounts is set to expire.

`Flt` Number of failed login attempts that each user has made since the last successful login attempt.

`Tout`
: Timeout limit in minutes.

`Comment`
: Sundry comments about each user.

Full User Status

To see full setup information about a user, take the *Full User Status* menu choice from the *User Admin* menu and enter:

`User`
: Name of the user for whom you would like information. If this field is left blank information for all users will be displayed. Wild cards may be used in the field. For example **`bigbox:t*`** specifies all reports for users on `bigbox` beginning with the letter `t`.

Sample Output

Sample output is as follows:

```
----------------------------- Full User Status ---------------------------
Username:                     RD:buzz
User ID:                      108
Group ID:                     10
Comment:                      Buzz -  prod. dev
Home Directory:               buzz
Shell:                        /bin/csh
Inactivity Timeout:           10 minutes
Time dependent timeout:       no
Inactivity timeout checking:  CPU, keyboard, screen
Password last changed:        921225
Password valid until:         930203
User valid until:             930508
Number of failed logins:      2
User blocked:                 no
Assigned Access Routes:       LOGIN:*->RD
                                    00:00-24:00, 1234567
                              SU    :*->root
                                    08:30-17:00, 12345
```

This sample report shows the following information about the user RD:Buzz:

- The user `buzz` belongs to the hostgroup RD.
- His user ID is `108` and his group ID is 10.
- His home directory is `buzz` and is created underneath the parent home directory that has been specified for that machine.
- He starts the C-Shell `/bin/csh` when he logs in.
- He can be inactive for ten minutes before being logged out
- He has no time dependent timeout limit set.
- His inactivity timeout criteria are CPU usage, keyboard usage and screen update.
- His password was last changed on the 25th December 1992 and is valid until the 3rd February 1993.
- He has had two failed login attempts since last logging in successfully.
- He has been assigned the LOGIN and SU access methods. He can log in from any terminal line 24 hours a day into any machine in the RD hostgroup, seven days a week.
- He may use the *su*(1B) command from any terminal line to the root account between 8.30 in the morning until 5.00 in the afternoon, between Monday and Friday.

For a more general description of these fields, please refer to the section below.

Field Description for the Full User Status Report

The following explains in detail the fields listed in the *Full User Status* report output.

`Username`
: User login name.

`User ID`
: User identity number.

`Group ID`
: Group identity number.

`Comment`
: Extra information about each user.

`Home directory`
: Home directory for each user.

`Shell`
: Shell that each user starts when logging in.

`Inactivity timeout`
: Number of minutes that each user can be inactive on the system before being logged out.

`Time dependent timeout`
: Time dependent timeout specification.

`Password last changed`
: Date the password was last changed.

`Password valid until`
: Date the password is valid until.

`User valid until`
: Date the user account is valid until.

`Number of failed logins`
: Number of unsuccessful attempts since the last successful login.

`User temporarily blocked`
: Specifies if the user is currently blocked from the system.

`User may use LOGIN`
: Specifies if the user is authorised to use *login*(1B)

`User may use SU`
: Specifies if the user is authorised to use *su*(1B).

`CPU-time Dependent Timeout`
: Specifies if CPU time dependent timeout is enabled.

`Terminal Input Dependent Timeout`
: Specifies if terminal input timeout is enabled.

`Terminal Output Dependent Timeout`
: Specifies if terminal output timeout is disabled.

`Assigned Access Routes`
: Access method information assigned to the user.

Listing Added Access Routes

For a list of the access routes that you have added take the *Added Access Routes* menu choice on *Access Route Admin* sub menu which is accessed from *User Admin* menu.

This page is intentionally left blank.

3

Password Administration

3.1 Outline

This chapter explains how to use the *Password Admin* menu. The *Password Admin* menu enables you to:

- Set parameters on the password format
- Ban certain strings from being used as or as part of a password
- Change user and system passwords

3.2 Outlook

Passwords are one of the principal methods of securing a UNIX system. The user's password is the means by which an individual is authorised to use the system. It is also one of the means by which the system identifies users. For this reason BoKS places great emphasis on password control and enables the system administrator to find the balance between a secure and realistic password policy. It is important to stress that if passwords are to be an effective security measure, users must take responsibility for keeping passwords secret and not creating passwords that are easily guessed.

3.3 Important Terms

In this chapter you encounter the following terms:

BoKS Domain

Machines which have the same BoKS database. In the standalone version of BoKS this is only one machine. In the network version of BoKS this is how ever many machines are controlled by the BoKS master-server database.

Character

Alphanumeric symbol, this encompasses; A-Z, a-z, 0-9.

Password Conditions

Criteria which define the format of the user password.

Password Default Life Span

Default length of time, in days, that passwords are valid (between 1 and 365).

Regular Expressions

Series of symbols which, when used in conjunction with certain UNIX search and editing programs, are set to map to a range of individual characters or strings. This means that search and editing functions can apply to a range of characters and strings.

System

In terms of BoKS, a system is a BoKS domain.

System Password

Password for a BoKS domain. A system password is a global one in the sense that all users in a BoKS domain use the same system password.

Time Limit for Expired Password

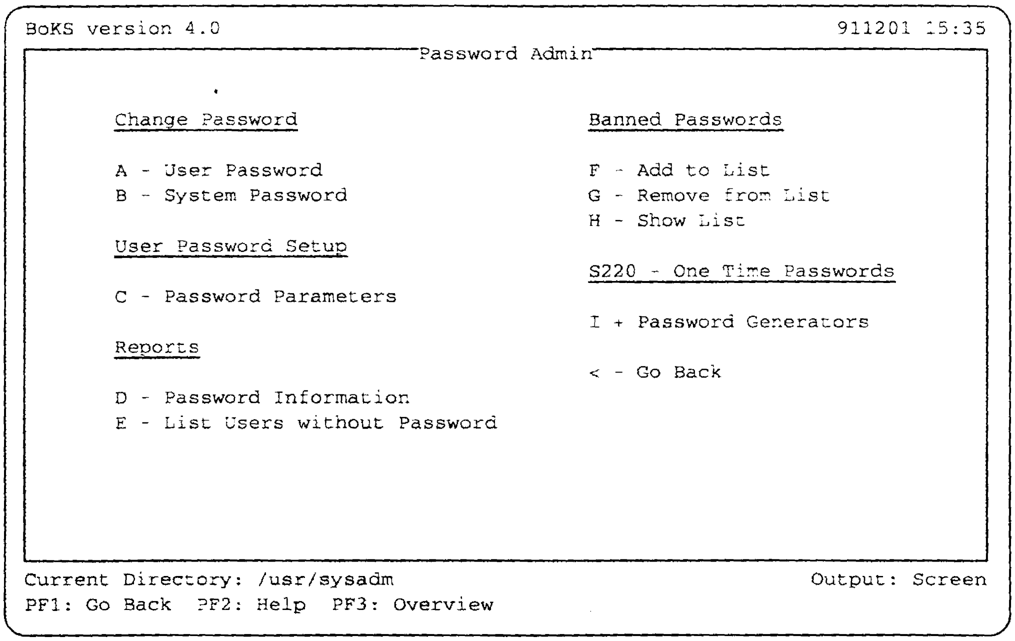
Amount of time after a password has expired that the user can still use the password to log in.

User Password

Individual user's password.

3.4 The Password Admin Menu

The *Password Admin* menu appears on the screen as displayed in figure *3.1*.



```
BoKS version 4.0                                                  911201 15:35
 ----------------------------------Password Admin-----------------------------
|                                                                              |
|       Change Password                      Banned Passwords                  |
|                                                                              |
|       A - User Password                    F - Add to List                   |
|       B - System Password                  G - Remove from List              |
|                                            H - Show List                     |
|       User Password Setup                                                    |
|                                            S220 - One Time Passwords         |
|       C - Password Parameters                                                |
|                                            I - Password Generators           |
|       Reports                                                                |
|                                            < - Go Back                       |
|       D - Password Information                                               |
|       E - List Users without Password                                        |
|                                                                              |
 ------------------------------------------------------------------------------
Current Directory: /usr/sysadm                                  Output: Screen
PF1: Go Back  PF2: Help  PF3: Overview
```

Figure 3.1 Sub menu, Password Admin

The *Password Generator* menu choice only appears on your menu if you have purchased the *Password Generator* module. Password generator functionality is explained in the *Password Generator* chapter.

3.5 Functionality

There are three main functionality areas covered by *Password Admin* menu, these areas are:

- defining and modifying password parameters
- banning passwords
- changing passwords

3.5.1 Defining and Modifying Password Parameters

The *Password Parameters* menu choice is used to alter the password parameters in order to configure the password format to meet the needs of your site.

The password parameters that can be altered are:

- minimum length
- password format
- password life span
- time limit for expired password
- number of times a user must specify a completely new password before reusing old ones
- minimum period between password changes
- backwards compatibility with the */etc/passwd*(4) file.

These parameters are important because they strengthen the login process on a UNIX system. Short words are easily guessed and are very little use as passwords. In the same way, if a password is never replaced, the probability of its being guessed increases as the password becomes older. By setting the password parameters you can enforce a more effective password policy.

Password Parameters

To set the password parameters, take the *Password Parameters* menu choice and enter:

`Minimum Length`

> Minimum length for a valid password. Entering **0** means that passwords can be any length.

`Password Format`

> Password format setting. Pressing the `Help` function key lists the following format options:

0	No Format Restrictions
1	At Least One Letter and One Digit
2	At Least Two Letters and Two Digits
3	Randomly Generated Password
4	Model This means the core of the password is generated by BoKS and the rest is input by the user. For example if BoKS randomly generates a pattern `??sa???` , the user must then enter two characters, for example **le** followed by the letters **sa** and then three more characters, for example **49b** so that the whole string would be: `lesa49b`.

`System Default Life Span`

> Number of days the password is to be valid for. Enter a number between 1 and 365.

`Time Limit for Expired Password`

> Number of days that the password can still be used after it has expired. If users log in during this period, they are forced to change

their password. Enter a number between 1 and 365.

NOTE *The first time that the user logs in after their password has expired they are forced to change their password. The password grace period is designed to enable those users who do not log in on the day their password expires, to be able to log in and change it within a period defined by the system administrator.*

`Password History Length`
Number of times a completely new password must be used, before old ones can be reused.

`Minutes Between Password Changes`
Minimum number of minutes that can pass after a change of password before users can change their passwords again.

`Update Password Information in /etc/passwd`
Specifies if the */etc/passwd*(4) file is to be updated with the changes to user passwords. Enter **yes** to enable updating and **no** to disable it. The default is no.

The parameters can be subsequently altered using the same menu choice.

Tracey considers her options when deciding what parameters to set to make the password procedure more secure. She knows that she has to balance two things:

1. *Securing the password feature by forcing users to use passwords which are not easy to guess and which have to be changed on a regular basis.*
2. *Not making the passwords so difficult to use that they are impossible to remember.*

Tracey takes the *Password Parameters* option and sets the following:

```
Minimum Length                        6
Password Format                       2
Password Default Life Span            30
Time Limit for Expired Passwords      14
Password History Length               20
Minutes Between Password Changes      60
Update Information in /etc/passwd     yes
```

By selecting the above values she has determined that the default password format is:

- at least 6 characters in length
- has at least two digits and two letters
- has a life span of 30 days

- 14 days grace to change the password after the life span has expired
- 20 consecutive passwords must be new for each user
- minimum time span for a password is 60 minutes. This means that a password can not be changed within the first 60 minutes of its lifetime
- */etc/passwd*(4) is to be updated with password changes

3.5.2 Banned Passwords

The culture that users work in tends to heavily influence such things as file names, machine names and passwords. Would-be crackers can exploit this group psychology and make educated guesses as to likely passwords that would be used. To prevent this, system administrators can make a list of passwords and strings of characters which could occur at a particular site. The combinations of characters on'this list are unable to be used passwords or parts of passwords.

Add to List

To add a password to the banned password list, take the *Add to List* option and enter:

`Password`
Password or string of characters that are to be banned.

There are two types of entry that can be made into this list:

1. Complete string of characters. Enter the full password that you want to ban.
2. Regular expressions. A regular expression must always be prefixed with a "/." This is so that the characters which have a special meaning with regular expressions is interpreted correctly.

Regular Expressions

The regular expressions used are of the variety and range found when using the UNIX command *egrep(1)*.

Examples of the types of regular expressions most used in the *Banned Passwords* menu choices are as follows:

NOTE *If you are unsure about using regular expressions in general, please refer to your UNIX reference manual, for a tutorial on how to use regular expressions.*

`/.*abc.*`
Zero or more characters can be entered before `abc` and zero or more characters after `/abc`.

`...abc..`
Three characters are to be entered before `abc` and two characters after `abc`.

`/[a-z]abc[0-9]`

One letter before `abc` and one character (either letter or integer) after `abc`.

`/[a-z]*abc[0-9][0-9]`

Zero or more letters before `abc` and two integers after `abc`.

For further information on these regular expressions please refer to the UNIX man pages or UNIX reference books explaining *egrep*(1).

NOTE *Banned passwords specified with regular expressions are case sensitive. This means that if you need to ban both upper and lower case versions of the same character combination, you must specify both an upper and lower case version.*

User names are automatically banned. Note however that user names which are part of a string are not banned automatically. For example: `tracey` *as a password would be automatically banned but* `/.*tracey*.` *would not.*

Tracey knows that Japanese food is a popular topic of conversation amongst many of the staff and Japanese "cook-ins" occur in the social area at lunch time. As a result Tracey decides to ban the most common Japanese cooking orientated passwords.

Tracey takes the *Add to List* option from the *Password Admin* menu and enters the following

```
Password /.sushi.*
```

She then presses **Return** to execute the menu choice and repeats the procedure for the rest of the Japanese cooking related vocabulary that she has listed down. She knows that she can remove any errors that she might make when inputting her list by taking the *Remove From List* option from the *Password Admin* menu.

When she has finished she lists all the banned passwords by taking the *Show List* option from the *Password Admin* menu.

Remove from List

To remove a banned password from the list of banned passwords, select the *Remove from List* option and do as follows:

`Password`

Use the multi-pick technique to select the password(s) that are to be able to be used as passwords. (Please refer to the chapter entitled *Welcome to BoKS* for details on how to use the multi-pick technique.)

3.5.3 Changing Passwords

Passwords can be set at both user and system level. A system administrator has to mostly set users' passwords when users have forgotten their password or have not used their passwords within the password grace period.

System administrators set system passwords to provide another security level on a particular access route into the system. The system password applies to all the machines in the BoKS domain. The use of a system password is specified for access routes by setting the authentication mode to request a system password (refer to the *User Authentication* chapter for further information.)

User Password

When changing a user password select the *User Password* menu choice and enter the name of the user followed by the password for the user. The password is requested twice.

Tracey receives a call from Brian the storeman in the loading bay. Brian had been working into the early hours of Saturday morning finishing off the annual stock take. His password had expired on Saturday and he had changed it just before he left the warehouse at dawn. Understandably Brian had got the password confused in his exhaustion and as a result could not log in on the terminal in the loading bay on Monday morning.

Tracey fixes this problem by taking the *User Password* option. She enters:

```
User bigbox:brian
```

She is then prompted to enter Brian's new password twice. Having done this she phones Brian to tell him his password so he can log in once more.

System Password

If you need to change or set a system password, select the *System Password* option in the *Change Password* section. The system password is a secondary password that can be set on an individual access route basis or can be set for system access as a whole. The system password relates to all the machines in a BoKS domain. All machines in the BoKS domain are controlled by the same database. This might be one machine as in the case of the standalone version of BoKS or many machines as in the case of the network version of BoKS. In the network version of BoKS, the BoKS database is located on the master-server.

3.5.4 Password Reports

There are three options which enable you to check the password parameter status. The options are:

- *Password Information*
- *List Users Without Password*

- *Show List*

Password Information

The *Password Information* option enables you to list the password parameters currently set. It also specifies whether:

- A system password has been set (see *User Authentication* chapter).
- */etc/passwd*(4) is updated when passwords are changed (for further information see the *Configuration* chapter).

Sample Output

Sample output from this report is as follows:

```
Password Information
Password minimum length:              6
Password format:                      At least two digits
                                         and two letters
Password term of validity:            31 days
Expired password term of validity:    31 days
Update /etc/passwd with passwords:    no
System password defined:              no
Length of password history            20
Minimum time between password changes 60
```

For an explanation of these fields, please refer to the section in this chapter entitled *Password Parameters.*

List Users Without Password

The *List Users Without Password* option lists the users without passwords. These users are automatically blocked from the system.

Sample Output

Sample output from this report is as follows:

```
Following Users have No Password
bigbox:sian   Invalid password (will not be able to log in)
bigbox:vera   Invalid password (will not be able to log in)
bigbox:damion Invalid password (will not be able to log in)
```

Show List

The *Show List* option is located under the *Banned Password* column header and lists the passwords and password combinations which have been expressly banned by the system administrator.

Sample Output

Sample output from this report is as follows:

```
Password
--------
/.*gohan.*
/[a-z]kunsei[0-9]
/[a-z]mizu[0-9][0-9]
/[a-z]*unaju[0-9][0-9]
noodles
san
sushi
wok
zarusoba
```

4

User Authentication

4.1 Outline

The following chapter explains how to use the *Authentication Methods* menu. This menu choice helps you to administer most means of system access.

This chapter explains how to set the following:

- default authentication method
- authentication methods on individual access routes

4.2 Outlook

Being able to control the various methods of system is an important part of a security policy, regardless of whether the system contains one machine or several. In order to maximise the ability to control system access, BoKS enables you to manipulate system access with access routes. All access routes have an authentication method which is already set. The authentication method specifies how users are determined as authorised or unauthorised for system access. In the standard configuration of BoKS, the authentication method is the user password.

An access route is composed of the 3 **W** s:

- **W** hich particular access method is available.

  Examples of access methods are: LOGIN, SU, RLOGIN, and TELNET.

- **W** here from

  Location the access method is to be used from.

- **W** here to

  Location the access method enables access to.

In addition you can specify:

- Period during the day when the access route is available.
- Days of the week when the access route is available.

By tackling the concept of system access in terms of different methods of system access you have much more control and flexibility when employing a system access policy.

4.3 Important Terms

In this chapter you encounter the following terms:

Access Method

Program used to access the system. The access methods that are controlled by BoKS:

- LOGIN

  The *login*(1B) program which is used by users when accessing the system. *login*(1B) checks the BoKS database to see whether the user is authorised to log in.

- SU (Substitute User)

  The *su*(1B) program enables users to temporarily adopt another user ID once they have logged in. *su*(1B) program checks the database to see if the user requesting to use *su*(1B) is authorised to use the program. If the user is able to use *su*(1B) all activities are logged to the user ID that the user had on logging in and not the adopted one.

- FTP (File Transfer Protocol)

  The *ftp*(1) program enables the transfer of data over the network. The daemon *ftpd*(1B) checks the BoKS database to see if the user is authorised to log in and transfer files using *ftp*(1).

- RSH (Remote Shell)

  The *rsh*(1) program enables you to execute a command on a remote machine. The *rshd*(1B) daemon checks the BoKS database to see if the user is authorised to use *rsh*(1). Other programs use *rshd*(1B) for example the *rcp*(1) program which enables you to copy files over the network from a remote machine.

- TELNET (Terminal Network Program)

  The *telnet*(1) program enables you to access a remote machine on the network from a login session on another machine. The *telnet*(1) program communicates with the *telnetd*(1) daemon which executes the *login*(1B) program on the target machine if the user is authorised in the BoKS database to use *telnet*(1).

- RLOGIN (Remote Login)

  The *rlogin*(1) program enables you to log in to a remote machine on the network from a login session on another machine. The *rlogin*(1) program communicates with the *rlogind*(1) daemon which executes *login*(1B) on the target machine if the user is authorised to use *rlogin*(1).

- REXEC (Remote Execute)

  The *rexec*(1) program enables you to execute commands via the *rexecd*(1B) daemon. *rexecd*(1B) function checks in the BoKS database to see if the user is authorised to use this function.

- XDM (X Display Manager)

  The *xdm*(1B) program is the system access program used in the X Window environment. *xdm*(1B) command checks to see if the user is authorised to use this command.

- PCNFS (Personal Computer Network File Server)

  The *pcnfs*(1) service enables you to access files on a personal computer which have been mounted using the personal computer network file server. Authentication is carried out via the daemon *pcnfsd*(1B).

For more technical information on these access methods, please refer to the *Configuration* chapter.

Access Route

Specification of the route that a user utilises to access a particular system. This route includes a specification of which access command is available to the user, where the command can be used from and where it can be used to gain access to.

Authentication Method

Pre-defined criteria placed on using an access route.

BoKS Domain

Machines which have the same BoKS database. In the standalone version of BoKS a domain consists of one machine. In the network version of BoKS a domain consists several machines with the BoKS database located on the BoKS master-server.

Password Generator

A password generator is a physical device enables the user to generate random passwords which can only be used for one login session.

S220

An S220 is a type of password generator.

System

All the machines that one BoKS database controls. In the standalone version of BoKS this is only one machine. In the network version of BoKS this is however many machines are controlled by the database which is located on the BoKS master-server. In BoKS terms the system is equivalent to a BoKS domain.

System Password

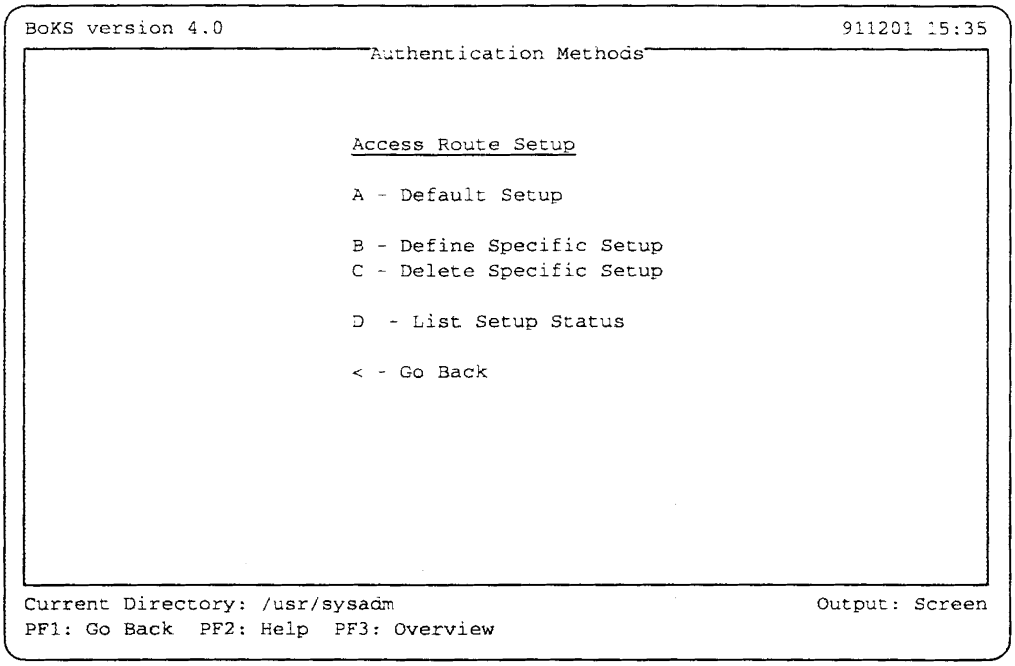
Password for a BoKS domain. This password is the same for all the machines in the BoKS domain and it is the same system password for all users.

User Password

Password for an individual user.

4.4 Authentication Methods Menu

The *Authentication Methods* menu appears as shown in figure *4.1.*



```
BoKS version 4.0                                                  911201 15:35
                         Authentication Methods

                          Access Route Setup

                          A - Default Setup

                          B - Define Specific Setup
                          C - Delete Specific Setup

                          D  - List Setup Status

                          < - Go Back

Current Directory: /usr/sysadm                                  Output: Screen
PF1: Go Back  PF2: Help  PF3: Overview
```

Figure 4.1 Sub Menu, Authentication Methods

4.5 Functionality

This menu enables you to define access routes for users individually, assigning an authentication method, other than the default one if necessary. It is possible to setup default access routes for users when they are first created. This is the usual practice of system administrators, but it is not essential. By using the functionality available with access routes you can build flexible control into all system access issues.

4.5.1 Authentication Method

An access route always has an authentication method set. An authentication method is a specification of what proof a user is to provide to show that it is the user who is allowed to use the access route. The default is always set unless an individual authentication method is set on an access route through the *Authentication Methods* menu. Different degrees of security can be applied to individual access routes. The degree of security is set by the authentication method assigned to the access route. Each authentication method has a particular code.

Authentication Method Exceptions

In general it is at the system administrator's discretion which authentication methods are used. However there are two exceptions:

1. SU

   Only authentication method `4` can be used with the SU access method. This is because the user password is always required by *su*(1B).

2. RSH

   Only authentication method `1` can be used. Once the access route is open no special authentication occurs.

Order of Precedence

The order of precedence of authentication methods is as follows:

1. All access routes disabled. No one is able to enter the system, except for `root` on the `console`.
2. User specific authentication method
3. Default authentication method

Available Authentication Methods

The following authentication methods and the number codes are available:

0 `Remove Definition (Enable Default).`

This removes the authentication method previously set on the access route and the default authentication method is used instead.

1 `Access Route Closed.`

If set as the default, this setting disables all access routes into the system, preventing system access. If set for an individual access route, this setting disables the particular access route.

NOTE *Rootaccess on the console is still available, even if this is the default authentication method.*

2 `System Password Only.`

Only the system password is required to use the access route.

4 `User Password Only.`

Users have to supply their passwords to utilise the access route.

6 `Both System Password and User Passwords.`

Both the system and user passwords have to be entered to use the access route.

12 `Compatibility Mode (eg uucp).`

All login messages are the standard UNIX ones with standard UNIX prompts. The UNIX prompts are: `login:` and `Password:`

Some programs, for example *uucp*(1) require this type of setup.

16 `UNIX Authentication (BoKS turned off)` Standard UNIX *login* (this means that BoKS is turned off). It is sometimes necessary to turn BoKS off on a particular access route so that the standard UNIX programs are used instead of the re-written DynaSoft ones.

36 `Use Password Generator if User has one.`

If the user is defined as a password generator user then the generator has to be used to utilise the access route. Otherwise the default authentication method applies.

100 `Password Generator (always)`

The one-time password generator must be used. If the user is not defined as a password generator user, the access route is inaccessible.

NOTE *All the above parameters (with the exception of method 0) can be used for all access routes as well as for specific ones.*

4.5.2 Setting an Authentication Method

Authentication methods can be implemented with two different menu choices:

1. *Default Setup*

   Authentication method for all access routes using the *Default Setup* menu choice. If there is no authentication method set on a particular access route, the default setting is applied. If the default authentication method is altered, the new default is used by existing access routes which use the default as well as new access routes created after the default is changed.

2. *Define Specific Setup*

   Authentication method for individual access routes. This is achieved by using the *Define Specific Setup* menu choice.

Default Setup

To set the default authentication method, take the *Default Setup* menu choice and enter:

`Authentication Method`

Number code of the authentication method that is to be the default value. Pressing the `Help` provides a pop-up box listing the authentication methods available. Pick and point the method you require.

In most computer environments the user's password is enough authentication for system access. The default authentication method when you purchase BoKS is 4 (user password only). If this is appropriate for your computer environment, do not alter this setting.

The following is a worked example which shows how the *Default Setup* feature can be implemented:

Tracey gives the issue of login control much thought. She feels that she would feel happiest if users had to supply two passwords to access the system. This would mean enforcing the authentication method which require each user to enter both the system-wide password and the user's personal password.

However realistically she knows that most of the users have enough problems remembering one password. As a result she sets the default to authentication method 4 "User Password Only" . To complement this authentication method, she forces the password format to be more complex by using the "Password Parameters" menu choice on the "Parameter Configuration" menu.

To set the authentication method, she selects the *Default Setup* menu choice on the *Authentication Method* menu and enters:

```
Authentication Method 4
```

After setting the default authentication method Tracey lists the access routes which need tighter security so that she can set the parameters for these on an individual basis using the *Defines Specific Setup* menu choice.

Define Specific Setup

If you want to specify an authentication method for a particular access route use the *Define Specific Setup* menu choice.

To set an an authentication method for an individual access route, take *Define Specific Setup* menu choice, enter:

`Access Route`

Access route which is to have a special authentication method. The format is:

access_method:*from_location*->*to_location*

An example is: **`LOGIN:tty14->bigbox`**

In this example the LOGIN access method is available to access the machine `bigbox` from the terminal `tty14`.

`Authentication Method`

Authentication method number code. Please refer to the *Available Authentication Methods* section in this chapter for further details.

`Start Time`

Time of day from which the authentication method applies. Format is HHMM.

`Stop Time`
: Time of day after which the authentication method ceases to apply. Format is HHMM.

`Days of Week`
: Days of the week on which the authentication method applies. Format is 1 2 3 4 5 6 7. Where "1" is Monday, "2" is Tuesday, "3" is Wednesday, and so on. For example "1234" = Monday, Tuesday, Wednesday, Thursday.

NOTE *Outside the time definitions the default authentication method applies.*

Tracey decides that she needs to tighten security on two access routes connected to the machine `bigbox`. *These access routes are:*

- *Access via the port which connects the terminal in the loading bay to the system. She feels security needs to be enhanced because unauthorised personnel are allowed into the loading bay.*
- *Access via the modem port which connects the modem to the system. She feels she needs to tighten security here because the outside world can dial into the system via the modem.*

To increase the security of these access routes, Tracey selects the *Define Specific Setup* option from the *Authentication Method* menu. She first tightens security on the terminal in the loading bay. To do this she enters:

```
Access Route              LOGIN:tty22->bigbox
Authentication Method     6
Start Time                1800
Stop Time                 0900
Days of Week              1234567
```

By entering the above Tracey has defined that the LOGIN access method is available on the port `tty22`, attached to the machine bigbox, requires that both the system password and a user password is entered (authentication method `6`) before it can be used. This level of security is enforced between 6.00 in the evening and 9.00 in the morning seven days a week.

Tracey then repeats the same procedure for `tty23` which is the modem port into the computer room and sets authentication method 6 (User and System Password) to apply twenty four hours a day, seven days a week.

4.5.3 Delete an Access Route

Access routes can not be altered once they have been created. If you consider an access route to be inappropriate once you have created, delete the access route and create a more suitable one.

Delete Specific Setup

To remove a specific authentication method from an access route, select the *Delete Specific Setup* option. This means that the default authentication method now applies to this access route.

To delete an authentication method from a specific access method, select the *Delete Specific Setup* menu choice from the *Authentication Method* menu and enter:

`Access Route`

Access route whose specific authentication method is to be deleted. The format is:

*access_method***:***from_location***->***to_location*

An example is: `LOGIN:tty14->bigbox`

In this example the LOGIN access method is available to access the machine `bigbox` from the terminal `tty14`. Pressing the function key `Help` lists a popup box with a list of all the access routes which have a specific authentication method set. Pick and point the access method whose authentication method you want to remove.

`Authentication Method`

Number code of the authentication method. You must press the `Help` function key to list the authentication method number code and pick and point the displayed value. The choice has to be made through the popup box because once you have selected the number code in this way the rest of the fields in the screen are automatically filled.

NOTE *BoKS does not accept number codes that are entered in manually.*

`Start Time`

Automatically entered.

`Stop Time`

Automatically entered.

`Days of Week`

Automatically entered.

4.5.4 Status Report

The *Authentication Methods* menu has one report menu choice which displays the setup of all access routes routes that differ from the default.

List Setup Status

The *List Setup Status* menu choice lists the following information:

`Default Authentication Method`

Specifies which is the default authentication method.

`Access Method(s)`

Access method for which has a special authentication method.

`Authentication Method`

Authentication method set for the specified access route.

`: From Host`

Location where the access method can be used from. The following alternatives are available for the *from_location:*

- terminal (/dev/ttyx) - used by the LOGIN and SU access methods.

Xterm - used by the XDM access method (applies to those using BoKS in an X-environment).

- host machine (any machine in the BoKS domain) - used by the other access methods not specified above.

`-> To Host`

Location where the access method can be used to gain access to. The following alternatives are available for the *to_location:*

- user account name - used by the SU access method to specify whose user identity may be adopted.
- host machine (any machine in the BoKS domain) - used by all access methods other than SU.

`Active Time`

Time of day and days of the week when the access method is available.

Sample Output

Sample output is as follows:

```
Default Authentication Method:  user password
Access Method(s)   : From Host -> To Host   Active Time
   Authentication Method  Access Route Setup
-------------------------------------------------------------------
LOGIN              : tty12     -> bigbox    09:00-17:00,12345
User Password only
RLOGIN             : bigbox    -> littlebox 17:30-09:00,1234567
System and User Password
```

This example shows that the access method LOGIN has the following parameters assigned to it:

- authentication method *user password only*
- access on the terminal line `tty12`
- to access the machine `bigbox`
- access is available between 9.00 in the morning and 5.00 in the evening, Monday to Friday

The second entry shows that the access method RLOGIN has the following parameters assigned to it:

- authentication method *system and user password*
- available from the machine `bigbox`
- able to access the machine `littlebox`
- access is available between 5.00 in the evening to 9.00 in the morning, seven days a week
- default authentication method is the user password

This page is intentionally left blank.

5

Menu Configuration

5.1 Outline

This chapter explains the functionality that BoKS provides for controlling access to menu choices on the BoKSADM menu. Menu choices can be configured for the following types of system administrators:

- Individual system administrators
- Group/s of administrators
- All administrators

This chapter helps you to configure the BoKSADM menu system for these three types of system administrators.

5.2 Outlook

BoKS is a menu driven product and can be significantly controlled by tailoring the menu tree.

This functionality means that by creating a number of system administrators you can divide the security administration role between a series of users without giving them full access to all security administration functionality.

It is important to realise that you can configure the BoKSADM menu system for users who are not system administrators. By default these users do not run the BoKSADM menu system as themselves. However if they log in via their normal account and then use the *su*(1B) to adopt a UID 0 account (system administrator account) and run the BoKSADM menu system, the menu tree for the user ID at login is used and not the adopted user ID.

5.3 Important Terms

The following are terms that you encounter in this chapter:

Copy Block Configuration
Copying one system administrator's menu tree configuration to another system administrator's menu tree configuration.

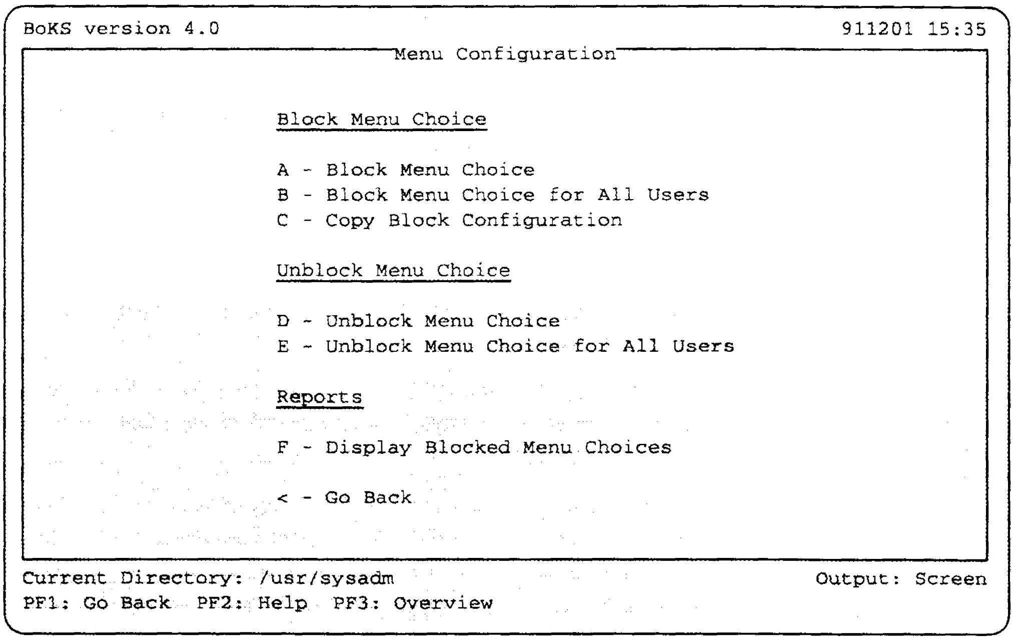
Menu Tree
Structure of menu choices which has been created using the DynaSoft menu building system MENUETT.

System Administrator
User who has a user identity number ("UID") of 0 (zero). The system administrator is sometimes referred to as the superuser or root. The default system administrator on a UNIX system is root.

User Name
User name for this menu is only the user's login name. The host name is not specified as only system administrators with access to the master-server or in the standalone version of BoKS can use the BoKSADM menu.

5.4 The Menu Configuration Menu

The menu *Menu Configuration* appears on the screen as shown in figure *5.1*.



```
BoKS version 4.0                                          911201 15:35
                         Menu Configuration

                    Block Menu Choice

                    A - Block Menu Choice
                    B - Block Menu Choice for All Users
                    C - Copy Block Configuration

                    Unblock Menu Choice

                    D - Unblock Menu Choice
                    E - Unblock Menu Choice for All Users

                    Reports

                    F - Display Blocked Menu Choices

                    < - Go Back

Current Directory: /usr/sysadm                            Output: Screen
PF1: Go Back  PF2: Help  PF3: Overview
```

Figure 5.1 Sub Menu, Menu Configuration.

5.5 Functionality

The following section explains how to use the *Menu Configuration* menu choice.

5.5.1 Blocking and Unblocking Menu Choices

Blocking a menu or menu choice from a system administrator means that this option no longer appears on this particular system administrator's version of the BoKSADM menu system. By blocking system administrators from using menus and menu choices you can divide the tasks of the system administrator. By locking system administrators into a configured version of the BoKSADM menu system, the scope of a system administrator's power can be greatly reduced.

NOTE *If you use the MENUETT Development product, you can build other menu trees which can be blocked and unblocked in the same way through this menu choice.*

Menus can either be blocked on a per system administrator basis or from all system administrators using the menu choices: *Block Menu Choice* and *Block Menu Choice for All Users*. Each menu choice has an identity code which can be blocked from a particular system administrator or from the system administrator population in general. This situation can later be reversed by using the *Unblock Menu Choice* and *Unblock Menu Choices for All Users* options.

In the case of the network version of BoKS only system administrators with access to the master-server machine are able to use the BoKSADM menu system as the BoKSADM menu system is only available on the master-server machine.

Block Menu Choice To block a menu choice for a specific system administrator take the *Block Menu Choice* and enter:

`User Name`
Name of the system administrator whose menu you would like to alter.

`Menu Tree`
Name of the menu tree that you would like to configure.

NOTE *Unless BoKS has been specially configured the only menu tree is btree.*

`ID Code`
Number of menu choices selected for blocking. Menu choices are selected by pressing `Help` and using the multi-pick technique explained in the chapter *Welcome to BoKS* to select the menu choices.

Block Menu Choice for All Users

It is sometimes advisable to globally remove a menu choice from the BoKSADM menu system so that no system administrators can access it. In this way only `root` is able to carry out the particular administration function from the command line.

The *Block Menu Choice for All Users* option is used to block menu choices from all system administrators. Select the *Block Menu Choice or All Users* option and enter:

`Menu Tree`

Name of the menu tree that you would like to configure.

NOTE *Unless BoKS has been specially configured the only menu tree is btree.*

`ID Code`

Number of menu choices selected for blocking. Press `Help` the help function key and use the multi-pick technique outlined in the *Welcome to BoKS* chapter to select the menu choices for blocking.

Unblock Menu Choice

The `Unblock Menu Choice` option is used to reinstate a menu choice on a system administrator's menu tree. This feature is often used when one system administrator is taking on the duties of another system administrator.

Take the *Unblock Menu Choice* menu choice and enter:

`User Name`

Name of the system administrator whose menu is to be altered.

`Menu Tree`

Name of the menu tree that is to be configured.

NOTE *Unless BoKS has been specially configured the only menu tree available is btree.*

`ID Code`

Number of menu choices selected for unblocking. Press `Help` function key and use the multi-pick technique outlined in the *Welcome to BoKS* chapter to select the menu choices.

An example of the application of these menu choices is as follows:

Tracey decides that she would like Dougal to be responsible for creating new users on the system and monitoring user and system activity once they are on the system. As a result she would like Dougal to be able to access the menus "User Admin", "Log Admin" and "Reports".

To achieve this she sets about blocking the rest of the menu choices that do not apply to Dougal. When Dougal does these jobs he runs as the system administrator `useradm`. The `useradm` account has been created as an account that can not be accessed by the *login*(1B) program, only by the *su*(1B) program. In addition Dougal is setup to be the only user who can su to useradm. This means that all the activity that Dougal performs as useradm is logged as performed by him. For details on how to set accounts up in this way, refer to the *User Administration* chapter.

Tracey takes the menu choice *Block Menu Choice* and enters

```
User Name   dougal
Menu Tree   btree
```

She selects the appropriate choices in the *ID Code* field by pressing `Help` and moving the cursor down to the first menu choice to be blocked. She presses the space bar by this menu choice and a plus sign appears by the side of it. She continues to use the multi-pick technique until she has selected all the menu choices she wants to block. She then presses `Return` and all the menu choices are entered for blocking in one swoop. The following is displayed in the `ID code` field:

```
ID code:  3
```

Tracey makes a mistake by blocking the *Reports* menu at the same time as blocking the other menu choices. To open the *Reports* menu she takes *Unblock Menu Choice* and enters:

```
User Name   dougal
Menu Tree   btree
```

She presses the `Help` function key to multi-pick the reports menu. Having made the selection the following is displayed on the screen:

```
ID code:   1
```

NOTE

The menu configuration is assigned to Dougal as Dougal logs in as `dougal` *and then uses su(1B) to adopt the* `useradm` *ID. When Dougal as useradm runs the BoKSADM menu system, it is dougal's ID at login that BoKS uses not the adopted user ID.*

Dougal must however adopt the user ID of useradm in order to have enough privileges to administer the system and run the BoKSADM menu system.

Unblock Menu Choice for All Users

The *Unblock Menu Choice for All Users* option is used to reinstate menu choices on a global basis. Take this menu choice and enter:

`Menu Tree`
: Name of the menu tree that is to be configured.

NOTE

Unless BoKS has been specially configured the only menu tree available is btree.

`ID Code`

Number of menu choices that have been unblocked for all users. Press the **Help** function key and use the multi-pick technique outlined in the *Welcome to BoKS* chapter to select the menu choices for unblocking.

5.5.2 Menu Configuration Administration

There are two menu choices enable you to administer menu configuration:

1. *Copy Block Configuration*
2. *Display Blocked Menu Choices*

Copy Block Configuration

To control system administrator functionality comprehensively requires much thought and subtle changes to different system administrators' menus. Often it is easier to copy a configuration from one system administrator to another and then tailor the copied configuration for each user.

The *Copy Block Configuration* menu choice enables you to copy the menu configuration of one system administrator to another. Take the *Copy Block Configuration* menu choice and enter:

`Block User`

Name of the system administrator whose menu choices are to be blocked.

`Menu Tree`

Name of the menu tree you want to configure.

`Use Configuration of User`

Name of the system administrator whose menu configuration is to be copied.

Tracey needs a rest to recover from the stress and long hours involved in installing a completely new system and decides to take a week's holiday. Tracey does all her day-to-day administration by logging in as the user `mainadm` *who has a tailored BoKSADM menu tree. She needs someone who can carry out her administration duties but does not want to let anyone else use this account. Tracey solves this problem in the following way:*

Dougal is doing so well that Tracey decides to give Dougal her system responsibilities whilst she is away. To do this she creates a system administrator called `subadm` *which Dougal is to log in as. She copies the* `mainadmin` *menu configuration over to this new system administrator.*

Tracey copies the configuration over by taking the *Copy Block Configuration* option and entering the following information:

```
Block User                      subadm
Menu Tree                       btree
Use Configuration of User     mainadm
```

In this instance Dougal logs in as `subadm` and therefore BoKS refers to the `subadm` user ID when displaying the BoKSADM menu system configuration.

Display Blocked Menu Choices

Take the *Display Blocked Menu Choices* option to see which menu choices are blocked for individual system administrators.

Take the *Display Blocked Menu Choices* menu choice and enter:

`User Name`
: Name of the system administrator whose menu configuration you wish to list.

`Menu Tree`
: Name of the menu tree whose system administrator's configuration you wish to see.

Sample Output

Sample output is as follows:

```
User Name  Menu Tree  ID Code    Menu Choice
useradm    btree      m_passw    Password Admin
useradm    btree      m_backup   Backup BoKS
```

This report shows that the user `useradm` is unable to access both the *Password Admin* and *Backup BoKS* menu choices.

For a more general description of these fields, please refer to the next section.

Description of the Fields in the Display Blocked Menu Choices Report

The output of the *Display Blocked Menu Choices* report has the following fields:

`User Name`
: Name of the user whose configuration is displayed.

`Menu Tree`
: Name of the menu tree that has been configured.

`ID Code`
: Code of the menu tree choice that has been blocked.

`Menu Choice`
: Name of the blocked menu choice as it appears on the menu.

6

Parameter Configuration

6.1 Outline

This chapter explains the functionality of the *Parameter Configuration* menu.

Not all the functionality explained in this chapter is applicable to both standalone and network versions of BoKS. This chapter clearly marks which functionality applies to which version.

BoKS parameters are divided into global and host specific parameters. The global parameters apply to all hosts in the BoKS domain. Host specific parameters are set for each individual machine.

These parameters are implemented slightly differently in the two different versions of BoKS.

Standalone Version of BoKS

In the standalone version of BoKS, the term BoKS domain is synonymous with the one standalone machine. As a result there is no differentiation between host and global parameters for the standalone version of BoKS.

Networked BoKS

In the network version of BoKS, the term BoKS domain means all the machines controlled by a common database. This database is situated on the master-server.

Using the Parameters

This chapter explains how to set the following parameters:

- User Administration Parameters

  Define the default values used when creating users.

- Login Parameters

  Define restrictions on login attempts and set the error response mode.

- Password Parameters

  Define password format and life span.

- Inactivity Parameter

  Defines period of inactivity after which a user is logged out.

- Log Parameters

  Define where the logs are stored and where the alarms are directed to.

- Language and Character Set Parameters

  Define the language and character set used to display BoKS text on the screen and in the logs.

6.2 Outlook

It is important to be able to configure your security environment so that it matches the requirements of your computer environment. When supplied, BoKS is in a standard configuration. This standard configuration meets the security requirements of most computer environments. However you may wish to fine-tune the BoKS settings. BoKS enables you to carry out almost all fine-tuning from the *Parameter Configuration* menu.

6.3 Important Terms

The following is a list of terms that you encounter in this chapter:

Character Set
Set of codes that the software uses to display text on the screen and record log events.

Default
Value which is used by a program unless another is specified.

Login Response Mode
Specifies whether *login*(1B) error messages are displayed on the screen.

Model Password
Randomly generated format which has two characters in a fixed position to which the user adds other characters.

Parameter
A setting that conditions the behaviour of a program.

Password Generator
(Only applies if you have installed the add-on password generator module.) Device which enables you to create random passwords, which are only valid for one login session. The one-time password is used as an authentication method for different access routes into and between machines in the BoKS domain.

Randomly Generated Password
Passwords that are generated by the BoKS password generator. (Only applies if you have the add-on Password Generator module.)

Search Path
List of the directories that are searched to find each program that a user tries to execute. Unless the original path setting is included, these values overwrite the default UNIX setting for $PATH.

Umask

A user's *Umask* defines the default permission settings on all files subsequently created by the user. Permission settings in UNIX are two dimensional. The user community is divided into three types of user:

- owner of the file
- system group of users which need special access to the file
- the rest of the user community not included in the previous groups

To each of these groups can be assigned all or some of the following three types of permissions:

- read
- write
- execute

The following is a table of *umask* values which manipulate the above permission settings:

Umask	Setting	User Access	Group Access	Other
000	`-rwxrwxrwx`	all	all	all
002	`-rwxrwxr-x`	all	all	read,execute
007	`-rwxrwx---`	all	all	none
022	`-rwxr-xr-x`	all	read,execute	read,execute
027	`-rwxr-x---`	all	read,execute	none
077	`-rwx------`	all	none	none

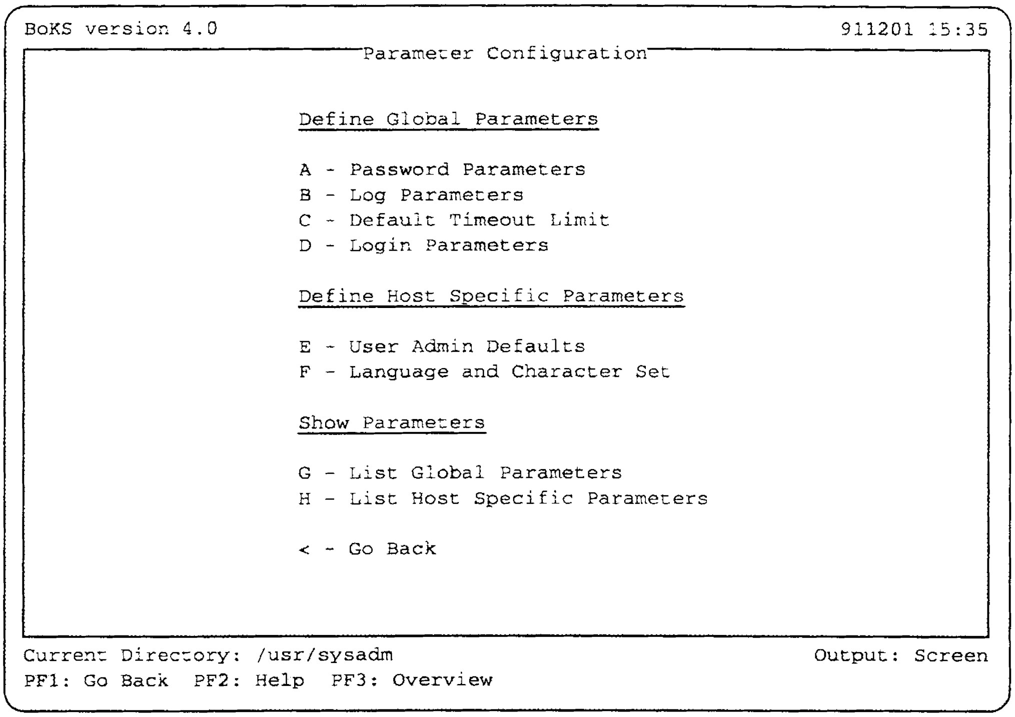
6.4 The Parameter Configuration Menu

The *Parameter Configuration* menu for the network version of BoKS appears on the screen as displayed in figure *6.1*.

The *Parameter Configuration* menu as it appears on the screen in the standalone version of BoKS is shown in figure *6.2*.

6.5 Functionality

This section explains how to use the functionality of the *Parameter Configuration* menu. If you do not wish to alter a particular value in one of the *Parameter Configuration* screens, press `Return` to move onto the next field. Alternatively, use the down arrow key to move onto the next field, or if using a mouse, move the marker to the next field where you intend to alter a value.



```
BoKS version 4.0                                                    911201 15:35
                            Parameter Configuration

                     Define Global Parameters

                     A - Password Parameters
                     B - Log Parameters
                     C - Default Timeout Limit
                     D - Login Parameters

                     Define Host Specific Parameters

                     E - User Admin Defaults
                     F - Language and Character Set

                     Show Parameters

                     G - List Global Parameters
                     H - List Host Specific Parameters

                     < - Go Back


Current Directory: /usr/sysadm                                    Output: Screen
PF1: Go Back  PF2: Help  PF3: Overview
```

Figure 6.1 Sub Menu, Parameter Configuration, BoKS Network

6.5.1 User Administration Defaults

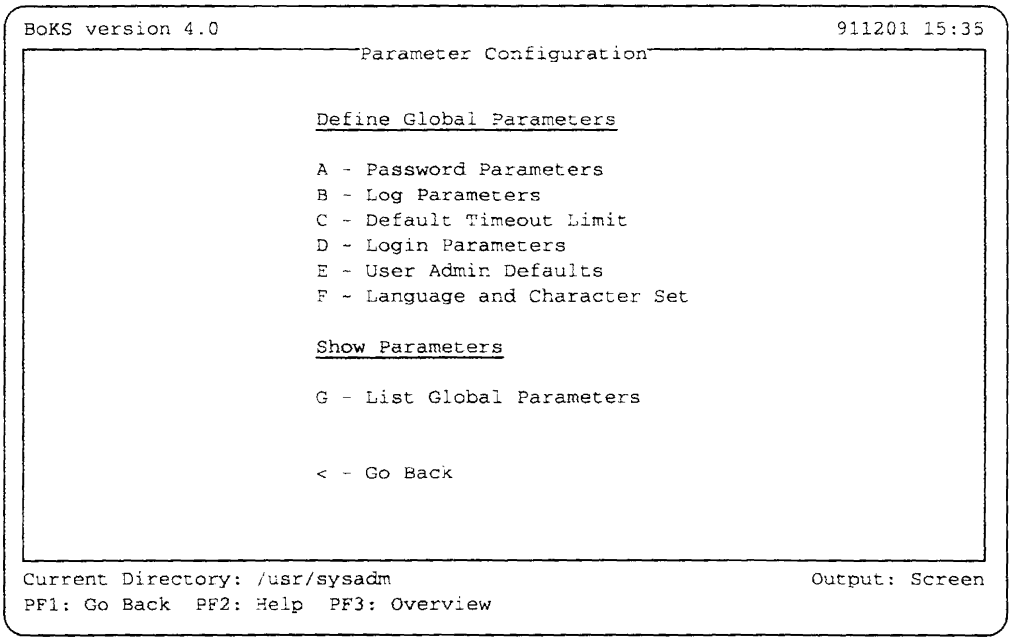
When setting up a user community it is important to create users in a linear fashion so that the users have consistent attributes and as a result are easier to administer. For example it is important that users have the following attributes in common:

- *umask* setting
- startup shell or program
- parent home directory

In this way a user community is easier to administer and the security of the system is easier to ensure. It is much easier to alter the default settings for an individual user than to create all settings from scratch each time a user is created.

These defaults are used when users are created, using the menu choices in the *User Admin* menu.

In the network version of BoKS the *User Admin Defaults* settings must be individually set for each machine in the BoKS domain.



```
BoKS version 4.0                                                   911201 15:35
 ──────────────────────────Parameter Configuration──────────────────────────

                          Define Global Parameters

                          A - Password Parameters
                          B - Log Parameters
                          C - Default Timeout Limit
                          D - Login Parameters
                          E - User Admin Defaults
                          F - Language and Character Set

                          Show Parameters

                          G - List Global Parameters


                          < - Go Back

Current Directory: /usr/sysadm                                   Output: Screen
PF1: Go Back  PF2: Help  PF3: Overview
```

Figure 6.2 Sub Menu, Parameter Configuration, Standalone BoKS

Using the User Admin Defaults Menu Choice

To alter the user administration defaults, select the *User Admin Defaults* option from the *Parameter Configuration* menu and enter:

`Host`
: Name of the host to which users are to belong.

`Parent Homedir`
: Name of the directory under which users' home directories are created.

> In the network version of BoKS, use the *Add/Modify* menu choice in the *Host Admin* menu and specify the parent home directory in the *Parent Homedir* field instead. When you execute the *User Admin Defaults* menu choice a message is displayed reminding you of this feature.

`Group`
: Name or identity number of the group to which users should belong.

`Shell`
: UNIX shell to be started when users log in.

`Start Program`
: Default program to be started when users log in.

`Umask`
: Umask settings for users. This defines the permissions for all new files that the user creates.

`Access Route`

An access route specifies how users can access the system by default. The format is as follows: *access_method* : *from_location* -> *to_location.*

An access route is made up of the 3 **W** s:

- **W**hich access method a user is able to gain system access with, for example *LOGIN, TELNET* and *XDM.*
- **W**here a user can access the system from. The *from_location* can be a terminal line (/dev/ttyXX), machine name or host group.

NOTE *Asterisk can also be used to specify that the access method can be accessed from any location. Please refer to the Access Route Setup chapter for further information.*

- **W**here the user can gain system access to. The location_to can be both a host and a host group.

For example:

```
LOGIN:tty10->bigbox
```

This example means that the user can log in on the terminal line `tty10` to the machine `bigbox`.

```
RLOGIN:bigbox->littlebox
```

This example means that the user can use the remote log in facility from the machine `bigbox` to access the machine `littlebox`.

```
FTP, RSH:bigbox->littlebox
```

This example means that the user can use both the file transfer protocol and remote shell facilities from the machine `bigbox` to access files and programs on the machine `littlebox`.

```
XDM:xterm1->bigbox
```

This example enables access via the *xdm*(1B) program from the X-terminal `xterm1` to the computer `bigbox`.

`Start Time`

Time of day from when the access route is available.

`Stop Time`

Time of day after which the access route is unavailable.

`Days of Week`

Days of the week when the access route is available.

`Path`

The command search path for the user. The full pathname must be specified. For example if you want to specify a directory called *cmds* in the directory */usr/local/bin* you must enter: **`/usr/local/bin/cmds`**. Enter the path in the following format: *full_pathname:full_pathname:full_pathname.*

NOTE *The default path is over-written when a path is specified. To append new directories to the path list enter $PATH into the list in the following way:*

$PATH:full_pathname:full_pathname:full_pathname.

For example:

$PATH:/usr/local/bin/cmds

`Security Mask`

The *umask* for the user. This specifies the permission settings that new files assume by default.

NOTE *It is not obligatory to alter all the default variables. Often it is not desirable to set/reset the values. For example, it is not always advisable to set default access routes for users as they are able to access the system from different points.*

6.5.2 Worked Example for Defining Parameters for Users in standalone BoKS

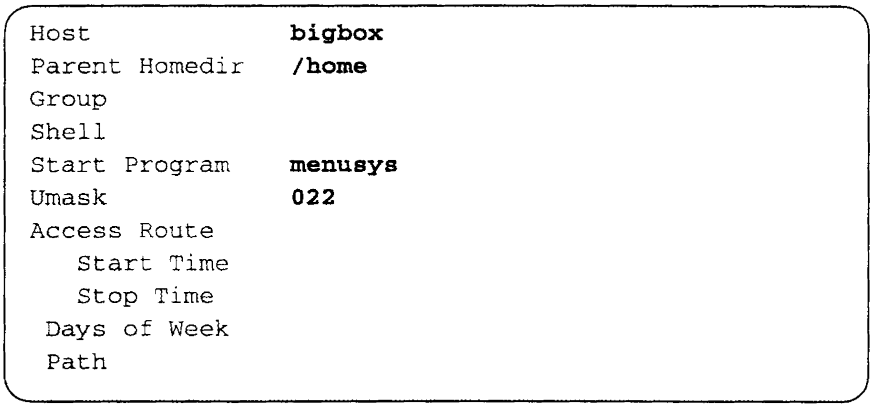
NOTE *There are two menu choices for creating users in BoKS:*

- *"Get User Data" menu choice in the User Admin menu is used for loading user who existed on the system before BoKS was installed.*
- *"Create User" option on the User Admin menu is used to create users once BoKS has been installed.*

Both these options use the User Admin Defaults settings to some extent. The "Create User" option uses all the settings. The "Get User Data" option only uses the parent home directory setting (if it is appropriate) and the access route settings.

Tracey thinks seriously about the user admin defaults before she sets them. She considers which group users should belong to. She decides to leave the group field blank for the time being. By doing this she has to enter the group manually for each user but this ensures all users do not have the same *group. She decides that most users should go into the menu system as soon as they log in. She decides that she must assign the routes individually. As most users must access a menu as soon as they login she decides that no extra PATH values need to be set and therefore the default PATH value is used. Once her decisions are made she takes the "User Admin Defaults" menu choice.*

Into the *User Admin Defaults* screen Tracey enters:



```
Host              bigbox
Parent Homedir    /home
Group
Shell
Start Program     menusys
Umask             022
Access Route
   Start Time
   Stop Time
 Days of Week
 Path
```

When Tracey subsequently loads the existing users from the */etc/passwd*(4) file into the BoKS database they assume the above settings. In future all new users that Tracey creates will also adopt the above settings unless the settings are altered.

After Tracey has loaded existing users into the BoKS database, using the *Get User Data* menu choice, she needs to set a system group and an access route for each user as she set no default values in these fields. To do this, Tracey selects the *User Admin* menu from the BoKSADM main menu. From the *User Admin* she selects the *Modify User* option to specify a group for each user. When she has taken the *Modify User* option for each user, she selects the *Access Route Admin* submenu which resides in the *User Admin* menu and specifies an access route for each user, using the *User Administration* chapter in the *BoKS Administration* guide to help her.

NOTE *When Tracey needs to create a user from scratch, as opposed to loading a user which existed prior to installing BoKS, into the database, she uses the "Create User" option on the User Admin menu.*

6.5.3 Worked Example : Network Version of BoKS

The following is a worked example of setting user admin defaults in the network version of BoKS.

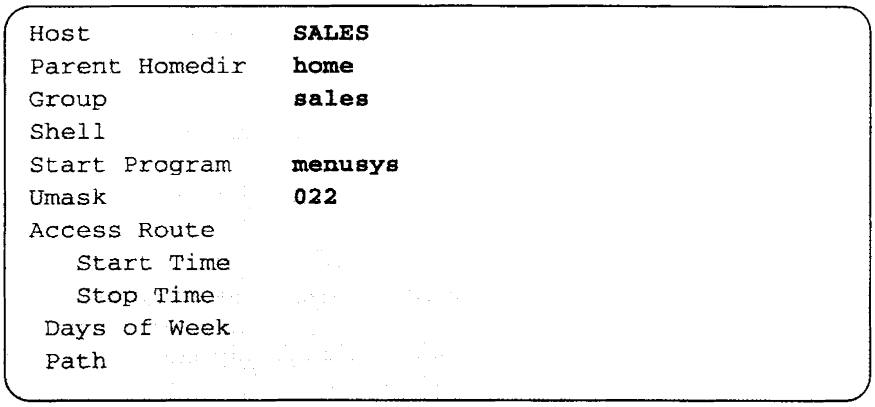
NOTE *There are two menu choices for creating users in BoKS:*

- *"Get User Data" menu choice in the User Admin menu is used for loading users which existed on the system before BoKS was installed.*
- *"Create User" option on the User Admin menu is used to create users once BoKS has been installed.*

Both these options use the "User Admin Defaults" settings to some extent. The "Create User" option uses all the settings. The "Get User Data" option uses the access route settings.

Tracey thinks seriously about the user parameters for the host group SALES. The SALES host group was set up to cover the sales and marketing machines. (Please refer to the "Host Administration" chapter for further details.) She decides to put the sales and marketing department users into a host-group called SALES as they belong to the same user group and have the same system requirements. She decides that the sales and marketing users start the in-house office automation system (Menu System) as soon as they log in. She decides that she must assign the access routes individually. As most users must access a menu as soon as they log in she decides that no extra PATH values need to be set. Once her decisions are made she takes the "User Admin Defaults" menu choice.

Into the *User Admin Defaults* screen Tracey enters:



```
Host                SALES
Parent Homedir      home
Group               sales
Shell
Start Program       menusys
Umask               022
Access Route
   Start Time
   Stop Time
 Days of Week
 Path
```

When Tracey subsequently loads the users from the */etc/passwd*(4) file onto the system they assume the above settings. She sees that some users are reported as not created. She uses the *User Administration* chapter to show her how to use the *Show Log from Get User Data* option on the *User Admin* menu. She needs to use this option to check which users were not created when she loaded the users into the database. The *User Administration* chapter advises her how to solve the problems that caused users not to be created.

In future all new sales and marketing staff that Tracey sets up will also adopt the above settings unless the settings are altered.

Tracey selects the *User Admin* menu from the BoKSADM main menu. When she has finished using the *Modify User* menu choice for each user in the SALES host group, she selects the *Access Route Admin* sub menu which resides in the *User Admin* menu to specify an access route into the system for each user. She uses the *User Administration* chapter in her *BoKS Administration* guide to help her.

NOTE *The parent home directory setting is made in the "Host Admin" menu with the "Add/Modify" menu choice.*

6.5.4 Login Parameters

The login procedure is the first level at which UNIX distinguishes between authorised and unauthorised users. It is one of the most important system obstacles against unwanted visitors. It is therefore essential that this facility is protected.

The *Login Parameters* menu choice enables you to define the number of consecutive failed login attempts that can be made against an account before the account is blocked. It is important to set this value to a reasonable value to allow legitimate users to mistype their password once or twice. At the same time it is important that crackers do not have the chance to try enough passwords to guess the right one. If a user account is blocked on account of too many failed access attempts it is possible that someone has been trying to abuse this account. If users successfully log in and see that there are a number of failed login attempts from the BoKS login message this could signify that someone has been trying to abuse the account.

NOTE *Any access attempt which fails counts as a failed log in attempt. This means that if someone attempts to access a user account with a BoKS access method other than LOGIN, for example failed RLOGIN and TELNET attempts are counted as a failed access attempts too.*

In addition the *Login Parameters* menu choice enables you to specify if you want to display the reason for a failed access attempt. By not displaying the error message you are not helping any potential would-be crackers find out why they are failing to access the system. However by displaying the error message you can more easily discover why a legitimate user can not log in.

The final login parameter enables you to specify the default number of days user accounts are valid for.

Using the Login Parameters Menu Choice

To alter the settings for the login procedure, select the *Login Parameters* option and enter:

`Failed Login Try Allowance`

Number between 1 and 99 specifying how many login attempts users can make before they are blocked.

`Login Response Mode`

Specify **v** (verbose) for the login error messages to be displayed. Specify **q** (quiet) for them to be suppressed.

`Default Life Span for Users (days)`

Number of days users accounts are to be valid for. Specify a number between 1 and 365.

6.5.5 Password Parameters

The harder a password is to guess, the less likely that someone can crack it. Unfortunately an un-obvious password is harder to remember. Users often set passwords which are easy to remember (if they set one at all). As a result the passwords are easy to guess. This has the effect of rendering UNIX's first line of defence (the login process) weak.

BoKS strengthens this line of defence in the following ways:

- Permitting system access only to those users who have a password
- Restricting the type of passwords that can be set with the *Password Parameters* menu choice.
- Restricting the use of old passwords.

The *Password Parameters* menu choice defines the format users have to follow when setting a password and determining a password's life span.

Using the Password Parameters Menu Choice

To alter the password parameters, take the *Password Parameters* menu choice and enter:

`Minimum Length`

Minimum acceptable length of a password. Specify a number between 0 and 8. The shorter the password the easier it is to guess.

`Password Format`

Specifies the format of the password. There is a choice of five settings:

0	No format Restrictions
1	At Least One Letter and One Digit
2	At Least Two Letters and Two Digits
3	Randomly Generated Password
4	Model

Enter the number of the setting most appropriate. Please refer to the *Password Administration* chapter for a detailed description of these formats.

`System Default Life Span`

Number of days between 1 and 365. This specifies how many days the password is valid for. When 10% of the life span remains, users have warning messages displayed on their terminals when they log in. Once the password has expired, users are forced to change their password the next time they log in.

`Time Limit for Expired Password`
Number between 1 and 365. This specifies the number of days during which users can log in with the old password. The first time users log in with the old password during this grace period they are forced to change their password.

`Password History Length`
Number of consecutive new passwords before old passwords can be reused. Specify a number between 1 and 20.

`Minutes between Password Changes`
Minimum number of minutes between password changes. This value specifies the shortest life span a password may have.

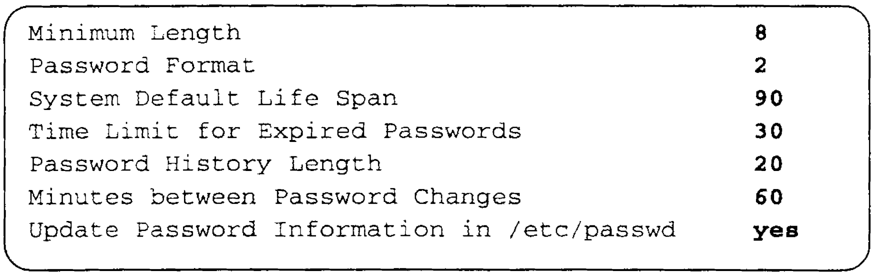
`Update Password Information in /etc/passwd`
Specifies if the */etc/passwd*(4) file is updated when a password change occurs. Enter **yes** to update the */etc/passwd*(4) file. Enter **no** to turn off */etc/passwd*(4) updating.

Tracey wants to maximise the password security on the system. She is aware that users are accustomed to sharing passwords and do not take data integrity seriously. She decides to run some system security awareness courses for all the staff and makes password security an important topic. In addition Tracey decides to tighten the password parameters. Initially she decides to use the password model for the password formatting so that users are given two random characters and have to add the rest themselves.

To set this value Tracey takes the *Password Parameters* option in the *Parameter Configuration* menu and enters:

```
Minimum Length                                 6
Password Format                                4
System Default Life Span                       90
Time Limit for Expired Passwords               30
Password History Length                        20
Minutes Between Password Changes               60
Update Password Information in /etc/passwd     yes
```

This strategy does not work very well however. Tracey's phone line is blocked every Monday morning with users who need new passwords as they have forgotten theirs. As a result Tracey decides to change the setting so that passwords are a minimum of eight characters long and have to be at least two digits and two characters. She takes the *Password Parameters* menu choice and enters:



```
Minimum Length                                   8
Password Format                                  2
System Default Life Span                         90
Time Limit for Expired Passwords                 30
Password History Length                          20
Minutes between Password Changes                 60
Update Password Information in /etc/passwd       yes
```

This strategy is much more effective, especially when users find that they can not use the same password twice.

6.5.6 Default Timeout Limit

Users often leave their terminals unattended whilst still logged in to the system. Even if users are away from their terminals for just a few minutes, it is long enough for a cracker to use the open account and cause some damage. To help prevent this occurring, BoKS times out the account after a period of inactivity.

Users working in an X Windows-environment are not logged out of the system but are locked from using the screen display. Locked out users have to enter their password to access the display. Please refer to the *Background Monitoring* chapter for further information.

Using the Default Timeout Limit Menu Choice

To alter the timeout setting, take the *Default Timeout Limit* menu choice and enter:

`Timeout Limit in Minutes`

Number between 0 and 1440 for the number of minutes of inactivity after which users are logged out. If the parameter is set to 0 (zero), the timeout facility is disabled. The default is 10.

When she first started thinking about system security, Tracey was horrified to discover that at least a third of users left their terminals logged into the system overnight. The terminals looked like the users had logged out, as the screen saver had blanked the screen but when she walked round the building pressing the space bar, a frightening number of terminals still had a connection to the system. Tracey decides to use the automatic timeout feature to modify this behaviour.

Tracey takes the *Default Timeout Limit* menu choice on the *Parameter Configuration* menu and enters:

```
Timeout Limit in Minutes    5
```

Tracey receives many complaints about this timeout feature, particularly from the Managing Director, Mr. Smythe-Jones. Tracey's first thought is to leave the setting and force users to adapt. However she likes her job and does not want to have to look for another one. She decides to adopt a strategy of gradually reducing the timeout limit. She starts with a timeout limit of twenty minutes and drops the limit by five minutes every two weeks until users are logged out after five minutes of inactivity. To put this plan into action she takes the *Default Timeout Limit* menu choice and enters:

```
Timeout Limit in Minutes    20
```

She repeats this every two weeks, entering a value five minutes less than the previous one. Within eight weeks users are back to a timeout limit of five minutes but this time with no complaints, not even from Mr. Smythe-Jones.

6.5.7 Log Parameters

Auditing system events and sending alarms about potential security hazards is an important part of a security system. BoKS is supplied with a default directory setting for log storage and a default destination for alarms. These defaults can be altered using the *Log Parameters* menu choice.

Using the Log Parameters Menu Choice

To alter the location and output of the log files and alarms, take the *Log Parameters* menu choice and enter:

`Log Directory`
: Name of the directory under which you want to store the system and user log files. The default is */boks/data.*

`Alarm Log Command`
: Command for displaying the alarms which defines where the alarms are output. There are many ways to display the alarms. The following four are common ways of displaying them:

1. Send the alarms to the console. The command for this action is:

   ```
   >/dev/console
   ```

   This is the default when BoKS is shipped. If there is no value set, the error messages are displayed on the console.

2. Send the alarms to the system default printer. The command from for this action varies from UNIX platform to platform. The two main possibilities are:

When running System V

```
|lp
```

When running BSD

```
|lpr
```

3. Append the alarms to a file, for example a file in */tmp*. The command for this action is:

```
>>/tmp/sushi2
```

6.5.8 Language and Character Set Parameters

To display all BoKS text in another language take the *Language and Character Set* menu choice. BoKS text occurs in five areas:

1. Messages from the the BoKS authentication programs (for example *login*(1B) and *su*(1B)) and all programs which use BoKS authentication programs (for example *ftp*(1) and *rsh*(1)).
2. Messages from the *passwd*(1B) program
3. Menu choice text
4. Help text

Both the language and the character set have to be specified for the language to be displayed correctly.

In the network version of BoKS the language and character set values must be defined for each machine in the BoKS domain.

Using Language and Character Set Menu Choice

To define the language and character set values, select the *Language and Character Set* option and enter:

`Host`
: Name of the host to which the setting applies. In the standalone version of BoKS this value is already entered.

`Language`
: Language to be used. Use `Help` to list the languages available.

`Character Set`
: Character set required to display the chosen language. Use `Help` to list the character sets available.

6.5.9 Displaying the Values in Network Version of BoKS

To display the BoKS default settings in the network version of BoKS, use the following two menu choices:

1. *List Global Parameters*
2. *List Host Specific Parameters*

These menu choices list the settings from the menu choices found under the *Global Parameters* and *Host Specific Parameters* column headers on the *Parameter Configuration* menu.

Global Parameters

Using the *List Global Parameters* menu choice lists the settings for all the functions administered by the following menu choices:

- *Password Parameters*
- *Log Parameters*
- *Default Timeout Limit*
- *Login Parameters*

Sample Output

A sample list is as follows:

```
Global Parameters:

Password Admin
==============
Password minimum length:                  6
Password format:                          At least two digits
                                           and two letters
Password term of validity:                31 days
Expired password term of validity:        31 days
Update /etc/passwd with passwords:        yes
Minimum Time Between Password Changes:    60
Length of Password History:               20

Log Admin and Inactivity
========================
Log directory:                            /boks/data
Log redirection command:                  |lp

Default inactivity timeout:               10 minutes

Login
=====
Number of login attempts:                 3
Login mode:                               verbose
Term of Validity for Users                365
```

List Host Specific Parameters

Using the *List Host Specific Parameters* menu choice lists the settings for the functions administered by the following menu choices:

- *User Admin Defaults*
- *Language and Character Set Parameters*

To list these values, take the *List Host Specific Parameters* and enter:

`Host`

Name of the host(group) whose parameters you want to list.

Sample Output

A sample list is as follows:

```
Host Specific Parameters:

User Admin
===========
Home Directory          /home
Group                   sales
Shell
Start Program           /usr/local/bin/menusys
Umask                   22
Access Route            *:*->*
Start Time              0900
Stop Time               1725
Week Days               12345
Path                    $PATH:/usr/local/bin/cmds

Default Login Language/Character Set
====================================
Language                eng
Character Set           7BIT
```

6.5.10 Displaying the Values in Standalone Version of BoKS

To display the values under the *Parameter Configuration* menu in standalone version of BoKS, take the *List Global Parameters* menu choice. This menu choice lists the settings for all the functions covered by the *Parameter Configuration* menu.

Sample Output

A sample list is as follows:

```
Password Admin
===============
Password minimum length:                    6
Password format:                            At least two digits
                                            and two letters
Password term of validity:                  31 days
Expired password term of validity:          31 days
Update /etc/passwd with passwords:          yes
Length of Password History:                 20
Minimum Time Between Password Changes:      60

Log Admin and Inactivity
========================
Log directory:                              /boks/data
Log redirection command:                    |lp

Default inactivity timeout:              10 minutes

Login
=======
Number of login attempts:                3
Login mode:                              verbose
Term of Validity for Users:              365

User Admin Defaults
====================
Home Directory:                          /home
Group:                                   other
Shell:                                   /bin/csh
Start Program:                           /usr/local/bin/wp
Umask:                                   022
Access Routes:                           LOGIN:tty*->bigbox
Start Time:                              0830
Stop Time:                               1800
Week Days:                               12345
Path:                                    $PATH:/usr/local/bin/cmds

Default Login Language/Character Set
======================================
Language                                 eng
Character Set                            7BIT
```

7

Backup Administration

7.1 Outline

This chapter explains how to use the *Backup BoKS* menu. It outlines the approach that BoKS has towards maintaining backups. This chapter shows you how to:

- Backup the essential files onto backup media
- Restore the essential files from backup media
- Backup system and user logs
- Restore system and user logs

7.2 Outlook

The BoKS backup facility enables you to backup the essential files in the BoKS database and other important system files.

You must backup the essential files in the BoKS database as precautionary measure, in case of the unlikely event that circumstances force you to rebuild the BoKS database. It is also important to backup essential system files in case they become corrupted or deleted.

In addition to backing up the database and essential utilities, the *Backup BoKS* menu also enables you to backup and restore the system and user logs.

7.3 Important Terms

In this chapter you encounter the following terms:

Device

Name of the backup device to be used for the backup.

Essential Files

Files important for the running of the system. These files are backed up by the BoKS backup function. This includes the files located in the BoKS database and essential system files.

System Log

Audit of events that effect the BoKS domain as a whole. For example:

- creation of users
- addition of user terminals
- all events detected by daemons
- all changes to the BoKS database

The data is stored in the system log file */boks/data/SYSLOG* by default. (See the *Parameter Configuration* chapter for further information.)

NOTE *Please refer to the "Configuration" chapter for details on the location of the* `data` *directory if this proves to be necessary.*

User Log

Log of user activity on the system. User activity includes:

- password changes
- log in attempts
- su attempts
- termination of login sessions

By default the data is stored in the */boks/data/LOG* file (see the *Parameter Configuration* chapter for further details).

NOTE *Please refer to the "Configuration" chapter for details on the location of the* `data` *directory if this proves to be necessary.*

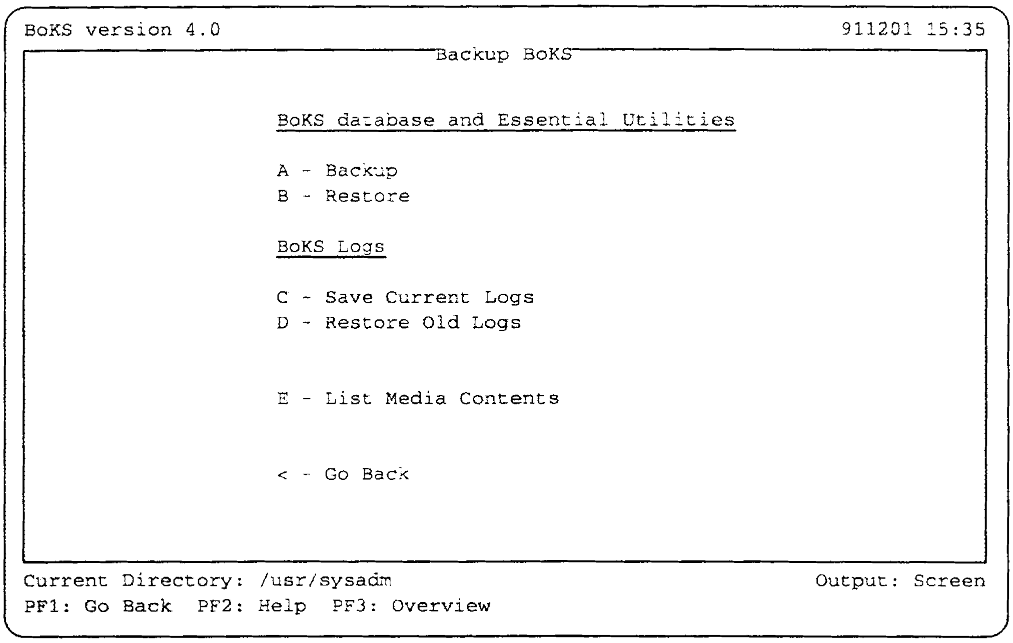
7.4 The Backup BoKS Menu

The backup BoKS menu appears as shown in figure *7.1.*

7.5 Functionality

There are two backup and two restore functions:

1. Backup and restore the BoKS database and essential system files



```
BoKS version 4.0                                                    911201 15:35
                                   Backup BoKS

                     BoKS database and Essential Utilities

                     A - Backup
                     B - Restore

                     BoKS Logs

                     C - Save Current Logs
                     D - Restore Old Logs


                     E - List Media Contents


                     < - Go Back


Current Directory: /usr/sysadm                                    Output: Screen
PF1: Go Back  PF2: Help  PF3: Overview
```

Figure 7.1 Sub Menu, Backup BoKS

2. Backup and restore the user and system administration logs

7.5.1 Backup and Restore BoKS

The *Backup* menu choices enable you to backup:

NOTE *The list of programs to be backed up may be altered by editing the /boks/bin/boks_bru (1B). Please refer to the "Configuration" chapter for further details.*

- Essential parts of the BoKS database
- The programs that BoKS replaces, for example */bin/login*(1B), */bin/passwd*(1B), and */bin/su*(1B)
- Standard UNIX counterparts to the BoKS replacement programs
- */etc/passwd(4)* file

Backup

All the files listed above are backed up when you select the *Backup* option on the *Backup BoKS* menu.

To backup these files, select the *Backup* option and enter:

`Device`

Name of the device for the backup.

The program requires you to enter **y** to confirm you wish to start the backup.

Restore

The files can be retrieved at a later date, using the *Restore* option on the *Backup BoKS* menu.

To restore these files, select the *Restore* option and enter:

`Device Unit`
: Name of the device to restore the data from.

The program requires you to enter **y** to confirm you wish to restore the files.

NOTE *You can only retrieve entire archives using the menu choice "Restore". This means that if you need to restore one particular file from the backup media, you must use the restore command from the operating system prompt and specify the flags necessary to restore individual files. On most UNIX variants, the provides this feature.*

Please consult your UNIX manual for further information on the tar (1) command.

Tracey comes into work on Monday morning and discovers that the system had crashed on Sunday night and no one can log in except for her and she can only log in on the console. She phones Duane in the Support Department at Safe&Sound Systems. Duane advises her that the problem is easily solved, as she has been backing up the BoKS database and essential system files every evening.

To enable system access, Tracey takes the latest backup of the database and essential utilities and inserts the media into the correct device. Next she selects the *Restore* option and enters:

```
Device /dev/rmt0
```

She enters **/dev/rmt0** because this is the device where the backup media is loaded. The program prompts Tracey to enter **y** to start the restore program.

Having successfully restored the essential system files and the BoKS database users are now able to access the system.

NOTE *In the above example Tracey was able to see an error message at login time because she had turned the login mode to verbose in the "Parameter Configuration" menu (see the "Parameter Configuration" chapter for further information).*

She was able to log in on the console because the system administrator is always able to access the system from the console.

7.5.2 Saving Current Logs and Restoring Old Logs

The *Save Current Logs* and *Restore Old Logs* options enable you to backup and restore the system and user logs.

Save Current Logs

The *Save Current Logs* option from the *Backup BoKS* menu enables you to copy both the user and system logs onto backup media. The logs are then automatically removed from the hard disk.

To backup the logs, select the *Save Current Logs* option and enter:

`Device`
Name of the device where the media to backup the logs is loaded.

After the logs are backed up, two events occur:

- Contents of the system and user logs are deleted from the hard disk.
- New entries are made into the current logs which detail the date, time and the contents of the logs after each backup.

It is essential that you label the backup media with the date and the contents of the backup. This means that if you need to restore the logs in the future, you can select the backup that you require by reading the media label.

Restore Old Logs

You can restore logs that have been previously saved to media by selecting the *Restore Old Logs* option from the *Backup BoKS* menu.

Take *Restore Old Logs* menu choice and insert the media into the correct device. Enter:

`Device`
Name of the device where the media is loaded.

The program prompts for confirmation that the restore is to continue. Enter **y** to confirm. The data is stored in a file specified for old system logs and user logs.

NOTE *Each time you restore an old system and user log any previously restored system and user logs are over-written. This does not effect the current system and user logs.*

7.5.3 Listing the Contents of the Media

To list the contents of the media, select the *List Media Contents* option from the *Backup BoKS* menu and enter:

`Device`
Name of the device where the media is loaded.

A list of the media contents is displayed on the screen.

7.5.4 Changing the Backup and Restore Programs

tar(1) By default, the program used to backup and restore logs is *tar(1)*. This can be altered so that another program is used by default. To do this involves altering one of the BoKS configuration files. For information on how to edit the relevant script, please refer to the *Configuration* chapter.

8

Log Administration

8.1 Outline

This chapter explains the *Log Admin* menu functionality. It gives details on the following:

System Logs

- Definition of a system log
- Contents of a system log
- How to query the current system log

User Logs

- Definition of a user log
- Contents of a user log
- How to query the current user log

Archived Logs

- Definition of an archived log
- How to query archived a system log
- How to query archived a user log

8.2 Outlook

An important part of any system security is the monitoring and logging of system events. The manner in which these logged events are presented has a great bearing on how useful the information is. Too much information can be as much of a problem as too little information. Detailed and complicated information can be as difficult to use as oversimplified information.

BoKS monitors and reports both:

- system

  and

- user

activity which occur in the BoKS domain. BoKS monitors and logs the following user activities:

- system access
- use of *su*(1B)
- inactivity timeout
- termination of a login session

BoKS logs the following system events:

- changes to the BoKS database
- background process activity
- alterations to the logs

The user and system information is presented in easy-to-use, informative reports. These reports are easy to query so that you can find the precise subset of system and user information that you require.

It is important to be able to archive old logs easily. It is equally important to retrieve information from archived material. Logs can occupy a significant amount of disk space and are often queried on a day to day basis making the information quickly obsolete. Simply deleting logs is not a solution to a lack of disk space. System and user information can be very valuable in the long term and therefore keeping archived copies is essential.

The *Backup BoKS* menu enables you to archive the BoKS logs on a regular basis. The *Backup BoKS* menu also enables you to restore the logs. The *Log Admin* menu enables you to query the restored logs precisely as you query current logs.

8.3 Important Terms

The following is a list of terms that you encounter in this chapter:

Alarm Events

System event which BoKS classifies as an alarm event. Notification of the alarm event is displayed in the manner specified in the *Log Parameters* menu choice, on the *Parameter Configuration* menu.

Access Route

Specifies the route that a user utilises to access a particular system. The access route is composed of the 3 **W** s:

- **W** hich method of system access is available (access method)
- **W** here the user is using the access method from (location_from)

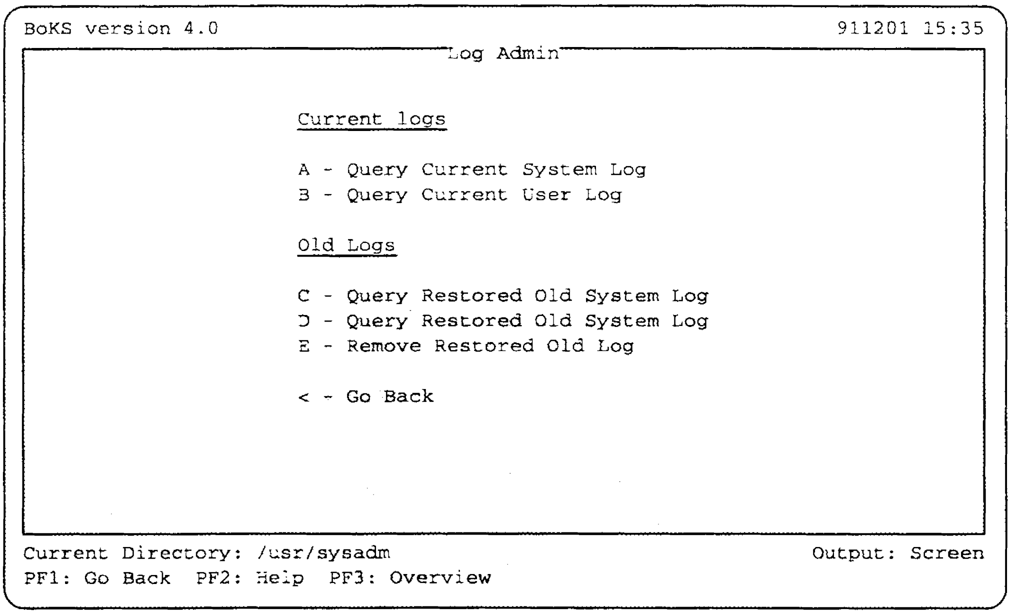
- W here the user is using the access method to gain access to (location_to)

Search Text

String of characters to search. The log entries displayed contain this particular string of characters.

8.4 The Log Administration Menu

The *Log Admin* menu appears on the screen as illustrated in figure *8.1.*



```
BoKS version 4.0                                                911201 15:35
                                   Log Admin

                      Current logs

                      A - Query Current System Log
                      B - Query Current User Log

                      Old Logs

                      C - Query Restored Old System Log
                      D - Query Restored Old System Log
                      E - Remove Restored Old Log

                      < - Go Back

Current Directory: /usr/sysadm                                Output: Screen
PF1: Go Back  PF2: Help  PF3: Overview
```

Figure 8.1 Sub Menu, Log Admin

8.5 Functionality

The following section explains how to use the functionality available on the *Log Admin* menu. The functionality can be divided into two parts:

- Querying the system and user logs that are current on the system
- Querying system and user logs that have been archived

8.5.1 Querying Current System and User Logs

The following section explains how to query the system and user logs using the *Query Current System Log* and *Query Current User Log* menu choices. The current logs are the ones that are live on the system and are continuously being updated by the BoKS system monitoring processes. The logs cease to be live when they are copied over to backup media and are deleted from the hard disk. New live logs are automatically created when this occurs.

Query Current System Log

The menu choice *Query Current System Log* lists the following information:

- Users added to the BoKS database
- Hosts added to the BoKS database
- Access routes added and removed for individual users
- User and system password changes
- BoKS parameters changed on a user and system-wide basis
- Access routes opened and closed on the system
- Modified user setups
- Files added and removed from the file monitoring list
- Results of system monitoring
- BoKS program usage
- Number of system integrity warnings

This feature is particularly useful when experiencing irregular system behaviour. It is advisable to check these logs on a regular basis so that you are familiar with system activity.

Query Current User Log

The *Query Current User Log* on the *Log Admin* menu enables you to read reports of the following activities:

- Usage of *su*(1B)
- System access attempts
- Inactivity timeout
- Password change carried out by the user
- Termination of login sessions

Querying Both Logs

Querying system and user logs involves the same procedure. The difference between them is that different files are interrogated and as a result different information is displayed.

To query either the system or user logs, select one of the following menu choices from the *Log Admin* menu:

- *Query Current System Log*
- *Query Current User Log*

NOTE *If the fields are not altered, then the existing values are used.*

Enter:

```
Alarm Events Only? (Y/N)
```

Specify **y** if only alarm events are to be displayed. Specify **n** if both alarm and standard system events are to be displayed. By default both types of events are reported.

`User Name`
: Host(group)name coupled with the login name of the user in the format *hostname : username.* Following this the *Host* field is automatically filled out with the host that the user is coupled with.

`Host`
: Host(group) to which the user is coupled. If the user name has been entered in the format *hostname : username,* then this field is automatically filled out.

`Terminal`
: Terminal that the event was executed from, for example */dev/tty**.

`Search Text`
: Text that is searched for in the logs. Records which contain this text and meet any other criteria that has been set in this screen are displayed. The wild cards "*" and "?" may be used in the search string. For example by entering ***password*** all the events containing the word "password" are displayed.

`Start Date`
: The date of the earliest log event you want to include in the report.

`Stop Date`
: The date of the latest log event you want to include in the report.

Sample Output

Sample output from the system log is as follows:

```
Date          Host   Tty  User Name  Text
------------ ------ ---- -----      ----------
921225:09:00 bigbox tty2  abc       Password changed for
for user abc
921226:10:05 bigbox tty12 fred      Login mode: verbose
921227:13:22 bigbox tty4  jack      User bigbox:mary created
```

Sample output from the user log is as follows:

```
Date         Host   Tty  User Name  Text
------------ ------ ---- -----      ----------
921225:00:00 bigbox tty2 abc        Successful
SU from user abc to root
921226:09:08 bigbox tty3  fred       Successful
login: fred
921226:10:01 bigbox tty3  fred       Logout
921227:13:24 bigbox tty7  mary       Successful
login: mary
```

The different fields are explained in the following section:

Explanation of the System and User Log Fields

The fields in the system and user logs give the following information:

`Date`
Date and time the event occurred.

`Host`
Machine on which the event occurred.

`Tty` Terminal (terminal device name) where the event occurred.

`User Name`
User to whom the event is attributed. This is the user who owned the process that caused the event.

`Text`
Explanation of what occurred.

Brian reports to Tracey that when he logged in that morning, BoKS reported that he had last logged in on Sunday at four in the morning. This concerns him as he was not at work at four in the morning on Sunday. Tracey checks the user log by taking the Query Current User Log menu choice and enters:

```
Alarm events only? (Y/N) n
User                     brian
Host                      bigbox
Terminal                 tty12
Search Text
Start Date               921106
Stop Date                921109
```

The resulting report is displayed:

```
Date         Host   Tty   User  NameText
------------ ------ ----  -----     ----------
921106:04:00 bigbox tty12 brian     Successful
login: brian
921106:04:10 bigbox tty12 brian     Unsuccessful
SU from user brian to root
921106:04.45 bigbox tty12 brian     Logout
921107:09:00 bigbox tty12 brian     Successful
login: brian
```

The output shows that someone did indeed log in as Brian at 4 am and logged out at 4.45. An su attempt was also made but was unsuccessful.

Tracey takes two course of action. As a short term measure Tracey changes Brian's password and makes sure that he does not stick the password underneath his desk this time. As a more permanent measure she makes sure that Brian is only authorised to log in between 8.30 in the morning and 6.00 at night.

8.5.2 Restored Logs

BoKS enables you to query archived system and user logs. This functionality means that you can archive system and user logs on a regular basis to save disk space. At the same time you can easily retrieve the archive using the *Backup BoKS* menu and interrogate the restored data in precisely the same fashion as you query the current logs.

In addition the *Remove Restored Logs* menu choice enables you to delete the restored archived logs once they are no longer required so that disk space is not taken up unnecessarily.

Query Restored Old System and User Logs

The menu choices *Query Restored Old System Log* and *Query Restored Old User Log* on the *Log Admin* menu are used to query the logs restored using the menu choice *Backup BoKS.* The procedure for querying these logs is exactly the same as when querying the current system and user logs.

NOTE *These logs must first have been restored using the "Backup BoKS" menu. Please refer to the "Backup BoKS" chapter for further details.*

To query a restored system or user log, select one of the following options:

- *Query Restored Old System Log*
- *Query Restored Old User Log*

Enter:

`Alarm events only? (Y/N)`

Specify if the alarms only or both alarms and standard system events are to be displayed. Enter **Y** for alarms only. Enter **N** for both system events and alarms. By default both are reported.

`User Name`

Host(group)name coupled with the login name of the user in the format *hostname : username.*

`Host`

Host whose events you want to display. If you entered the user name in the previous field in the format *hostname : username* the hostname is automatically entered.

`Terminal`

The terminal where the program is executed from, for example */dev/tty*.*

`Search Text`

Text that is searched for in the logs. Records which contain this text and meet any other criteria that has been set in this screen are displayed. The wild cards "*" and "?" may be used in the search string. For example by entering **`*password*`** all the events containing the word "password" are displayed.

`Start Date`

The date of the earliest log event you want to include in the report.

`Stop Date`
The date of the latest log event you want to include in the report.

NOTE *It is not obligatory to enter data into these fields. If specified, they make up the criteria under which the logs are queried. If the fields are left blank then events since the last backup of the logs are displayed.*

The output is in the same format as the current system and user logs.

Remove Restored Old Logs

The restored logs can be removed once they are no longer required by taking the *Remove Restored Old Logs* option from the *Log Admin* menu.

NOTE *Only restored archived logs can be removed from the system with the "Remove Restored Old Logs" menu choice. Current logs can not be removed in this manner.*

Select the *Remove Restored Old Logs* and enter:

`OK to Remove Old Logs? (Y/N)`
Enter **Y** to confirm the deletion. Enter **N** if you want to abort the deletion.

Entering **Y** deletes the restored logs. Entering **N** aborts the deletion and you return to the *Log Admin* menu.

8.5.3 Re-classifying Alarms

Certain events in BoKS are characterised as extremely serious and are immediately output as alarms as well as being logged in the log files. This is so that the system administrator is able to react to these events immediately. In the standard configuration of BoKS there are a number of events which are classified as alarms. An example of this is the usage of the *su*(1B) command.

The system administrator is able to define which events are treated as alarms. You may both specify normal events to be treated as worthy of an alarm and "demote" alarms to normal events, so that events that were previously treated as an alarm are now treated as a normal system event. See the *Configuration* chapter for further information.

9

Reports

9.1 Outline

This chapter explains the range of system reports that BoKS enables you to produce. The following reports are explained:

- *User Data*

  Displays the key user parameters
- *Full User Status*

  Provides a detailed user setup report
- *Login/Logout Time*

  Displays users' login and logout times
- *Added Access Routes*

  Displays access routes available for each user and the time of the day they are available
- *BoKS System Information*

  Displays the BoKS setup parameters
- *List Setup Status*

  Lists the authentication mode for each access route
- *Integrity Check Report*

  Displays the results of the system integrity check

9.2 Outlook

System information is only effective and useful if it can be analysed and manipulated quickly. DynaSoft ease the load of the system administrator by collating system information in a series of easy-to-understand reports which the administrator is able to view on the screen or send to the printer using the direct command `Ctrl` `U` (see the chapter entitled *Welcome to BoKS*)

This chapter explains the report contents and shows why the information is necessary.

9.3 Important Terms

In this chapter you encounter the following terminology:

Access Route

Specification of the route that may be utilised to access a particular system. An access route is comprised of the 3 **W** s:

- **W** hich system access program to be used (access method)
- **W** here the user is able to use the access method from (location_from)
- **W** here the user is able to gain access to with the access method (location_to)

The type of entry used to specify *location_from* and *location_to* depends on the requirements of the access method.

Alarm Log Command

Command used to define where and how the alarms are displayed.

APPLPATH

Environment variable which defines where the majority of BoKS programs are located.

GID (Group ID)

Identity number of the group that a user belongs to. The expression GID is often used.

Home Directory

Location (directory) on the file system under which a user may create files and directories.

Su

A UNIX program, */bin/su(1B)* ,which allows users to adopt the identity of other users, although the system knows that it is the original user operating under another identity.

UID (User ID)

Identity number that a user is assigned when created. The expression UID is often used.

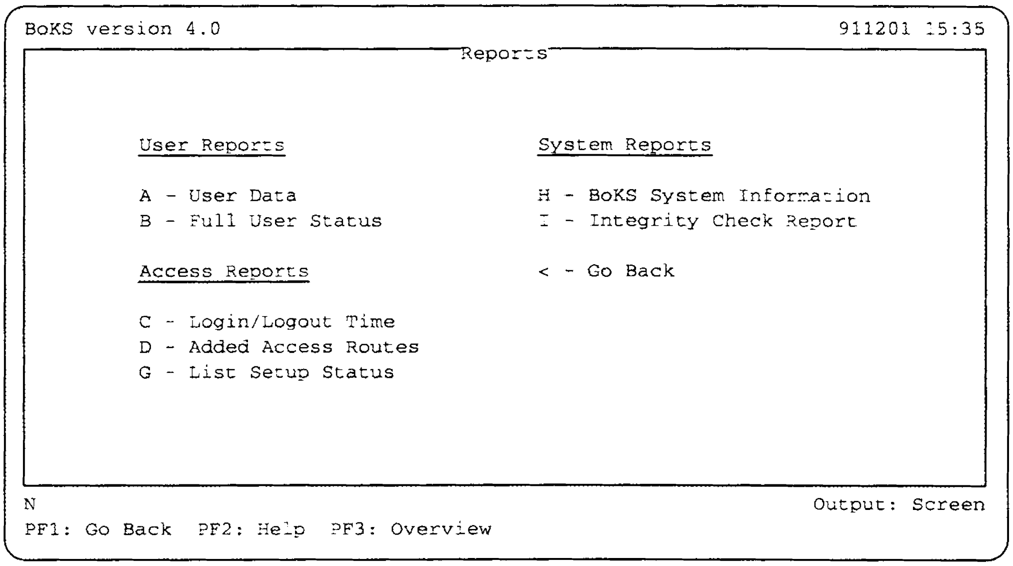
9.4 The Reports Menu

The *Reports* menu appears on the screen as illustrated in figure *9.1*

9.5 Functionality

The following section explains the functionality found in the *Reports* menu.

NOTE *The reports explained below can be printed on the printer by changing the output device before taking the menu choice. To do this use the direct command* `Ctrl` `U` *Specify* `printer` *as the output device. You are prompted to specify which printer you wish it to go to.*



```
BoKS version 4.0                                                911201 15:35
 ----------------------------------Reports-----------------------------------


          User Reports                      System Reports

          A - User Data                     H - BoKS System Information
          B - Full User Status              I - Integrity Check Report

          Access Reports                    < - Go Back

          C - Login/Logout Time
          D - Added Access Routes
          G - List Setup Status



 ----------------------------------------------------------------------------
N                                                             Output: Screen
PF1: Go Back  PF2: Help  PF3: Overview
```

Figure 9.1 Sub Menu, Reports

The output of all reports are sent to the specified printer each time it is executed until you either leave BoKS or change the output device back to `screen.`

9.5.1 User Reports

The following section outlines the user report facilities.

User Data

The *User Data* menu choice on the *Reports* menu provides you with the key setup information for users on the system. To display this information, select the *User Data* option and enter:

`Host`

The name of the host whose users you would like to list. If you are using the standalone version of BoKS, this field is already completed. If you are using a network version of BoKS and would like information about users on all machines in the network, leave this field blank.

`Sort by`

The sorting order of the data. The sorting possibilities are as follows:

0 `User Name.` Enables you to list the user records in alphabetical user name order.

1 `User ID.` Enables you to list the user records by UID.

2 `Group ID.` Enables you to list the user records by GID.

3 `Password Expire Date.` Enables you to list the user records by password expire date, listing those that are blocked first, followed by user records ordered by oldest password expire dates.

4 `User Expire Date.` Enables you to list the user records by oldest user expire date first.

Sample Output

Sample output when sorting by user name looks as follows:

```
User          UID  GID   Password   User    Flt  Tout  Comment
                         Expire     Expire
bigbox:audit   9   audit blocked    930814  0     10
bigbox:brian  109  staff 921225     930101  0     10  Brian Brain
```

Explanation of the User Data Report Output

The *User Data* report displays the following data:

`User`
Host(group) name that the user belongs to coupled with the user's login name

`UID`
Identity number of the user

`GID`
Group identity number of the user's group

`Password Expire`
Date that the user's password expires

`User Expire`
Date after which the user's account on the machine is no longer valid

`Flt`
Number of current failed login tries (this value is reset to 0 every time the user successfully logs in)

`Tout`
User's timeout limit in minutes

`Comment`
Full name of the user/comment about the user

Full User Status

The *Full User Status* menu choice on the *Reports* menu provides detailed information about an individual user or users.

Select the *Full User Status* option and enter:

`User`
Host(group)name and the user login name in the following format *hostname : login name.*

NOTE *If you do not enter the name of the user you receive reports about all the users in the database. You may however specify an individual user* *name or specify a group of users by using wild cards. For example by entering hostname : b* the reports of all users whose user names begin with b are displayed.*

Sample Output

Sample output appears as follows:

```
Username:                          bigbox:brian
User ID:                           109
Group ID:                          10
Comment:                           Brian Brain
Home directory:                    /home/brian
Shell:                             /bin/csh
Inactivity timeout:                10 minutes
Time dependent timeout:            yes
Inactivity timeout checking:       CPU, keyboard, screen
Password last changed:             921031
Password valid until :             921131
User valid until:                  930101
Number of failed logins:           0
User blocked:                      no
Assigned Access Roots:             LOGIN:tty12->bigbox
                                    08:30-18:00, 12345
                                   SU:tty12->root
                                    08:00-19.00, 12345
```

An explanation of these fields is made in the following section.

Explanation of Full User Status Report

The *Full User Status* report displays the following information:

`Username`

Host(group)name coupled with the login name of the user

`User ID`

Identity number of the user

`Group ID`

Identity number of the group that the user belongs to

`Comment`

Any comment assigned to the user during setup

`Home directory`

Where the user resides on the system

`Shell`

Shell that the user starts up when logging in

`Inactivity timeout`

Timeout limit set for the user in minutes

`Time dependent timeout`

Specifies if the user has a special timeout limit which applies to particular day of the week, during a certain time of day

`Inactivity timeout checking`
Specifies which criteria are used to establish if a terminal session should be timed out

`Password last changed`
Date the user's password was last changed

`Password valid until`
Date the user's current password is valid until

`User valid until`
Date user account expires

`Number of failed logins`
Number of failed logins since the last successful one

`User blocked`
Specifies if the user is temporarily blocked from the system. If the user is blocked an explanation is provided

`Assigned Access Routes`
Access routes that the user may use and when these are accessible

9.5.2 Access Reports

The following section explains the range of system access reports available from the *Reports* menu. The access reports are:

- *Login/Logout Time*
- *Added Access Routes*
- *List Setup Status*

Login/Logout Time

The *Login/Logout Time* menu choice on the *Reports* menu is used to report the users' latest login and logout times (if the user has logged out, otherwise only the login time is specified).

Select the *Login/Logout Time* option and enter:

`Host`
Name of the host(group) whose login times you would like to check

NOTE *In the standalone version of BoKS the menu choice displays the report immediately as no host name is required.*

In the network version of the product leaving the host field blank means that all login access for all machines in the BoKS domain are displayed.

Sample Output

A sample report looks as follows:

```
User          Comment        Login  Time Logout Time Login Tty
-----------------------------------------------------------------
bigbox:brian Brian Brain    921030 0845 921030 1735 bigbox:tty12
bigbox:alice Alice Springs 921030 0800      -      bigbox:tty14
```

This report shows that Alice is still logged in on `tty14` on the machine `bigbox` as the *Logout Time* field has a hyphen in it.

Explanation of the Login/Logout Time Report

The *Login/Logout Time* report displays the following information:

`User`
: Host(group)name coupled with the user's login name

`Comment`
: Further user information

`Login Time`
: Date and time the user last logged in

`Logout Time`
: Date and time the user logged out after the last login session. If the user is still logged in a hyphen is entered in this field

`Login tty`
: Terminal line on which the user logged in

Added Access Routes

The *Added Access Routes* menu choice on the *Reports* menu displays the access routes that have been assigned to individual users. Select the *Added Access Routes* menu choice and enter:

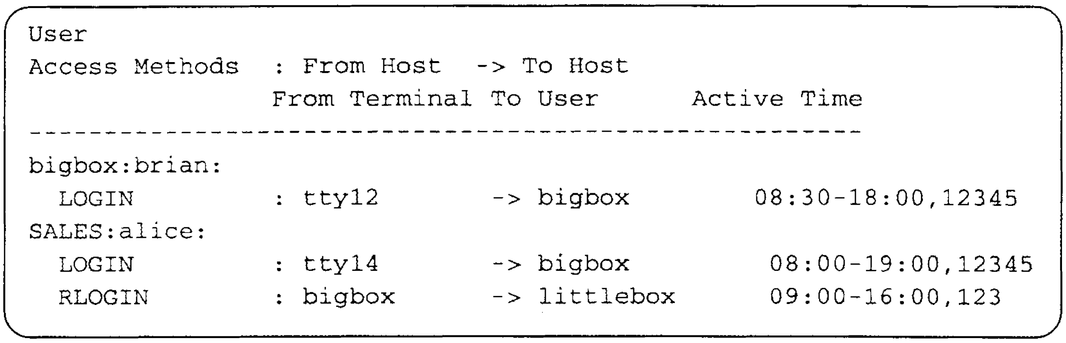
`Host`
: Name of the host(group) whose access routes you would like listed

NOTE *In the standalone version of BoKS taking the menu choice displays the report immediately as it is not necessary to fill out the host field.*

In the network version of the product, leaving the host field blank means that all access routes all machines in the BoKS domain are displayed.

Sample Output

A sample report looks as follows:



```
User
Access Methods  : From Host   -> To Host
                  From Terminal To User      Active Time
-------------------------------------------------------
bigbox:brian:
  LOGIN         : tty12        -> bigbox         08:30-18:00,12345
SALES:alice:
  LOGIN         : tty14        -> bigbox          08:00-19:00,12345
  RLOGIN        : bigbox       -> littlebox       09:00-16:00,123
```

Explanation of the Added Access Routes Report

The *Added Access Routes* menu choice lists the following information:

`User`

Hostname coupled with the username for whom the listed access routes apply. The format is *Host(group)name : username.*

`Access methods`

Means of access that have been allocated to each user.

NOTE *An asterisk denotes all access methods.*

`:From Host`

`From Terminal`

Location from where each access method may be used (in the case of LOGIN and SU this is tty lines, in the case of other programs this is a host(group) name).

NOTE *An asterisk denotes that the access method is available from any where within the BoKS domain.*

`-> To Host`

`To User`

Location which can be accessed by a particular access method. This can be a machine in the BoKS domain or in the case of SU a username whose user ID can be adopted.

`Active time`

Time of the day and days of the week when each access route is available.

This listing displays the access route information for all the users on a specified host.

List Setup Status

The *List Setup Status* menu choice lists the following information:

`Access Method`

Access method which has a special authentication method.

Authentication Method

Authentication method set for the specified access route.

The following authentication methods are available:

Locked Access Route is closed

Standard UNIX login Operating system's normal authentication method is used (and BoKS is switched off on this access route).

User Password User password is entered.

System Password System password is entered.

System and User Passwords Both user and system passwords are entered.

Compatible Mode Prompts displayed at login are compatible for programs such as *uucp*(1).

If you have purchased the *Password Generator* add-on module the two following authentication methods are also available:

Password Generator (if user has one)

One-time password is to be entered if the user is a registered S220 user. (See the *Password Generator* chapter for further details.)

Password Generator (Always)

One-time password must always be used, which means that if the user is not registered as an S220 user they can not use this particular access route.

: From Host

Location where the access method can be used from. The following alternatives are available for the from_location:

- terminal (/dev/ttyx) - used by the LOGIN and SU access methods
- Xterm - used by the XDM access method (applies to those using BoKS in an X Windows-environment)
- host machine (any machine in the BoKS domain) - used by the other access methods not specified above

-> To Host

Location where the access method can be used to gain access to. The following alternatives are available for the to_location:

- user account name - used by the SU access method to specify whose user identity may be adopted
- host machine (any machine in the BoKS domain) - used by all access methods other than SU.

Active Time

Time of day and days of the week when the access method is available.

Sample Output

Sample output is as follows:

```
Access Method(s)   : From Host -> To Host   Active Time
   Authentication Method
LOGIN              : tty12     -> bigbox    09:00-17:00,12345
User Password only
RLOGIN             : bigbox    -> littlebox 17:30-09:00,1234567
System and User Password
```

This example shows that the access method LOGIN has the following parameters assigned to it:

- authentication method *user password only*
- access on the terminal line `tty12`
- to access the machine `bigbox`
- access is available between 9.00 in the morning and 5.00 in the evening, Monday to Friday

The second entry shows that the access method RLOGIN has the following parameters assigned to it:

- authentication method *system and user password*
- available from the machine `bigbox`
- able to access the machine `littlebox`
- access is available between 5.00 in the evening to 9.00 in the morning, seven days a week

9.5.3 System Reports

The following section explains the system reports available to you from the *Reports* menu.

BoKS System Information

To display the system parameter settings, select the *BoKS System Information* menu choice on the *Reports* menu. This automatically displays the following system parameters:

`Database last changed`
: The date and time that the BoKS database was last updated

`Number of login attempts`
: Number of failed login attempts before a user is blocked from the system

`Default inactivity timeout`
: System default in minutes after which users are logged out if they have been inactive

Password minimum length
Minimum length of any password

Password term of validity
Default number of days a password is valid for

Password format
Default password setting that all new passwords must conform to

System Password Defined
Specifies whether a system password has been set

Update /etc/passwd with passwords
Specifies whether the password field in */etc/passwd (4)* is updated

Expired password term of validity
Specifies how long the grace period is once a user's password has has expired

Login mode
Specifies if the reason for a failed login is to be displayed at the user's terminal

Language in logs
Specifies which language is used in the BoKS logs

Log directory
Specifies which directory the logs are stored in

Log redirection command
Specifies the command used to redirect the alarms that BoKS produces

Default system login status
Default authentication method for accessing the system

Length of Password History
Consecutive number of new passwords a user must specify before using an old one.

Minimum Time Between Password Changes
Shortest lifespan of a password.

BoKS Product Directory (APPLPATH)
System location where BoKS is installed.

BoKS System Directory (BOKSDIR)
System location of BoKS database

Sample Output

A sample report looks as follows:

```
Database last changed:                 920101
Number of login attempts:              3
Default inactivity timeout:            10 minutes
Password minimum length:               6 characters
Password term of validity:             150 days
Password format:                       Model
System password defined:               yes
Update /etc/passwd with passwords:     yes
Expired password term of validity:     25 days
Login mode:                            verbose
Language in Logs:                      eng
Character set in logs:                 7BIT
Log directory:                         /boks/data
Log redirection command:               >/dev/console
Default system login status:           User password
Length of Password History:            20
Minimum Time Between Password Changes: 60
Product Directory (APPLPATH)           /usr/dynprods/boks
BoKS System Directory (BOKSDIR)        /boks
```

Integrity Check Report

The *Integrity Check* report menu choice on the *Report* menu displays:

- Level of seriousness of each warning
- Warning message
- In the case of the most serious warnings, displays, the fix reference number if one exists.

Select the *Integrity Check Report* menu choice and enter:

`Host`

Name of the host to which the integrity check report applies.

`Show Excluded Warnings`

Specify **Y** to included excluded warnings in the report. The default is set to 'no'.

Sample Output

The following is sample output from the integrity check report:

```
Level Warning
-------------------------------------------------------
Warning for Host: bigbox Report Created: 92.08.20:01.07

0)        /bin/login could have a hole/bug (CA-89:01)
0)        /bin/mail could have a hole/bug (CA-91:01a)
1)    User brian's home directory /home/brian is mode 0777
2)        /bin/fd0 is group readable
2)    /usr/adm/sulog is world readable
```

This page is intentionally left blank.

10

Background Monitoring

10.1 Outline

This chapter explains how to use two elements of the BoKS system monitoring functionality. These two elements are:

- file monitoring
- inactivity timeout

Collectively these elements are termed *background monitoring* because they are monitoring features which constantly run in the background and monitor the system activity of the user community. (For a more rigorous technical explanation, please refer to the *Configuration* chapter.)

The results of background monitoring form part of the data reported in the the menu choices on the *Reports* menu.

This chapter explains how to setup and run:

- File monitoring
- Inactivity timeout
- X-display lock for those running BoKS in an X-Windows environment

10.2 Outlook

System monitoring is an important feature of any security system. BoKS has two types of system monitoring features:

1. Background Monitoring (file and inactivity monitoring)

   Background monitoring is carried out by background processes (daemons) which periodically monitor:

- user activity
- changes to file content, permissions and file deletion
- system clock activity

The results of background monitoring decide and instigate the following:

- decision to log off users who have exceeded their inactivity limit
- logging of changes to file content, permission changes and file deletion
- logging of changes to the system clock
- locking an X display for those running BoKS in an X Windows-environment

2. System Integrity Checking

The system integrity checker monitors potential and actual security threats to the system. Its findings are reported in two comprehensive reports. The functionality of the integrity checker is explained in the *Integrity Check* chapter.

10.3 Important Terms

In this chapter you encounter the following terms:

Nice Value

This value represents the priority of a process. The priority can be lowered by incrementing the nice value. The higher the increment the lower the priority. The range of incrementing varies from UNIX variant to UNIX variant. On BSD systems the increment range is between -19 and +20. On System V machines the range is between 0 and 40.

XDM

X Display Manager program which administers the process of logging into the system from an X-terminal via the XDMCP protocol. Users enter their names and passwords into a window containing login and password prompts.

NOTE

Older X-terminals do not support XDM and enable access via another method, for example telnet(1).

X-Server

Software essential to the X-Window system which enables the output from programs to be displayed. The X running under Motif, Open Look and DECWindows window managers all use an X-server. The X-server can run as a program on a workstation. It may also be built into the X-terminal so that the X-terminal can only run as an X-server.

10.4 The Background Monitoring Menu

The background monitoring menu appears on the screen as shown in figure *10.1.*

10.5 Functionality

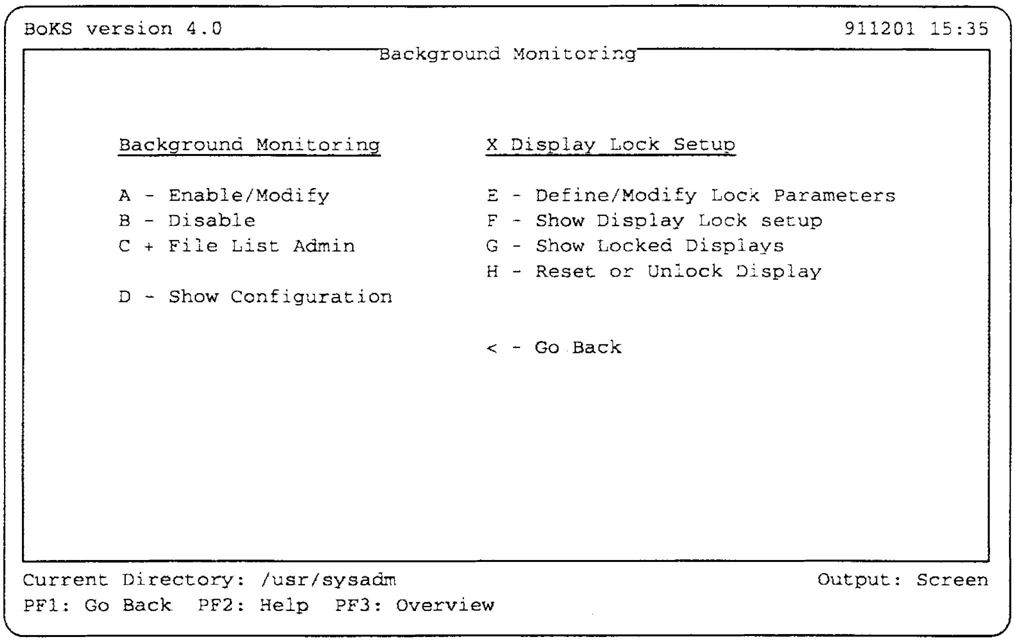
The following section explains how to use the menu choices on the *Background Monitoring* menu. There are two column headers on this menu:

1. *Background Monitoring*
2. *X Display Lock Setup*

   The menu choices under *X Display Lock Setup* are only applicable to those running BoKS in an X Windows-environment.

10.5.1 Running Background Monitoring

The *Background Monitoring* menu choices include the features listed below. To administer and run these monitoring features, use the following menu choices:



```
BoKS version 4.0                                                        911201 15:35
                                   Background Monitoring

       Background Monitoring          X Display Lock Setup

       A - Enable/Modify              E - Define/Modify Lock Parameters
       B - Disable                    F - Show Display Lock setup
       C + File List Admin            G - Show Locked Displays
                                      H - Reset or Unlock Display
       D - Show Configuration

                                      < - Go Back

Current Directory: /usr/sysadm                                        Output: Screen
PF1: Go Back  PF2: Help  PF3: Overview
```

Figure 10.1 Sub Menu, Background Monitoring

- *Enable/Modify*
- *Disable*
- *File List Admin*
- *Show Configuration*

Features of Background Monitoring

The following features comprise background monitoring:

NOTE

The results of the background monitoring features can be found in the system logs which are found under the Log Admin menu choice.

Inactivity Monitoring

After a pre-defined period of inactivity (see *Parameter Configuration* chapter for further details on timeout) users are automatically logged out of the system.

If users have logged in from an X-terminal or started an X-server on a workstation, the users' screens are locked after a period of inactivity and users must enter their password to restart the session.

File Monitoring

File monitoring checks for changes to the contents, permissions and deletion of files and directories listed in the file monitoring list. All occurrences of content changes are logged in the system log (see the *Log Administration* chapter for further information).

NOTE *In the network version of BoKS, files and directories on remote partitions must not be included in this list as it increases network traffic too much. All file monitoring for a specific host must be carried out on the local host.*

System Clock

The background monitoring daemons also monitor and log changes to the system clock. Any changes are logged in the system log (see *Log Administration* chapter for further information).

Enable/Modify

The *Enable/Modify* menu choice on the *Background Monitoring* menu enables you to start background monitoring and determine the parameter settings for the background monitoring processes. This menu choice is also used for altering these background monitoring parameters.

To enable background monitoring and alter the parameters, take the *Enable/Modify* menu choice and enter:

`Host`
: Name of the machine to which background monitoring applies.

`Inactivity Monitoring`
: Specifies if the inactivity check is enabled. Enter **on** to enable the process. Enter **off** to disable the process.

`Sleeptime in Seconds`
: Number of seconds between each inactivity check. The default is thirty seconds. It is not normally necessary to change this value.

`File Monitoring`
: Specifies if file monitoring is enabled.

`Interval Between Monitorings (Minutes)`
: Number of minutes between each file check. Default is 30 minutes.

`Process Priority (Nice)`
: Priority the file monitoring process has over other programs. This is called the nice value. A nice value of 39 is the minimal priority and no other activities on the system are effected by file monitoring. The highest value is 0 which means that file monitoring will have priority over most other programs. The default setting is 10.

NOTE *Note that the default values that are set when BoKS is supplied are used if no other values are set.*

The hostname must be entered if you are using the network version of BoKS, even if all the other values are left blank.

Executing this menu choice enables background monitoring. To alter the values in the future, use this menu choice.

Sample Entry Screen

A sample setting for this screen would be:

```
Host                                    bigbox
Inactivity Monitoring                   on
Sleeptime in Seconds                    40
File Monitoring                         on
Interval Between Monitorings (minutes)  60
Process Priority (nice)                 10
```

In the above example the sleeptime and interval between monitorings settings have been altered.

Disable

To disable background monitoring on a particular host, use the *Disable* menu choice on the *Background Monitoring* menu and enter:

`OK to Disable Background Monitoring? (Y/N)`

Enter `Y` to confirm the disabling of system monitoring.

`Host`

Name of the host where system monitoring is to be disabled. In the case of the standalone version of BoKS, the hostname is automatically entered.

Displaying the Background Monitoring Settings

You can display the configuration of the system monitoring function with the *Show Configuration* option on the *Background Monitoring* menu. If you are using the network version of BoKS you are required to enter the name of the host whose configuration you need to list.

NOTE *The results of background monitoring are displayed by various options on the "Log Admin" menu.*

Sample Output

```
System Monitoring:                  on

 - Inactivity Check:                on
   Sleep Time (seconds):            30

 - File Monitoring:                 on
   Process Priority (nice value):   10
   Start Interval (minutes):        20
```

File List Administration

Part of the functionality of the *Background Monitoring* menu in BoKS, is to check for alterations to files. The file monitoring occurs periodically and the results are sent to the system logs which can be queried using the *Log Admin* menu.

By default BoKS supplies a list of key files and directories. These are:

- */bin*
- */boks/bin*
- *$APPLPATH/bin*

To add or alter the list of files, use the *File List Admin* sub menu. Files and directories on remote partitions must not be included in this list as it would increase network traffic too much. All file monitoring for a specific host must be carried out on the local host. The *File List Admin* sub menu appears as shown in figure *10.2*.

Add File/Directory to List

To add a file to the list of files to be monitored, select the *Add File/Directory to List* option on the *File List Admin* menu and enter:

`Host`

Name of the host where the file resides. In the case of the standalone version of BoKS this is entered automatically.

`File/Directory`

Full path name of the file or directory that is to be added to the list.

Delete File/Directory

To delete a file or directory from the list, take the *Delete File/Directory* menu choice on the *File List Admin* menu and enter:

`Host`

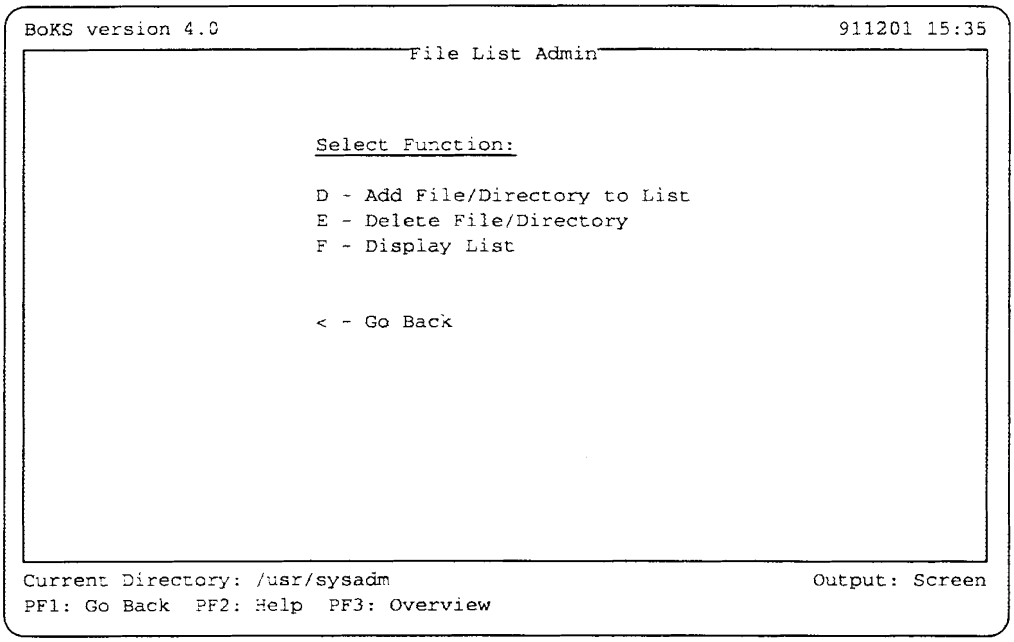
Name of the host where the file resides. In the standalone version of BoKS this is already entered.

`File/Directory`

Full path name of the file or directory that is to be deleted from the list.

Display List

The *Display List* option on the *File List Admin* menu, enables you to list the files that are to be monitored. In the case of the network version of BoKS,



```
BoKS version 4.0                                                911201 15:35
                             File List Admin

                         Select Function:

                         D - Add File/Directory to List
                         E - Delete File/Directory
                         F - Display List


                         < - Go Back

Current Directory: /usr/sysadm                                Output: Screen
PF1: Go Back  PF2: Help  PF3: Overview
```

Figure 10.2 Sub Menu, File List Admin

you have to enter the name of the host where the file is located.

Tracey decides that it is important that all changes to the personnel directory are monitored. For this to happen Tracey needs to add the personnel directory to the list of files to be monitored.

Tracey takes the *File List Admin* menu choice from the *Background Monitoring* menu. Once in the *File List Admin* sub menu she takes the *Add File/Directory to List* menu choice and enters:

```
Host              bigbox
File/Directory    /home/admin/personnel
```

The next time that the file monitoring process runs on `bigbox` it checks the `/home/admin/personnel` directory, noting the last time it was updated. An alarm is sent to the console if the directory is subsequently updated. Updating a directory in this context means a file being deleted from the directory, being moved from the directory or new files and directories being added to this directory. In addition any permission and ownership changes are noted.

Sample Output

The following is a sample of the output from the *Display List* command:

```
The Following Files/Directories Are Monitored
/bin
/usr/dynprods/BOKS
/boks
```

10.5.2 X-lock functionality

This section explains how to use the menu choices under the *X Display Lock Setup* header on the *Background Monitoring* menu. These menu choices are available for those who are using BoKS in an X-Windows environment. This feature replaces the automatic timeout feature available to those using BoKS on character terminals.

X-lock functionality contains the following features:

NOTE *The X-lock functionality is available for those who log in from an X-terminal or have started an X-Server from a workstation.*

Enables you to customise the way in which X-lock performs by tailoring the following:

- Length of the period of inactivity before the display is locked
- Number of attempts allowed to unlock the display
- Number of warnings before a display is locked

These features are already configured when BoKS is supplied. By taking the *Define/Modify Lock Parameters* menu choice, you can alter these pre-set values.

`Show Display Lock Setup`
: Enables you to report the X-setup and status.

`X-Lock Administration`
: Enables you to reset number of failed display access attempts and to unlock a display.

Define Lock Parameters

To define the X-lock parameters, select the *Define/Modify Lock Parameters* menu choice on the *Background Monitoring* menu and enter the following:

`Host`
: Name of the host to which the X-lock parameters apply. In the case of the standalone version of BoKS, the host name is already entered.

`Timeout Limit`
: The period of inactivity before the display is locked. The period is specified in minutes. The default is 15 minutes. Specifying 0 turns

the X-lock feature off.

NOTE *If the period specified is longer than the one specified in the "Enable/Modify" menu choice on the "Background Monitoring" menu then the shorter period is used instead.*

`Warn Time`
Period during which the user is warned that the display is about to be locked. Period is specified in seconds. The warning takes the form of an alarm bell. The default is 12 seconds.

`Beep Interval`
Number of seconds between alarm bell soundings. The default is 4 seconds.

`Fast Beep Period`
Period immediately before the display is locked when the alarm bell is sounded once every second to signify that display-lock is imminent. The default is 4 seconds.

`Volume`
Loudness of the alarm bell. This value is expressed as a percentage of the loudest volume that the alarm bell can be sounded at. This means that:

- `100` specifies that the alarm bell is sounded as loud as possible
- `50` specifies that the alarm bell is sounded half as loud as possible
- `0` specifies that the alarm bell is not sounded at all

The default is machine-dependent, but is normally approximately 70.

`Transparent Display`
Display contents on the screen when the display is locked.

`Log Display Locks`
Specifies whether locking a display is logged in the user log.

`Wait Time`
Period of time during which further attempts to unlock the display is refused. Period specified in minutes.

`Login Retries`
Number of failed unlocking attempts before a display is locked.

Modify Lock Parameters

To modify the parameters, use the *Define/Modify Lock Parameters* menu choice, select the *Define/Modify Lock Parameters* menu choice and enter the name of the host whose parameters you would like to alter. Go to the relevant fields, altering the values as required and execute the menu choice.

Reset or Unlock a Display

To both reset the number of failed attempts to unlock the display and to unlock a display, select the *Reset or Unlock Display* menu choice and enter:

`Display`
Name of the display to be unlocked or whose unlocking attempts are

to be reset.

`Action`

Specify **`unlock`** if the display is to be completely unlocked. Specify **`reset`** if the display is to have the number of unlocking attempts reset.

Show Display Lock Setup

To list the parameters that have been set using the *Define/Modify Lock Parameters* menu choice, select the *Show Display Lock Setup* menu choice. To use this menu choice, enter:

`Host`

Name of the host whose X-lock parameters are to be displayed. In the case of the standalone version of BoKS the name of the host is automatically entered.

Sample Output

The following is sample output from the menu choice *Show Display Lock Setup:*

```
Timeout in Minutes                              15
Seconds to warn before locking                User 12
Seconds between alarm bell warnings           User 4
When to start warning faster (seconds left)   User 4
Bell volume in percent                        User 70
Transparent mode                              User no
Log when display is timed out and locked      no
Maximum number of retries                     4
Minutes to reject input after too many tries  20
```

The values prefixed by *User* can be altered on a user by user basis. This is done by altering the values in the *Xuserenv* file in a user's home directory. (Please refer to the *Configuration* chapter for further details.)

Show Display Lock Setup Report Field Description

The following explains the fields listed in the *Show Display Lock Setup* menu choice:

`Timeout in Minutes`

The period of inactivity before the display is locked. The period is specified in minutes.

`Seconds to Warn before Locking`

Period during which the user is warned that the display is about to be locked. Period is specified in seconds.

`Seconds Between Alarm Bell Warnings`

Number of seconds between alarm bell soundings.

`When to Start Warning Faster (seconds left)`

Period immediately before the display is locked when the alarm bell is sounded once every second to signify that display-lock is imminent.

`Bell Volume (in percent)`

Loudness of the alarm bell. This value is expressed as a percentage of the loudest volume that the alarm bell can be sounded at.

`Transparent Display`
Display contents on the screen when the display is locked.

`Log When Display Times Out and Locks`
Specifies whether locking a display is logged in the user log.

`Maximum Number of Retries`
Number of failed unlocking attempts before a display is locked.

`Minutes to Reject Input After Too Many Tries`
Period that a display does not accept unlocking attempts after a certain number of failed unlocking attempts. Period is specified in minutes.

Show Locked Displays

This menu choice reports the displays that are currently locked. Select the menu choice and the following fields are displayed:

`Display`
Name of the X-displays that are locked.

`Name`
Name of the user using the display.

`PID` Identity number of the lock process.

`Host`
Name of the host that the display is connected to.

Sample Output

The following shows sample output from the *Show Locked Displays* report:

```
Display      Name      PID        Host
-------      ----      ---        ----
xterm:2      tracey    12345      bigbox
xterm:9      dougal    54321      bigbox
```

11

Integrity Check

11.1 Outline

This chapter explains how to use the integrity check features in BoKS. The integrity check functionality is closely related to the options on the *Reports* menu. This chapter explains how to:

- Setup and run integrity check features
- Display the integrity reports

11.2 Outlook

Integrity checking is an important feature of any security system. The integrity checker is a collection of programs which check the system for potential security problems. The results of the integrity check are put into several reports. The integrity check can be set to run automatically on a day to day basis.

The results of the monitoring are reported in a series of rigorous reports which are easy to use and interrogate.

11.3 Important Terms

In this chapter you encounter the following terms:

/etc/rc* Files

System startup files. These programs are executed when the system is booted.

CERT

CERT advisory notes are publically available data which determines whether a security bug is present in program. The information is available via anonymous *ftp*(1) from cert.sei.cmu.edu.

Cron File

File or series of files that contain a list of commands to be executed at regular intervals. The cron files are are maintained by the *cron* daemon. The files consist of a number of lines. Each line consists of a command and a specification of when the command is to be executed.

Device Files

Hardware control files. They are special files in the */dev* directory which are part of the UNIX kernel, enabling the operating system to access such hardware devices as tape drives, disks, terminals, printers, and so on.

Integrity Check

Monitoring of the vulnerability of a system.

Key Files

Files important to the security of the system.

Nice Value

This value represents the priority of a process. The priority can be lowered by incrementing the nice value. The higher the increment the lower the the priority. The range of incrementing varies from UNIX variant to UNIX variant. On BSD systems the increment range is between -20 and +19. On System V machines the range is between 0 and 40.

Setuid

Permissions which enable the executor of a utility to run the utility with the permissions of the owner of that utility.

The set user id permission bit is a flag that may be enabled for a program by the *chmod(1)* command. When this flag is enabled, the program takes on the permissions of the owner of the program upon execution. For example the *su*(1B) program is usually owned by `root` and has the setuid bit set. This means that when users execute the *su*(1B) program, they have the permissions of `root`.

Setgid

Permissions which enable the executor of a utility to run the utility with the permissions of the group belonging to that utility.

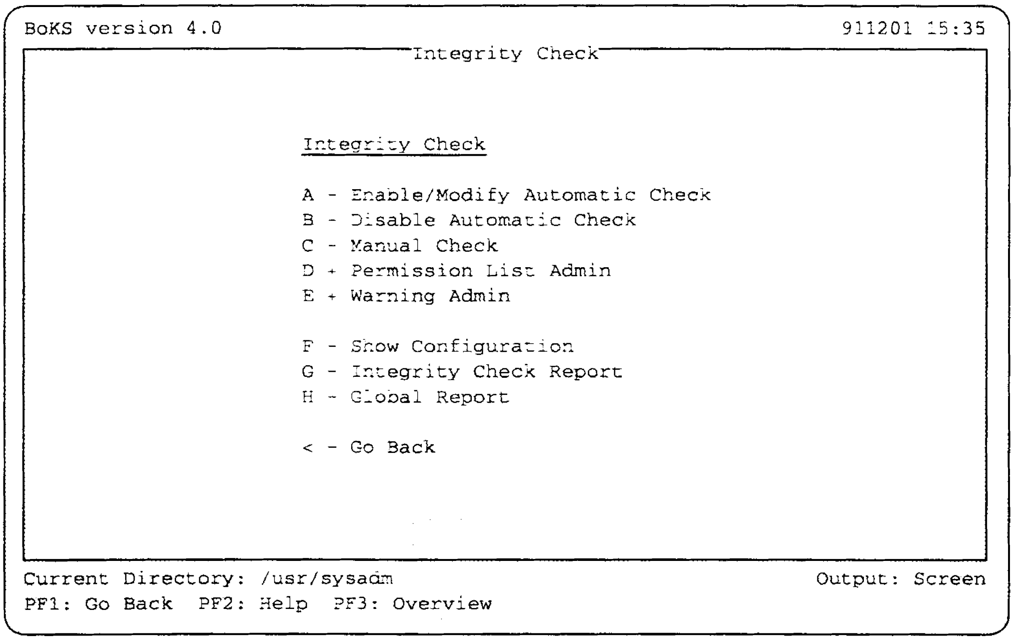
The set group id bit works like the set user id bit except that the executor assumes the permissions of the group ownership of the program instead of the user permissions.

World Writable

All users have permission to write to the file.

11.4 The Integrity Check Menu

The *Integrity Check* menu appears on the screen as shown in figure *11.1*.



```
BoKS version 4.0                                                 911201 15:35
┌──────────────────────────────Integrity Check──────────────────────────────┐
│                                                                           │
│                                                                           │
│                      Integrity Check                                      │
│                                                                           │
│                      A - Enable/Modify Automatic Check                    │
│                      B - Disable Automatic Check                          │
│                      C - Manual Check                                     │
│                      D + Permission List Admin                            │
│                      E + Warning Admin                                    │
│                                                                           │
│                      F - Show Configuration                               │
│                      G - Integrity Check Report                           │
│                      H - Global Report                                    │
│                                                                           │
│                      < - Go Back                                          │
│                                                                           │
│                                                                           │
└───────────────────────────────────────────────────────────────────────────┘
Current Directory: /usr/sysadm                                 Output: Screen
PF1: Go Back  PF2: Help  PF3: Overview
```

Figure 11.1 sub menu, Integrity Check

11.5 Functionality

The following section explains how to use the BoKS *Integrity Check* functionality.

The integrity checker checks the following:

- Contents of the system startup shell script files, for example */etc/rc**.
- Writability of devices and special files.
- Write/read ability of files listed in a permission list.
- Contents of the cron files for possible security problems.
- */etc/passwd*(4) and */etc/group*(4) files for inconsistencies.
- Setup for *ftp*(1), including anonymous *ftp*(1).
- User home directories to see if any are world writable.
- Key files in user home directories for world writability.
- Changes in setuid and setgid files.
- Programs for security bugs according to the CERT advisories.

The results from the integrity check are collected in an integrity report. The results take the form of warnings which are classified by severity level. The severity level is displayed at the beginning of each warning. The severity levels are as follows:

Level 0 A problem that, if exploited, can gain an intruder almost instant root access.

level 1 A serious security problem, for example: a poor password.

Level 2 Potential serious security problem, but the precise details are out of the scope of the integrity check.

11.5.1 How the Integrity Checker Works

The following section explains how the Integrity Check reports are produced. It explains the source of these reports and how they can be configured.

The system administrator has access to two integrity check reports:

- *Integrity Check*
- *Global*

The key report is the *Integrity Check* report in which all integrity check information can be displayed or where only the integrity check information that it is especially relevant is displayed. This is done by specifying if you wish to show excluded warnings. Excluded warnings are kept in a list generated through the *Warning Admin* menu choices.

The *Global* report is an summary of the results of the *Integrity Check* report.

The configuration reports that determine the shape of the integrity check reports that BoKSADM menu system enables you to interrogate are as follows:

- *Reference Report*
- *Full Integrity Check Report*
- *Difference Report*

Reference Report The *Reference Report* is created at install time. It contains a list of "acceptable" warnings which in other circumstances could cause a security problem but on this platform, in this system setup does not. An example of this type of warning is:

```
/bin/su is an SUID-program
```

A setuid program can be a security problem but UNIX needs some programs to have setuid permissions for them to work. In the case of */bin/su*(1B) it is written in such a way that its setuid permission poses no problem and therefore is not a warning that needs reporting.

Full Integrity Check Report

Each time the integrity check is run the *Full Integrity Check Report* is created. This report contains all the warnings which have been reported during the system integrity check and is the report that the *Integrity Check Report* is based on if excluded warnings are to be displayed.

Difference Report

The *Difference* report is a list of those warnings which are included in the *Full Integrity Check* report but are not in the *Reference* report. It is this report that the *Integrity Check Report* menu choice on the *Integrity Check* menu is based on if the excluded warnings are not requested.

Reclassifying Warnings

To alter an "acceptable" warning to one that is listed in the *Difference Report* use the *Warning Admin* sub menu, in the *System Monitoring* menu, in the BoKSADM menu system.

Similarly the above menu enables you to add to the list of "acceptable" warnings if the *Difference Report* regularly reports warnings that in the case of your system does not pose a threat.

11.5.2 Running the Integrity Check

This section explains how to use the following menu choices:

- *Enable/Modify Check*
- *Disable Automatic Check*
- *Manual Check*

These menu choices enable you to run and administer the integrity check facility.

Enable Integrity Check

To enable the integrity checker to be run automatically take the *Enable Integrity Check* menu choice from the *Integrity Check* menu and enter:

`Host`

Name of the host on which the integrity check is to run. The name of the host is already entered in the standalone version of BoKS.

`When to Run`

Time of day in hours and minutes (HHMM) when the integrity check is automatically run.

An entry is made in the host's cron file to enable the integrity check to run automatically.

Use this menu choice to alter the values that have been set.

Disable Automatic Check

To stop the integrity check running automatically, take the *Disable Automatic Check* menu choice from the *Integrity Check* menu and enter:

`Host`

Name of host whose integrity check is to be stopped from running automatically. In the standalone version of BoKS you are not prompted for this field. The integrity check is automatically disabled by selecting the menu choice.

This removes the integrity check entry in the host's cron file.

Manual Check

If you wish to run the integrity check on a one-off basis use the *Manual Check* menu choice from the *Integrity Check* menu and enter:

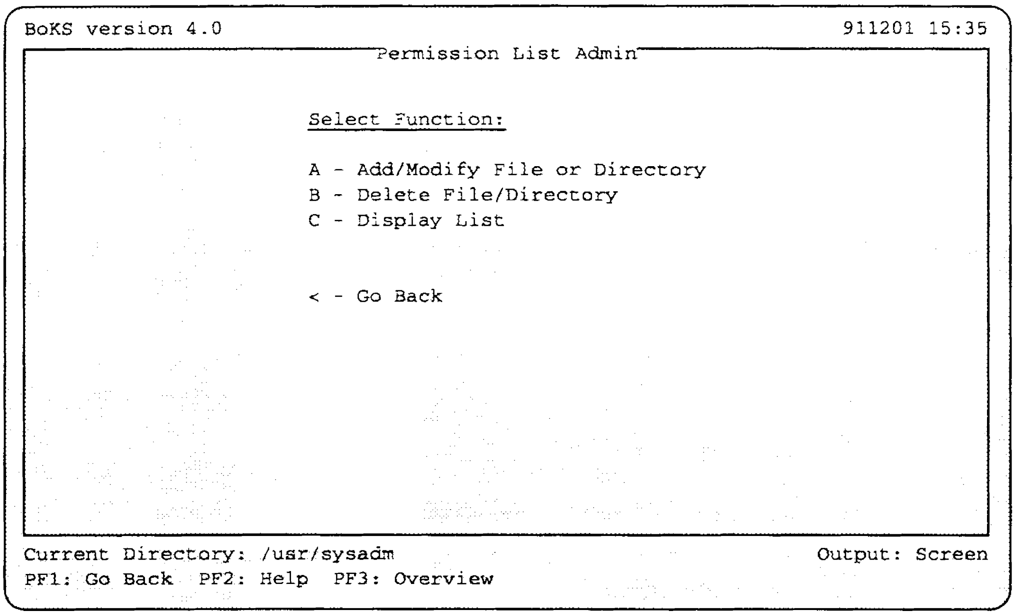
`Host`

Name of the host where you want to run the integrity checker. In the standalone version of BoKS you are not prompted for the hostname. The integrity checker starts automatically by selecting the *Manual Check* option.

It typically takes approximately 15 minutes for a full integrity check to be completed.

11.5.3 Configuring the Permissions List

The menu choices held in the sub menu *Permissions Lists Admin* enable you to alter the list of files/directories and the permissions that are to be checked. The *Permissions Lists Admin* appears on the screen as shown in figure *11.2*.



```
BoKS version 4.0                                                  911201 15:35
                         Permission List Admin

                        Select Function:

                        A - Add/Modify File or Directory
                        B - Delete File/Directory
                        C - Display List


                        < - Go Back

Current Directory: /usr/sysadm                                   Output: Screen
PF1: Go Back  PF2: Help  PF3: Overview
```

Figure 11.2 Sub Menu, Permission List Admin

Add/Modify File or Directory

The *Add/Modify File or Directory* menu choice on the *Permissions List Admin* menu enables you to add a file to the list and specify what type of permissions are to be checked. This means that you can configure the range of files that the integrity check covers to meet the needs of your site.

Take the *Add/Modify File or Directory* menu choice and enter:

`Path`

Full path name for the file or directory to be added to the list. This entry can contain wild cards ("*" and "?"). For example **/usr/lib/*** .

`Check Access For`
: Test for alterations to permissions for group members or world members. Enter **g** for group or **w** for world.

`Warn On`
: Specify whether you are looking for alterations to read permissions or write permissions. Enter **w** for write, **r** for read or **b** for both.

Modify File or Directory

If you wish to modify a definition use the *Add/Modify File or Directory* menu choice from the *Permission List Admin* menu and modify the definition.

Delete File/Directory

To delete a file or directory from the list use the *Delete File/Directory* menu choice from the *Permission List Admin* and enter:

`Path`
: The full pathname of the file or directory to be deleted from the list of those checked by the integrity checker.

Listing the Files to be Checked

To display your list of files use the *Display List* option on the *Permission List Admin* menu. This list has the following headings:

`Path`
: Full pathname of the file or directory.

`W/G` Specifies if the group or world permissions are to be tested for.

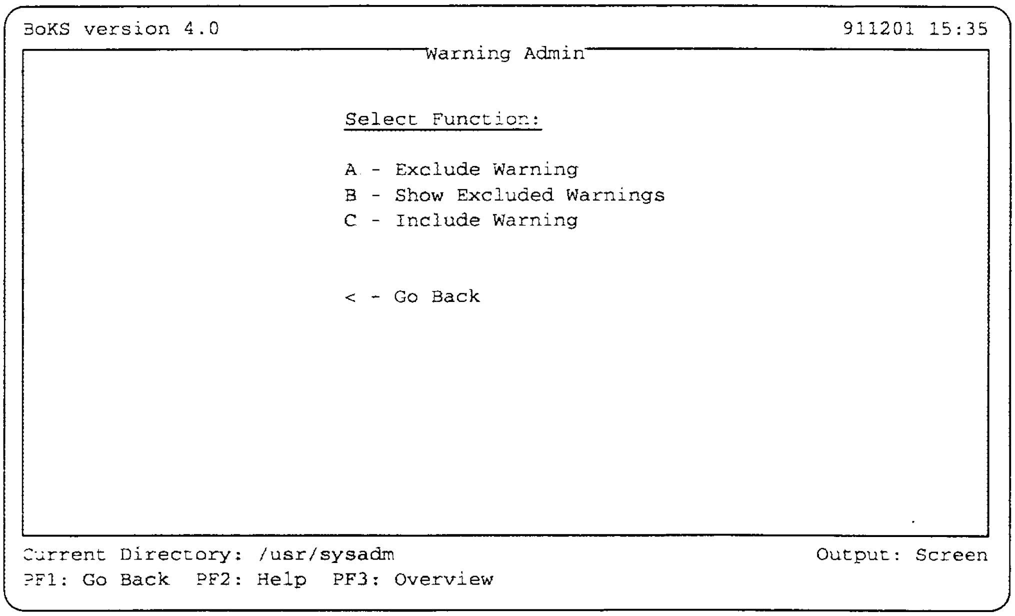
`R/W/B`
: Specifies whether read, write or both permissions are to be checked.

Sample output from this report is as follows:

```
Path                          W/G          R/W/B
--------------------------------------------------------
/                              w            w
/.*                            w            w
/bin                           w            w
/dev/kmem                      w            b
```

11.5.4 Warning Administration

To select which warnings are included in the reference report use the *Warning Admin* sub menu. By including the warnings in the reference report these warnings are excluded from the integrity check reports. The sub menu appears on the screen as shown in figure *11.3.*



```
BoKS version 4.0                                          911201 15:35
                          Warning Admin

                        Select Function:

                        A - Exclude Warning
                        B - Show Excluded Warnings
                        C - Include Warning


                        < - Go Back








Current Directory: /usr/sysadm                            Output: Screen
PF1: Go Back  PF2: Help  PF3: Overview
```

Figure 11.3 Sub Menu, Warning Administration

Exclude Warning

Excluding superfluous warnings helps you to concentrate on the current security issues that effect your system. To exclude warnings use the *Exclude Warning* menu choice on the *Warning Admin* menu and enter:

`Host`
: Name of the host on which to exclude the warnings. In the standalone version of BoKS this field is already filled out.

`Selected warnings`
: Warning numbers to be excluded. Use the multi-pick method to select multiple menu choices.

NOTE *The Exclude Warning menu choice removes the selected warnings from the current integrity report and places them in the Reference Report (see the section entitled "How the Integrity Checker Works" for further details). This means that the current report on the "Integrity Check" menu reflect the changes that have just been made. The changes in warnings also effect all future reports.*

Show Excluded Warnings

To list the excluded warnings select the *Show Excluded Warnings* option from the *Warning Admin* menu and enter:

`Host`
: Name of the host whose excluded warnings you want to see. In standalone version of BoKS you are not prompted for the host name and the list is displayed on selecting the *Show Excluded Warnings* option.

NOTE *The current version of integrity check does not detect the existence of dormant warnings in the reference report. A dormant warning is a warning that is no longer produced during the integrity check and can therefore not be excluded.*

The headings in this list are:

`Level`
The severity level of the warning.

`Warning`
Warning message that has been excluded.

Sample Output

Sample output from this report is as follows:

```
Excluded Warnings for Host: bigbox
Level      Warning
---------- ----------------------------------------------
0)         105 /usr/ucb/rdist could have a hole/bug (CA-91:20)
1)         60 User alice's home directory /usr/alice is mode 0777
2)         11 /dev/fd0 is group readable
2)         82 Need user (null) for anonymous ftp to work
```

Include Warning

The *Include Warnings* option on the *Warning Admin* menu removes the selected warning(s) from the reference report for the host and inserts them in the (current) integrity report. Therefore this has an immediate effect on reports produced for that host. As the included warnings may include an old dormant warning, integrity report should be considered invalid until the new one is run.

To include previously excluded warnings select the *Include Warning* option and enter:

`Host`
Name of the host to which the warning applies. In the standalone version of BoKS this field is already filled in.

`Select warnings`
Warning number to be included. Use the multi-pick method to select multiple warnings.

11.5.5 Integrity Check Reports

The results of the integrity checks are reported in the following menu choices:

- *Show Configuration*
- *System Integrity Report*
- *Global Report*

These menu choices are located on the *Integrity Check* menu. Using these menu choices enables you to evaluate the integrity of your system.

Show Configuration

To list the integrity check configuration on each host in the BoKS domain select the *Show Configuration* option from the *Integrity Check* menu. This report has the following headings:

`Host`
: Name of the host with the integrity check settings.

`On/Off`
: Specifies whether the integrity check is enabled or disabled.

`At Time`
: Time at which the integrity check runs on each host.

`Last Report Date`
: Date and time of the last report or the report that is running now. If the report is running the message `Running Now` is displayed.

Sample Output

Sample output appears on the screen as follows:

```
Host            On/Off At Time  Last Report

bigbox          on     0100     92.08.20:01.07
littlebox       on     0107     92.08.20:01.15
```

System Integrity Report

To display the results of the last integrity check select the *System Integrity Report* option and enter:

`Host`
: Name of the host whose warnings are to be displayed. In the standalone version of BoKS this field is already filled out.

`Exclude Warnings (Y/N)?`
: Specify if the excluded warnings are to be displayed. Enter **N** to include excluded warnings.

Sample Output

Sample output appears on the screen as follows:

```
Warning for Host: bigbox Report created: 92.08.20:01.07
-------------------------------------------------------
0)       /bin/login could have a hole/bug (CA-89:01)
0)       /bin/mail could have a hole/bug (CA-91:01a)
2)       /bin/fd0 is group readable
```

NOTE *Please refer to the "Troubleshooting" chapter for an explanation of the most common integrity checker warnings.*

Global Report

To summarise the results of the last *Integrity Check* report select the *Global Report* option from the *Integrity Check* menu. This report breaks down the *Integrity Check* report in the following way:

`Host Name`
: Name of the host to which the summaries apply.

`Number of level 0 warnings`
: Number of warnings of a severity level 0 nature. (Most serious)

`Number of level 1 warnings`
: Number of warnings of a severity level 1 nature.

`Number of level 2 warnings`
: Number of warnings of a severity level 2 nature. (Least Serious)

Sample Output

Sample output from this report appears as follows:

```
Summary of Number of Warnings per Host,
including Warning Level. Level 0 is very serious!
                Level
Host            0    1   2
-----------------    -   -
bigbox:         14   183 19
littlebox:      6    45  15
```

This page is intentionally left blank.

12

Host Administration

12.1 Outline

This chapter explains how you can administer the hosts in the BoKS domain through the BoKSADM menu. It explains how to do the following:

- Add and remove hosts from the BoKS database
- Group hosts together into host groups
- Delete users attached to a host

12.2 Outlook

DynaSoft regards a network as one or more machines which are either logically and/or physically linked in some way. The menu choices under the *Host Admin* column header apply to both the standalone and network versions of BoKS, whereas the menu choices under *Host Group Administration'* networks containing more than one machine.

If you are running the standalone version of BoKS the *Host Admin* menu enables you administer the one standalone machine. In the network version of BoKS it enables you to administer all machines in the network, this includes UNIX hosts in the network not running BoKS, PC hosts running PC Guard as well as UNIX BoKS hosts.

Networks are often regarded as difficult to administer and difficult to secure. BoKS provides a centralised approach to network security by controlling all the computers in the BoKS domain from the BoKS master-server. All access to the system, whether remote or local is controlled through access routes.

By administering all computers in the network centrally the security is greatly increased and administration problems reduced.

12.3 Important Terms

In this chapter you encounter the following terms:

BoKS Domain

Machines that are administered and have their access controlled by the same BoKS database.

BoKS Servers

Machines in the BoKS domain that have a copy of the BoKS database.

Client

Computer in a network which is controlled by a BoKS database on the master-server and contains no local BoKS database itself.

Host

Computer, whose access to which is controlled by BoKS.

Host Group

Collection of hosts which are treated as a single entity by the BoKS database for user administration and access route administration purposes.

Master-Server

Computer in a network that holds a read-write copy of the BoKS database. It is used to validate system access and to administer the other computers in the network. Only one master-server can exist in each BoKS domain.

Slave-Server

Computer in a network that holds a read-only copy of the BoKS database. It is used to validate system access and can step in and maintains access to the machines in the BoKS domain if the master-server should go down. Any number of slave-servers may exist in the BoKS domain.

Wild Cards

Symbols which can be substituted for characters by the operating system. The two wild cards are "*" and "?." The "*" is a substitute for all characters and blank spaces. For example:

```
*soto*
```

means a string with zero or more characters before *soto* and zero or more characters after *soto*. The "?" is a substitute for characters on a one-to-one basis. For example:

```
soto?????
```

means that the characters *soto* must be followed by five characters for a substitution to be made.

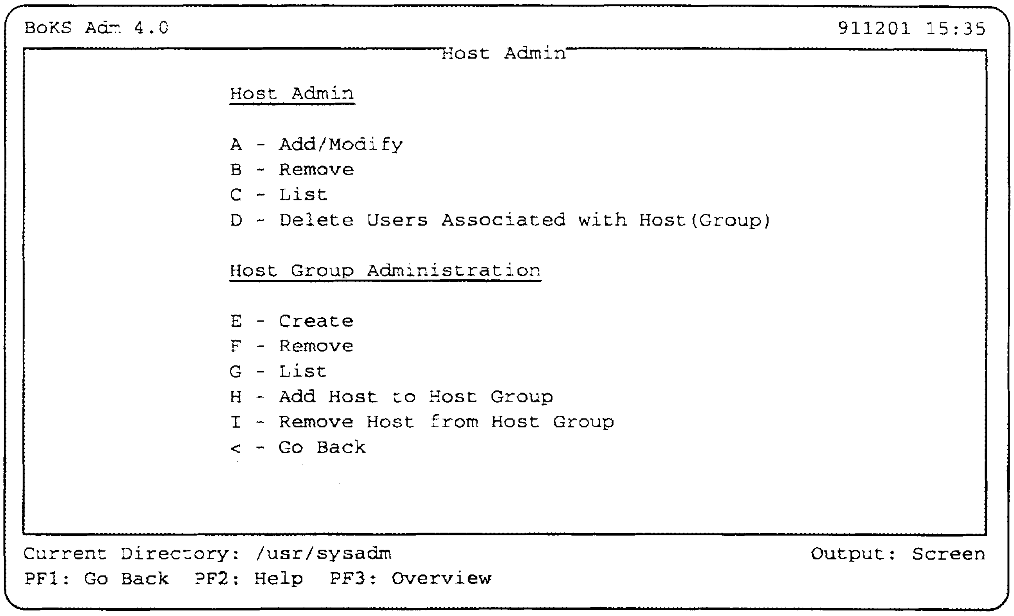
YP/NIS

YP/NIS is a distributed database which enables multiple machines to share the password and group files. In this way user administration can be centralised.

NOTE *For further details on how BoKS works with the YP/NIS database please refer to the "Configuration" chapter.*

12.4 The Host Admin Menu

The *Host Admin* menu in BoKS appears on the screen as displayed in figure *12.1.*



```
BoKS Adm 4.0                                                          911201 15:35
                                   Host Admin
                Host Admin

                A - Add/Modify
                B - Remove
                C - List
                D - Delete Users Associated with Host(Group)

                Host Group Administration

                E - Create
                F - Remove
                G - List
                H - Add Host to Host Group
                I - Remove Host from Host Group
                < - Go Back

Current Directory: /usr/sysadm                                     Output: Screen
PF1: Go Back  PF2: Help  PF3: Overview
```

Figure 12.1 Sub menu, Host Admin

12.5 Functionality

The following section explains how to administer the host facilities within BoKS. Using these features correctly makes administering the network considerably easier thereby increasing system security.

12.5.1 Adding and Removing Hosts

Before a host can be administered through BoKS it must first be added to the database whether you are using the standalone or network version of BoKS. It is essential that the host is added to the BoKS database otherwise BoKS is not able to administer it.

BoKS only accepts hosts that are listed in the */etc/hosts*(4) file on the master-server or those hosts that have been added to the YP map if YP/NIS has been installed. Once the host has been added to the database access to it is controlled centrally from any server, either master-server or slave-server.

Add/Modify

A host can not be administered through BoKS until it has been added to the BoKS database. The *Add/Modify* option on the *Host Admin* menu you can add and modify hosts in the BoKS database. The hosts must be registered either in the */etc/host*(4) file or in YP/NIS. The hosts can be one of three types:

- NONBOKSHOST
  Host not running BoKS software but is never the less in the network.
- UNIXBOKSHOST
  Host running UNIX and BoKS software.
- PCBOKSHOST Host running DOS and BoKS software.

To add hosts to the BoKS database take the *Add/Modify* option and enter:

`Host`
: Name of the host that is to be added to the BoKS database. The host must be either listed in the */etc/host*(4) file or in the NIS database.

`Type of Host`
: Specify the relationship of the host with BoKS as follows:

  - **NONBOKSHOST** for a host outside the BoKS domain
  - **UNIXBOKSHOST** if the machine is running UNIX and is a member of the BoKS domain
  - **PCBOKSHOST** if the machine is running DOS and is a member of the BoKS domain

`Parent Homedir`
: Name of the directory under which user home directories are created on the host machine. This is the name of the directory as the user sees it. If the directory is symbolically linked to another directory the original/real directory is specified in the next field. If a user is set up with a relative home directory, the parent home directory is used as the path to the user's home directory. For example if user set up as `tracey` the full path of this user's home directory is *parenthomedir/tracey* where *parenthomedir* might be */home* for example.

`Physical Homedir`

NOTE *If using the standalone version of BoKS this directory is on the standalone machine too.*

Original name of the parent home directory if the home directory specified in the *parent homedir* field is in some way symbolically linked to another directory. For example in the case of NFS (Network File System) mounted home directories. The physical home directory setting specifies the name of the directory entered in the field `Parent Homedir` as the system knows it. Use the format *hostmachine* : *directory*, where the directory must be specified with the full pathname.

The following are two examples of how this screen might be filled in:

```
Host               littlebox
Type of Host       UNIXBOKSHOST
Parent Homedir     /usr/people
Physical Homedir
```

This example specifies that the host to be added is called `littlebox` and the directory under which the home directories are located is */usr/people.* The `Physical Homedir` field is blank signifying that */usr/people* is not linked to another directory.

```
Host             littlebox
Type of Host     UNIXBOKSHOST
Parent Homedir   /usr/people
Physical Homedir colourbox:/shared/usr/people
```

The second example specifies the host to be added as `littlebox` and the directory under which the home directories are located as */usr/people.* This time the *Physical Homedir* is specified as *colourbox:/shared/usr/people.* This means that */usr/people* has been mounted from the machine colourbox using the directory */shared/usr/people.*

NOTE *To check whether or not you need to specify a physical home directory you should check for network mounted file systems. This means that you are checking to see if any file systems on your host are residing on another computer. One way to do this is to use /etc/mount(1) which lists the location of mounted file systems.*

The format for the physical home directory is machine:directory path.

NOTE *The computer that you are mounting the directory from must also be part of the network controlled by BoKS and must have been added as a host to the BoKS database. The menu choice "List" under the "Host Admin" header lists all hosts known to the BoKS database.*

Remove

To remove hosts from the BoKS database select the *Remove* option under the *Host Admin* header on the *Host Admin* menu. Once this menu choice has been used for a particular host BoKS users are not able to access it through the BoKS *login*(1B) program.

Select the *Remove* option and enter:

`Host`

Name of the host to be removed from the database.

NOTE *Do not remove machines that are required by users. If this does occur users are blocked from logging in on that machine. You can check which computers are likely to be needed with the "Login/Logout" menu choice under the Reports menu. Even if the computer is not listed, this does not necessarily mean that is not required.*

12.5.2 Grouping Hosts Together

Hosts can be grouped together into *host-groups.* Users who are to have access to more than one machine in the BoKS domain must have the following attributes:

- Same group ID on each machine
- Same user ID on each machine

If grouped together correctly, user and access route administration in a network is simplified considerably. Host groups should consist of computers which are used for similar purposes in terms of the workplace they are used in. It is common, for example, to group machines according to people's roles in a company. In this way the system setup on all the machines in the group is compatible. In this way user ID conflicts and group ID conflicts are avoided.

Create

BoKS users are able to access more than one host by being assigned to a host group. A host-group is a group of hosts referred to by a particular name. The hosts must already have been added to the BoKS database before they can be grouped using the *Create* option under the *Host Group Admin* header on the *Host Admin* menu.

To create a host group select the option *Create* under *Host Group Admin* and enter:

`Host Group`

Name of the host group. By convention all host group names are written in upper case. This is not enforced but is recommended so that the host groups can be easily distinguished from individual hosts.

The group ALL already exists and should not be deleted. This group is synonymous with the wild card "*" and all hosts registered in the BoKS database are automatically included in this group. The advantage of having a group to which all hosts belong is that users can be quickly and simply set up to have access to all hosts on the system.

`Members`

Names of the hosts to be included in the new group. Wild cards may be used. The list of members is entered in the format of the names of the hosts, separated by a space.

Tracey has five computers on the network on which she has installed the network version of BoKS. The machines play the following roles:

- *bigbox - main machine containing almost all employees home directories*
- *littlebox - marketing machine containing the customer database and marketing literature*
- *colourbox - sales machine containing the leads database and sales literature*
- *blackbox - research and development machine used by the designers running a graphics package*
- *moneybox - personnel and financial records machine*

Tracey needs to group these boxes together to simplify network administration.

Tracey decides that the sales and marketing departments will need access to both `bigbox`, `littlebox` and `colourbox` as these departments' home directories are on bigbox, the customer database is on `littlebox` and the leads database is on `colourbox`. Tracey checks that the system setups are compatible and that there are no user ID conflicts with the same user having different identity numbers on each machine. This is the case for three of the users. Tracey edits the */etc/passwd*(4) file so that the conflict is removed. She alters the permissions on their files and home directories so that the ownerships are correct for the new user IDs.

Tracey takes the *Create* menu choice under the *Host Admin* menu and enters:

```
Host Group  SALES
Member      bigbox colourbox littlebox
```

Tracey decides to group `blackbox` and `bigbox` together for the Research and Development department, checking for any user ID conflicts and system setup compatibility. She takes the *Create* option again and creates the hostgroup RD.

Finally Tracey decides to group `moneybox` and `bigbox` together for the personnel and finance departments, checking for any user ID conflicts and system setup compatibility. She takes the *Create* option again and creates the hostgroup ADMIN.

Remove Host Group

To remove a host group select the *Remove* option under the *Host Group Admin* column on the *Host Admin* menu. This results in users who are coupled with this host group being unable to access the system. These users have to be re-created in the BoKS database and coupled to another host or host group.

WARNING **Removing a host-group incurs the same risk as removing a single host. Check that the host group is not in need before removing it otherwise users attached to that group are blocked from logging in as BoKS does not have control over access to that machine.**

Select the *Remove* option and enter:

`Host Group`
Name of the host group to be removed.

Add Host to Host Group

New hosts may subsequently be added to a host group using the *Add Host to Host Group* menu choice on the *Host Admin* menu.

Select the *Add Host to Host Group* option and enter:

`Host Group`
Name of the host group you want to add a new host to.

`Host`
Name of the host or hosts you want to add. A list of new members is entered in the format `hostname hostname hostname`.

Remove Host from Host Group

To remove a host from a host group use the *Remove Host from Host Group* menu choice under the *Host Group Admin* column on the *Host Admin* menu. Removing the host only removes the host entry in the database and not the users. If the users have been created as *hostname : user* instead of `host(group)name : user`, these users will not be able to access the system. The users are not automatically transferred to another machine but at the same time the home directories are not destroyed and their entry in the BoKS database is not removed either. The users have to be manually recreated on other machines.

Users attached to hostgroups are still be able to login onto the network provided that the other machines in the group are controlled by BoKS.

Select the *Remove Host from Host Group* option and enter:

`Host Group`
Name of the host group you want to remove a host from.

`Host`
Name of the host or hosts to be removed. The hosts which are members of this group and which are to be removed are entered separated by spaces.

Delete User Associated with Host(Group)

To delete users which are located in a host or host group take the *Delete Users Associated with Host(Group)* on the *Host Admin* menu. The users are deleted from the BoKS database but the entry in the local password file on the host is not removed.

Select the *Delete User Associated with Host(Group)* under the *Host Admin* column and enter:

`Host(Group)`
Name of the host or host group whose users you would like to delete. Once this option has been taken the users are deleted from the BoKS

database.

12.5.3 Listing Hosts and Host Groups

There are two report menu choices on the *Host Admin* menu:

1. *List* under the *Host Admin* column
2. *List* under the *Host Group Administration* column

List Under Host Admin

To list the hosts that have been added to the BoKS database take the *List* option under *Host Admin.* This menu choice lists:

`Host Name`
: Name of the host added.

`Address`
: Network address of the host added.

`Type of Host`
: Status of the host. Specifies if the host is controlled by BoKS, running UNIX or DOS.

`Parent Homedir`
: Name of the directory under which home directories are created if the home directory specified is a relative one.

`Physical Homedir`
: Name of the directory that the parent homedir is linked to.

`Comment`
: Comments about the host.

`Update the passwd File`
: Specifies if the password file is updated when changes are made to the BoKS database.

Sample Output

Sample output is as follows:

```
-----------------------List---------------------
Host :                     bigbox
IP-address:                123.987.001.876
Host Type:                 UNIXBOKSHOST
Parent Home Directory:     /usr/home
Physical Home Directory:   colourbox:/usr/home
Comment:
Update passwd-file:        Yes
```

List Under Host Group Administration

To list members of host groups take the menu choice *List* under *Host Group Administration.* This menu choice lists:

`Host Group`
: Name of the host group.

`Members`
List of machines in the host group.

Sample Output

Sample output is as follows:

```
Host Group   Members
ALL          *
SALES        littlebox colourbox
```

13

Password Generator Administration

13.1 Outline

This chapter explains how to use the *Password Generators* menu which resides in the *Password Admin* menu under the *S220 - One Time Passwords* column. This chapter is only appropriate for those who have purchased the password generator add-on module. This chapter explains how to:

- Setup a password generator entry in the BoKS database
- Remove a password generator entry in the BoKS database
- Access the system using a password generator
- Synchronise a password generator with the BoKS database
- Use the password generator in a network
- Maintain the password generator

13.2 Outlook

The BoKS Password Generator looks like and can be used as (if in the correct setting) a pocket calculator. The password generator identifies the user by generating a pseudo-random number as the password, which is then used in place of a normal password during the *login* process. The random number is practically impossible to guess and can only be used once. The advantage of the password generator is that even if a cracker were to see a user's password it is of little use as the password is only valid for one access session.

13.3 Important Terms

In this chapter you encounter the following terms:

Forced One-time Password

An authentication method which permits access to a particular access method only if the user is a one-time password user.

ID

Unique identity number which is given to the generator on initialisation.

IPIN

Random value which is used when the generator is initialised.

Mode

In the context of this chapter this means the function setting of the generator. The modes can be set by pressing the buttons on the left hand side of the generator. The function settings are as follows: PIN, MAC, TAN, ID.

PIN

Personal identity number - five figure code which is used when users identify themselves to the password generator. The code has to be entered into the generator before the one-time password is generated.

SPIN

Session PIN (number code) which is applicable only for one session. It is the randomly generated one-time password which has been generated for a specific system access session.

Setting/Set to

In the context of this chapter this is the setting of the black switch in the bottom right hand corner of the generator. The switch can be set to SAFE, CALC or BATT.

Synchronisation

Bring the generator and the database to the the same iteration of the one-time password.

XPIN

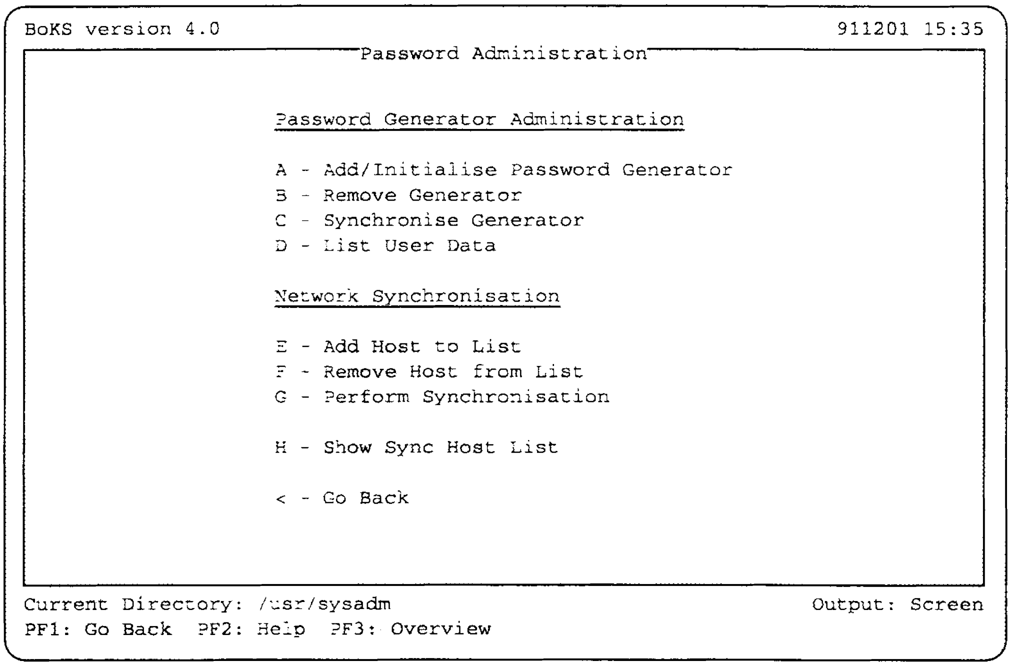
Exchange pin number only used when changing a generator's PIN code. This code works as a synchroniser between the BoKS database and the password generator when the PIN code is changed.

13.4 Password Generators Menu

The *Password Generators* menu appears on the screen as shown in figure *13.1.*

13.5 Functionality

The following section explains both the functionality from the *Password Generators* menu and how to use and maintain the password generator itself.



```
BoKS version 4.0                                              911201 15:35
                     Password Administration

                  Password Generator Administration

                  A - Add/Initialise Password Generator
                  B - Remove Generator
                  C - Synchronise Generator
                  D - List User Data

                  Network Synchronisation

                  E - Add Host to List
                  F - Remove Host from List
                  G - Perform Synchronisation

                  H - Show Sync Host List

                  < - Go Back

Current Directory: /usr/sysadm                               Output: Screen
PF1: Go Back  PF2: Help  PF3: Overview
```

Figure 13.1 Sub Menu, Password Generators

13.5.1 Adding and Removing Password Generators

Before a user can log in using a password generator the user has to be first registered in the BoKS database as a password generator user with a unique identity number. The password generator has to also be initialised so that it can be used by the BoKS database.

Add/Initialise Password Generator

The *Add/Initialise Password Generator* menu choice on the *Password Generators* menu has two functions:

1. Register users as password generator users
2. Register a password generator

NOTE *The password generator must be intialised directly after using the "Add/Initialise Password Generator" menu choice.*

To create a user as a password generator user, take the *Add/Initialise Password Generator* option and enter:

`User`
: Hostname coupled with the user name of the user in the format *host(group)name : username.*

`Generator ID`
: Unique number that BoKS generates. To accept the number, press

`Return`

WARNING **If you alter the number BoKS displays the new id number must not be an existing generator id number. It must not contain leading zeros, for example 000456 as the leading zeros are stripped. Maximum length is 10 figures.**

`IPIN for Generator`
Random number (maximum of 10 figures) which BoKS generates. To accept the number, press `Return` Leave out leading zeros.

`Your PIN-code`
Unique five figure pin number which is the user's identification code which is used to identify the user to the password generator.

WARNING **As this PIN code is the user's password generator signature it must be unique, just as a user's standard password should be unique, so as to not compromise system security.**

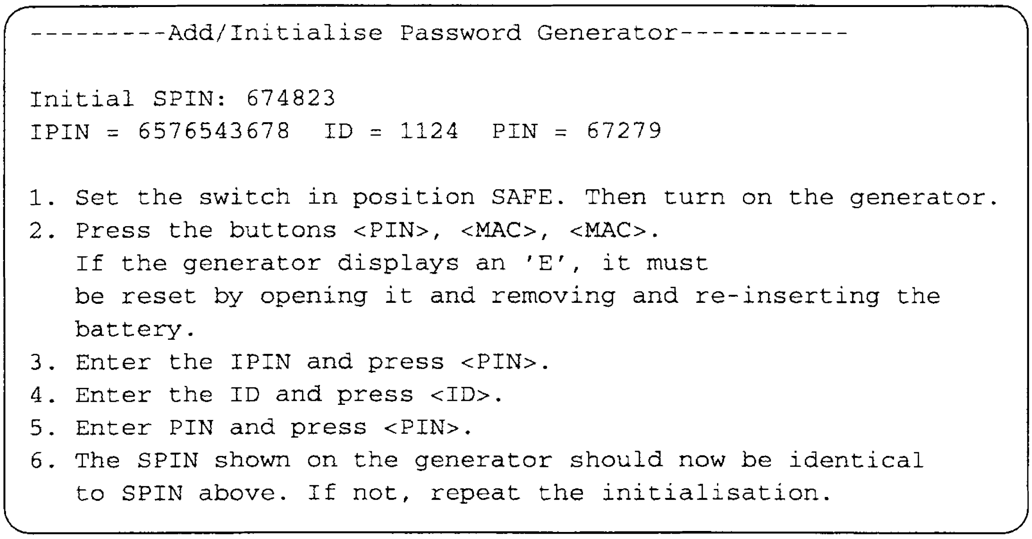
`Forced one-time password`
Specify if the user must always use the password generator, regardless of which access route is used or the authentication method applied. Specify **yes** to enforce the use of a password generator.

Executing this menu choice displays the first SPIN value, followed by the value that is to be entered into the generator. You must now initialise the generator, following the steps outlined below.

WARNING **The generator must be initialised before it can be used.**

Initialise the Generator

The screen lists the values you have just entered in the following way:



```
---------Add/Initialise Password Generator-----------

Initial SPIN: 674823
IPIN = 6576543678  ID = 1124  PIN = 67279

1. Set the switch in position SAFE. Then turn on the generator.
2. Press the buttons <PIN>, <MAC>, <MAC>.
   If the generator displays an 'E', it must
   be reset by opening it and removing and re-inserting the
   battery.
3. Enter the IPIN and press <PIN>.
4. Enter the ID and press <ID>.
5. Enter PIN and press <PIN>.
6. The SPIN shown on the generator should now be identical
   to SPIN above. If not, repeat the initialisation.
```

Thus to initialise the password generator, carry out the following:

1. Check that the generator is switched to SAFE.
2. Check that the generator is in PIN mode. This is confirmed by the presence of a "?" in the top left-hand corner of the generator.

   If the generator displays a zero, press `PIN` to switch it into PIN mode.
3. Press MAC twice.

WARNING **If the generator displays an E the generator was already initialised. In which case the generator must be reset (see the section *Reset the Generator*) as it has become uninitialised.**

4. Enter the same IPIN number which you have just entered into the screen and press `PIN`
5. Enter the generator ID that was entered into the screen, into the generator and press `ID`
6. Enter in the **PIN** code and press the `PIN` button
7. The same SPIN value is displayed on the generator as is displayed on the screen.

WARNING **If the two SPINs do not agree, the generator must be re-initialised by repeating this procedure.**

Removing a Generator User/Password Generator

To set a user back to being a ordinary password user, select *Remove Generator* option on the *Password Generators* menu. This removes the user as a password generator user and removes the entry for the generator. The user now uses a regular password. Select the *Remove*

Generator menu choice and enter:

`User`

Name of host coupled with the username of the user that is to cease using the password generator. Enter the username in the format *host(group)name : username.*

Listing Password Generator Users

To list all the users who are set up to use the password generator use the *List User-Data* option on the *Password Generators* menu. This option lists the users in the BoKS database and specifies which have access to a password generator and their one time password identities. Those who do not have password generator access are allocated a series of dots in the ID column.

Sample Output

A sample list is as follows:

```
User            ID
-----------     --
bigbox:tracey   12345
bigbox:dougal   678967
RD:buzz         .........
```

13.5.2 Logging in Using the Password Generator

To log in using the password generator take the following steps:

1. Switch the generator to on by pressing `ON`
2. Make sure the generator is set to SAFE.
3. Make sure that the generator is in PIN mode. This is confirmed by the presence of a "?" in the top left-hand corner of the generator.
4. Generate the one-time password by entering your five figure PIN number and then pressing `PIN` The resulting number that is displayed on the password generator is termed the SPIN.
5. Enter the SPIN number at the password prompt when logging in. For example:

```
login:             Tracey
password (SPIN):   456287
```

13.5.3 Adding New Access Route Authentication Methods

When you add the password generator module to the standard BoKS configuration two authentication methods are added which define the mode of security added to each access route. (See the *User Authentication* chapter for more information) These extra authentication methods are:

36 `One-time password (if a password generator user)`

Enables you to force the user to use the password generator when employing a particular access route, provided that the user is a password generator user, if not the user uses a normal password.

100 `One-time Password (always)`

Enables you to force the access route to always require a password generator when employing the specified access method.

13.5.4 Maintaining the Generator

The following explains how to:

- Alter your PIN number
- Change the generator batteries and reset the generator. (See the section entitled *Reset the Generator* for further details.)

Changing the PIN-number

The PIN number can be changed by the system administrator and by users themselves using the */bin/passwd(1B)* program or using *chs220pin*(1B).

Change the PIN as follows:

NOTE

Press C/CE *at any point during this procedure to terminate events. This leaves the old PIN still valid.*

1. Enter **`passwd -t s220pin`** at the system prompt.
2. Check that the generator is switched to SAFE.
3. Switch the generator on by pressing the ON button.
4. Enter the current PIN number (5 figures) and press PIN PIN.
5. The generator displays the six figure SPIN number.
6. Enter this number into the into the screen
7. Press PIN followed by TAN
8. Enter a new five figure PIN number and press PIN

   The generator now displays the six figure XPIN number.
9. Enter the XPIN into the screen
10. The PIN number is now altered.
11. Press MAC to finish this procedure.

Changing the Batteries

To change the batteries take the following steps:

1. Switch the generator to BATT.

2. Loosen the back plate with a screw driver.
3. The battery should now be visible.
4. Change the used battery.
5. Screw in the back plate.
6. Switch the generator back to SAFE. To check that the generator is working, press $\boxed{\texttt{ID}}$ and make sure that you get the correct ID displayed.

Reset the Generator

To reset the generator do the following:

1. Switch the generator to SAFE.
2. Loosen the back plate with a screw driver.
3. The used battery is now be visible.
4. Take the battery out.
5. Put the battery back in.
6. Screw in the back plate.

13.5.5 Synchronising the Generator

If a user has generated more than five one-time passwords which have not subsequently been used to access the system the generator and the database are at the wrong iteration and need re-synchronising.

Synchronise Generator

To synchronise the generator and the database take the *Synchronise Generator* menu choice from the *Password Generators* menu and enter:

`Generator ID`
: Identity number of the generator to be synchronised.

`SPIN from Generator`
: Generate a new SPIN in the usual way and enter the number displayed into this field.

If several BoKS domains need synchronising, a list must be created of these hosts so that they can be synchronised together. Use the *Add Host to List* option.

Add Host to List

NOTE

This section only applies if you need to synchronise several BoKS domains.

When the hosts are synchronised across several BoKS domains they must first be added to the lists of machines that are to be synchronised together. To do this take the *Add Host to List* option and enter the names of the hosts to be synchronised.

Synchronising Across a Network

Normally synchronisation is performed in conjunction with the local database being updated whenever a user logs in. The options under the column *Network Synchronisation* enable several machines which are governed by different BoKS databases (different BoKS domains) to be be synchronised so that all the password generator users on each of these machines are at the same one-time password iteration. If the machines are out of step with each other then a user can not use the same password generator for all the machines.

At installation a cron-entry is set up so that *cron*(1) initiates synchronisation on a regular basis.

NOTE

Only the hosts in the synchronisation list are synchronised.

The *Perform Synchronisation* option on the *Password Generators* menu enables hosts across a network to be manually synchronised. The following parameter can be given:

`Generator ID`

Enter the existing generator identity number.

If this field is left blank all existing password generators are synchronised.

Remove Host from List

To remove a host from the list take the *Remove Host from List* option and specify the name of the host.

Show Sync Host List

To list the hosts that are synchronised when using *Perform Synchronisation* select the *Show Sync Host List* option from the *Password Generators* menu. This menu choice only has one column entitled *Hosts* and lists the host names of the machines that are synchronised whenever the *Perform Synchronisation* option is taken.

This page is intentionally left blank.

14

PC-UNIX Integration

14.1 Outline

NOTE, THIS IS A PRELIMINARY DRAFT.

This chapter explains how to use the *BoKS PC-UNIX Integration* add-on module. This chapter enables you to add and remove the following information and objects:

- PC users
- Predefined views
- Access rules for predefined views
- Access rules for PC users

In addition this chapter explains how to manipulate the reports produced by the functionality outline above.

14.2 Outlook

The PC-UNIX integration feature enables you to administer users who log in via PC-Guard to a PC which is part of a BoKS domain and therefore controlled by a BoKS master-server. Through this module you are able to create and remove PC users and control the access rights assigned to each user.

NOTE *PC users can only be assigned to hosts that are setup in the BoKS database as the type PCBOKSHOST. Please refer to the "Host Administration" chapter for further details.*

Setting up PC users in this way means that their access to the system is authenticated by the central BoKS database. It also means that the access rights for each PC user can be controlled centrally from the BoKS master-server. A PC user can be assigned precisely the same type of access route attributes as any other user in the BoKS domain. These access routes are defined from the *User Admin* menu and the procedure is explained in the *User Administration* chapter. Assigning predefined views and access rights to PC users and PC groups is carried out from the *PC Guard User Admin* menu and is explained in this chapter.

14.3 Important Terms

In this chapter you encounter the following terms:

Access Rights

The right to access a system resource where resource can be a file, hard disk drive, directory. The access rights available are:

- read
- write
- open
- purge
- delete
- create
- administrate
- modify
- purge
- execute

Access Rule

The access rights assigned to a resource.

PC-Group

Grouping of the PCBOKSHOST user community. By default there are three groups:

- Master Administrator Group
- Local Administrator Group
- User Group

PC-User

User who resident on a host running DOS and is protected by PC-Guard.

Predefined View

Collection of access rules required to run certain applications.

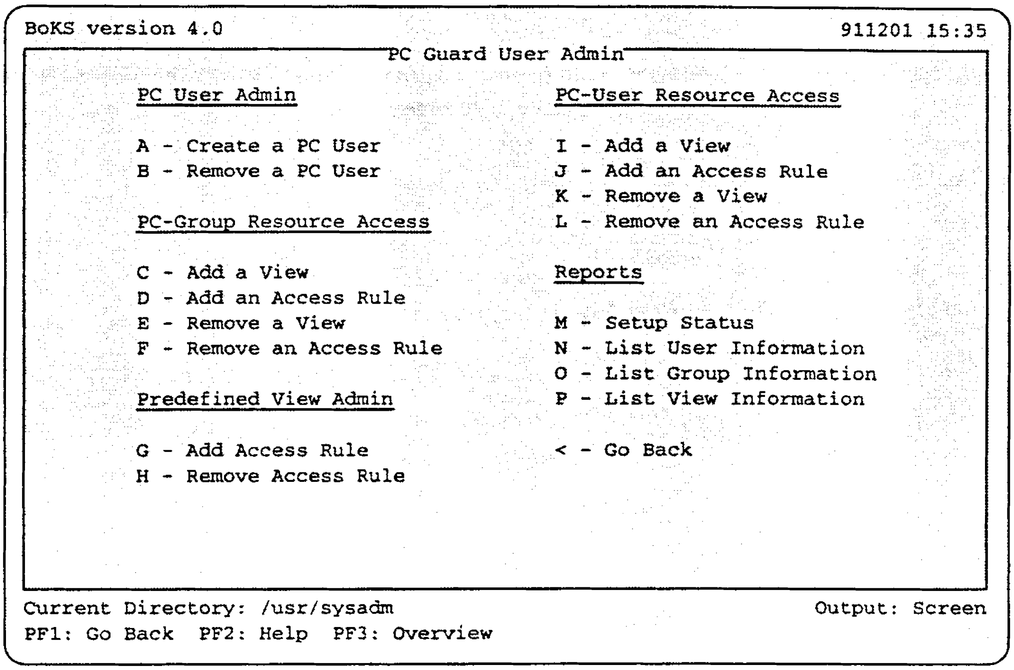
14.4 PC Guard User Admin Menu

The *PC Guard User Admin* menu in BoKS appears on the screen as displayed in figure *13.1.*

14.5 Functionality

This section explains how to use the menu choices on the *PC Guard User Admin* menu. Functionality can be divided into the following sections:

- Creating and removing PC-Users
- Adding and removing views for a PC-Group



```
BoKS version 4.0                                                  911201 15:35
                              PC Guard User Admin

      PC User Admin                      PC-User Resource Access

      A - Create a PC User               I - Add a View
      B - Remove a PC User               J - Add an Access Rule
                                         K - Remove a View
      PC-Group Resource Access           L - Remove an Access Rule

      C - Add a View                     Reports
      D - Add an Access Rule
      E - Remove a View                  M - Setup Status
      F - Remove an Access Rule          N - List User Information
                                         O - List Group Information
      Predefined View Admin              P - List View Information

      G - Add Access Rule                < - Go Back
      H - Remove Access Rule


Current Directory: /usr/sysadm                                  Output: Screen
PF1: Go Back  PF2: Help  PF3: Overview
```

Figure 13.1 Sub Menu, PC Guard User Admin

- Adding and removing views for a PC-User
- Adding and removing access rules for a view
- Reports

14.5.1 Adding and Removing PC-Users

Before PC-users can be administered centrally from the BoKS database they must first be added to the database. This is carried out using the *Create PC-User* menu choice.

NOTE *PC-users can only be added to hosts that have been defined as PCBOKSHOST using the "Add/Modify" option on the "Host Admin" menu.*

If you wish to remove a PC-user from the BoKS database, use the *Remove User* menu choice.

Create PC-User

To create a PC-User, select the *Create PC-User* menu choice and enter as follows:

NOTE *Once PC-users have been added to the BoKS database they can be administered from the "User Admin" menu in the same way as all other BoKS registered users.*

Host(group)

Host(group) that the PC-user is to be assigned to. This machine must have already been added to the BoKS database through the *Add/Modify* menu choice on the *Host Admin* menu. It must also have been registered as a PCBOKSHOST with this menu choice.

User

PC-user account name, which the PC-user enters when logging in.

Comment

Further information about the user. Typically this is the user's full name and possibly department details.

Access Route

Access method and route that the PC-user is to use to access the PC. Typically the following type of access route is used:

LOGIN:pc_console->pcnod

Where LOGIN is the access method used, pc_console is the location from where the access method is used and pcnod is the host that the PC-user able to access.

Start Time

Time of day from when the PC may be accessed. Entering 0 means that the PC may be accessed from 00:00. The entry format is HHMM using the 24 hour clock.

Stop Time

Time of day from when the PC may not be accessed. Entering 0 means that the PC may not be accessed from 24:00. The entry format is HHMM using the 24 hour clock.

Days of Week

Days of the week when the PC-user may access the PC. Format is 1234567, where 1 = Monday, 2 = Tuesday, 3 = Wednesday, and so on.

PC-Group

PC-Group the PC-user is assigned to. If the group that you specify here does not exist, it is not automatically created.

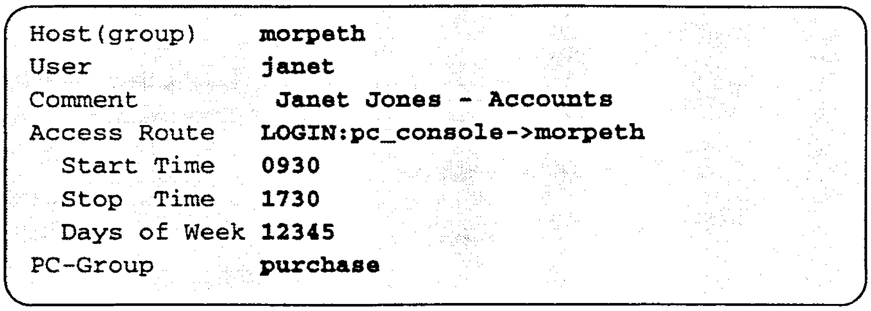
NOTE *You are required to provide the PC-user with a password when you first create the PC-user.*

Having brought the company's UNIX network under control with the help of BoKS, Tracey begins on stage 2 of her computer resource centralisation project. This stage involves connecting all the PCs running DOS to the network that she has setup with the UNIX machines and administering their machines from the BoKS master-server.

Tracey has already installed PC-Guard (a Data Access and Control System) on the DOS machines so that they are secured locally. Tracey was delighted with how easy it was to install PC-Guard on the PCs. When she had completed the tasks in the PC-Guard "Installation and Setup" guide she *confidently proceeded to add these PCs to the BoKS database using the "Host Admin" menu from the BoKSADM main menu, taking care to specify these hosts as PCBOKSHOSTs.*

Having added these hosts she was ready to add the PC-users to the BoKS database.

She selects the *Create PC-User* option and enters:



```
Host(group)     morpeth
User            janet
Comment          Janet Jones - Accounts
Access Route    LOGIN:pc_console->morpeth
  Start Time    0930
  Stop  Time    1730
  Days of Week  12345
PC-Group        purchase
```

Tracey repeats this for the rest of her PC-users. Once the PC-users are added to the database she administers them in the same way that she has administered all the other users previously.

Remove a PC-User

To remove a PC-user from the BoKS database, select the *Remove a PC-User* option and enter:

`User`
: Name of PC-user to be removed from the BoKS database.

`Remove All Information`
: Specify **yes** to remove PC-Guard information and the user. Specify **no** to remove PC-Guard information only.

14.5.2 Adding and Removing Access Rules for Predefined Views

Access rules may be both added and removed from a predefined view. This means that the users who have access to this predefined view access the current setup of the predefined view each time they log in.

Add Access Rule

The *Add Access Rule* menu choice under the *Predefined View Admin* column header enables you to add an access rule to a predefined view. Select this menu choice and enter:

`Predefined View`
: Name of the predefined view you wish to alter.

`Access Rule`
: Access rule you wish to add. The format is as follows:

```
resource;access_rights
```

For example: `C:DIR=.EXT;RWOCDASMX`

A sample screen entry is:

```
Predefined View     edlin
Access Rule         C:*;RWOCDMSX
```

Remove Access Rule

To remove an access rule from a predefined view, select the *Remove Access Rule* option under the *Predefined View Admin* column header and enter:

`Predefined View`

Name of the predefined view you wish to remove an access rule from.

`Access Rule`

Access rule you wish to deny the specified predefined view. Use the multi-pick function to specify the access rules.

14.5.3 Adding and Removing Predefined View for a PC-User

This section explains how to add and remove predefined views to/from a PC-User. A predefined view is a set of access rules which enables the PC-user to run an application. Several predefined views can be added to one PC-user.

Add View

To add a predefined view to a PC-user, select the *Add View* option under the *PC-User Resource Access* column header. Enter the following information:

`User`

Name of the PC-user to add the predefined view to.

`Predefined View`

Existing predefined view. The predefined view must be specified by one word only. If the predefined view does not exist it is not automatically created.

Remove View

To remove a predefined view from a PC-user, select the *Remove View* option and enter:

NOTE *When access to a predefined view is removed from a PC-user, the user loses the access rights specified in that view.*

`User`

Name of the PC-user to be denied access to a specific predefined view.

`Predefined View`

Name of a predefined view which was previously allocated to the PC-user.

14.5.4 Adding and Removing PC-User Access Rules

Specific access rules can be assigned and remove to/from PC-users. An access rule comprises:

- resource - the object that access is opened for. The format for a resource is "drive:resource name", for example `C:DIRed`. Wild cards may also be used when specifying the resource name. The following wild cards are available:

?	maps to one character
*	maps to any number of characters
=	maps to all files in the directory and all sub directories

  For example: `C:DIR=`

- access rights - the nature of the access that is being granted (one or a combination of the access rights below may be specified)

Possible access rights are as follows:

R	Access to a file and the permissions to read the contents of the file.
W	Access to a file and the permissions to add and edit data in the file.
O	Access to a file and the permissions to both read and write the file.
C	Create a new file.
D	Delete a file.
P	Overwrite the file and then delete it.
A	Create or remove sub-directories.
S	Search for a file.
M	Modify the name of a file or the DOS file attributes.
X	Execute permissions on a program.

Add an Access Rule

To add an access rule to a PC-user, select the *Add an Access Rule* menu choice under the *PC-User Resource Access* header and enter:

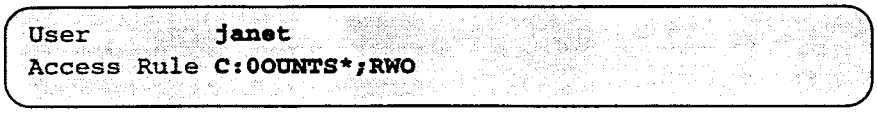
`User`
: Name of PC-user who is to gain access to an access rule.

`Access Rule`
: Name of the access rule to be added to the PC-user in the format:

```
resource;access_rights
```

For example: `C:DIR=.EXT;RWOCDASMX`

A sample screen entry is:



```
User         janet
Access Rule C:OOUNTS*;RWO
```

The above example enables members of the PC-user `janet` to read, write and open all files in the ACCOUNTS directory on drive `C`.

Removing an Access Rule

To remove an access rule from a PC-user, select the *Remove Access Rule* option under the *PC-User Resource Access* column header and enter:

`PC-Group`
Name of a PC-user you wish to deny an access rule for.

`Access Rule`
Access rule(s) to be removed from the PC-user. Use the multi-pick function to select the access rules.

14.5.5 Adding and Removing Predefined View for PC-Groups

This section explains how to add and remove predefined views to/from a PC-group. A predefined view is a set of access rules which enables members of the PC-group to run applications. Several predefined views can be added to one PC-group.

Add View

To add a predefined view to a PC-group, select the *Add View* option under the *PC-group Resource Access* column header. Enter the following information:

`PC-group`
Name of the PC-group to add the predefined view to.

NOTE *All members of the PC-group are granted access rules from the predefined view.*

`Predefined View`
Existing predefined view. The predefined view must be specified by one word only. If the predefined view does not exist it is not automatically created.

Remove View

To remove a predefined view from a PC-group, select the *Remove View* option and enter:

NOTE *When access to a predefined view is removed from a PC-group, all members of PC-group lose the access rights specified in that view.*

`PC-Group`
Name of the PC-group to be denied access to a specific predefined view.

`Predefined View`
Name of a predefined view which was previously allocated to the PC-group.

14.5.6 Adding and Removing PC-Group Access Rules

Specific access rules can be assigned and remove to/from PC-groups. An access rule comprises:

- resource - the object that access is opened for. The format for a resource is "drive:resource name", for example `C:DIRed`. Wild cards may also be used when specifying the resource name. The following wild cards are available:

?	maps to one character
*	maps to any number of characters
=	maps to all files in the directory and all sub directories

For example: `C:DIR=`

- access rights - the nature of the access that is being granted (one or a combination of the access rights below may be specified)

Possible access rights are as follows:

R	Access to a file and the permissions to read the contents of the file.
W	Access to a file and the permissions to add and edit data in the file.
O	Access to a file and the permissions to both read and write the file.
C	Create a new file.
D	Delete a file.
P	Overwrite the file and then delete it.
A	Create or remove sub-directories.
S	Search for a file.
M	Modify the name of a file or the DOS file attributes.
X	Execute permissions on a program.

Add an Access Rule

To add an access rule to a PC-group, select the *Add an Access Rule* menu choice under the *PC-Group Resource Access* header and enter:

`PC-Group`

Name of PC-group which is to gain access to an access rule.

NOTE *All members of the PC-Group gain access the specified access rule when they log in.*

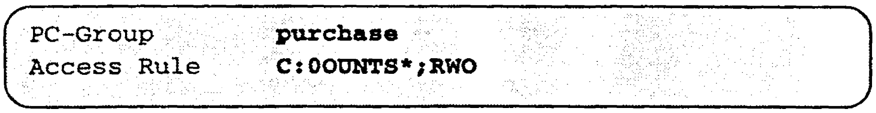
`Access Rule`

Name of the access rule to be added to the PC-group in the format:

```
resource;access_rights
```

For example: `C:DIR=.EXT;RWOCDASMX`

A sample screen entry is:



```
PC-Group        purchase
Access Rule     C:OOUNTS*;RWO
```

The above example enables members of the PC-group `purchase` to read, write and open all files in the ACCOUNTS directory on drive `C`.

Removing an Access Rule

To remove an access rule from a PC-group, select the *Remove Access Rule* option under the *PC-Group Resource Access* column header and enter:

`PC-Group`

Name of a PC-group you wish to deny an access rule for.

`Access Rule`

Access rule(s) to be removed for the PC-group. Use the multi-pick function to select the access rules.

15

BoKS Configuration

15.1 Outline

The following chapter explains the technical structure of BoKS. The chapter is divided up in the following manner:

- Introduction and background information on BoKS
- Tailoring the installation procedure with the *Setup*(1B) program
- Starting the BoKS daemons
- Configuring the BoKS menu system for different computer environments
- Different ways of administering BoKS
- Configuring some of the programs used by BoKS

15.2 Background Configuration Information

This section is designed to provide you with a deeper insight into how BoKS works and to the location of the different BoKS files. This section also explains which UNIX system files BoKS uses and which it replaces.

15.2.1 BoKS Geography

BoKS Product Directory - APPLPATH

The directory under which BoKS is installed. This directory is referred to as the *BoKS Product Directory* or APPLPATH. The majority of the BoKS files are located under this directory. APPLPATH is a variable which is set, for example, when **boksadm** is entered from the system prompt so that the administration programs can be located.

BoKS System Directory - BOKSDIR

When BoKS is installed a system directory is created. Typically this directory is */boks,* but can be defined anywhere on the system. Which ever file system is used must be mounted when the machine is booted otherwise system access is not possible. The location of this directory is specified using the *Setup*(1B) program. The *Installation Configuration* section further on in the chapter explains how to use the *Setup* program. The location of the system directory is specified by the variable BOKSDIR.

BOKSDIR and APPLPATH Settings

To discover which values the BOKSDIR and APPLPATH variables have, select the *BoKS System Information* menu choice from the *Reports* menu. This report displays the settings for both these variables.

BoKS System and Product Directory Contents

Figure *15.1* shows the structure of the BoKS product and system directories. In this example the product directory is */usr/boks* and the system directory is */boks.*

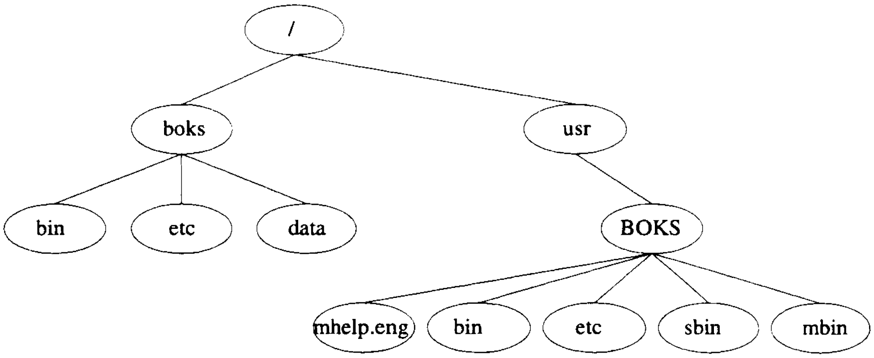


Figure 15.1. Contents of the BoKS Product Directory (/usr/boks) and system directory /boks). The directories under the BoKS system directory comprise:

`bin` All the background programs which are always executed on a host in the BoKS domain.

`data`

All the data files which are the heart of the BoKS domain. The information in these files covers system and user configuration, users access permissions, host configuration details, and so on. All the data entered from the BoKSADM menu system is stored here.

`etc` Combination of of text files which specify the current BoKS configuration and the important *Boot*(1B) program which is used when the BoKS daemons are stopped or started.

The directories under the BoKS product directory comprise:

`bin` Administration programs called by the BoKSADM menu system.

`inst`

Configuration files for the different installation scenarios and the programs used when installing or uninstalling BoKS.

`sbin`

Programs which are copied to the *bin* directory under the BoKS system directory during installation.

`mbin`

Menu tree binary files for the languages that BoKS supports. These files dictate the language and contents of the BoKSADM menu screens.

`mhelp.$MLANG`

Help directories which contain the menu choice help for the different menu choices in the BoKSADM menus. There is a directory for each language that BoKS supports (denoted by the $MLANG setting). For example the English help files are located under `mhelp.eng`.

Files Located Outside of the Product and System Directories

When BoKS is installed BoKS logs which files the installation procedure places outside of the BoKS system directory and which files or programs BoKS replaces. Precisely which files these are varies from UNIX-system to system. This information is placed in a log file which is located directly under the BoKS product directory. Typically this file is called LOGFILE. Please consult the log file to find out which files are located outside of the system and product directories on your system.

15.2.2 How BoKS Uses the UNIX System Files

This section explains how BoKS uses some of the UNIX system files.

/etc/passwd (4)

The file */etc/passwd*(4) is not used by BoKS when identifying and authenticating users. BoKS however does update this file with new users and information relevant to old users.

Password Field in /etc/passwd (4)

The password field in */etc/passwd*(4) is updated when a user's password is changed. This functionality can be turned off by using the *Password Parameters* menu choice on the *Parameter Configuration* menu.

If the passwords are no longer updated in the */etc/passwd*(4) file the entry `*no login*` is made in the password field.

NOTE

If NIS is running BoKS replaces the NIS database with the password file. When BoKS is installed users can be loaded into the BoKS database from the local password file and from the NIS database. From BoKS' point of view all usage of the NIS database stops from this point on.

The files *.rhosts*(4) and */etc/hosts.equiv*(4) is used to provide remote authentication for users accessing remote machines. It uses the concept of "trusted" users and hosts. These files are not used by BoKS. If a user is to access a remote machine, a relevant access route must be specified and entered into the BoKS database.

/etc/hosts(4)

The */etc/hosts*(4) file contains the names and IP addresses for each host in the local network. The format of an entry is:

```
IP-address   machine_name [alias]
IP-address   machine_name [alias]
256.240.0.23 bigbox mainmachine
```

BoKS uses the */etc/hosts*(4) file to discover which machines are stored on the local network.

NOTE

If NIS is enabled, the NIS database is used instead of the /etc/hosts (4) file.

/etc/group (4)

This file is used by `Help` when the field requires a list of existing system groups.

Overview of BoKS vs. NIS

As explained in the previous sections, BoKS uses parts of the NIS database if NIS is enabled. The following points explain how BoKS and NIS work together:

- Password section (passwd) can be read by the *Get User Data* menu choice when creating existing users from the NIS database. After this the password section (passwd) is not used by NIS.
- The group section (group) is used by the program which generates the on-line help for the `group` field.
- Host section (host) is used to find out which machines are included in the local network.
- All other parts of NIS are not used by or do not effect BoKS.

15.2.3 Examples of Different BoKS Domains

There are two main types of BoKS domain:

1. standalone version of BoKS with only one machine
2. network version of BoKS with one master-server, *n* number of slave-servers and *n* number of clients.

The standalone version of BoKS is almost identical to the BoKS master-server in a network. The BoKS network version can comprise several servers and a number of clients. A number of programs installed on the master-server are where appropriate also found on the other servers and clients.

BoKS Daemons

Updating the BoKS database and all user authentication is carried out by a number of daemons which are started when BoKS is installed. Which type of BoKS configuration has been installed determines which daemons run on each machine.

Program	Master-server	Slave-server	Client	Standalone
boks_master	Yes	No	No	Yes
boks_drainmast	Yes	No	No	Yes
boks_servc	Yes	Yes	No	Yes
boks_servm	No	Yes	No	No
boks_clntd	Yes	Yes	Yes	Yes
boks_bksd	Yes	Yes	Yes	Yes
boks_xd	Yes	Yes	Yes	Yes
boks_bridge	Yes	Yes	Yes	No

Functionality of the BoKS Daemons

This section explains the roles the different daemons fulfill:

boks_master

Reads, updates and removes fields in the BoKS database. This daemon runs on the machine in the standalone version of BoKS and on the master-server in the network version of BoKS.

boks_drainmast

Drains the BoKS database on the master of information which is queued to be retrieved by the `boks_servm` daemon for updating the slave database.

boks_servm

Retrieves a copy of the BoKS-database from the master-server. Sends information to the master-server. This daemon only runs on the slave-server.

boks_servc

Responds to queries from BoKS client programs. For example this daemon can respond to queries from *login*(1B), *passwd*(1B) and *su*(1B). This daemon runs on the standalone BoKS machine and on all servers in the network version of BoKS.

boks_clntd

Manages requests from BoKS administrative programs running on the master. This program runs on all machines in the BoKS domain.

boks_bksd

A daemon which checks the BoKS background monitoring function. This daemon runs on all machines in the BoKS domain.

boks_xd

Manages the inactivity monitoring for the BoKS screen lock functionality. Runs on all machines in the BoKS domain.

boks_bridge

Communication link between the different machines in the BoKS domain. This daemon only runs on the machines in the network version of BoKS

Figure *15.2* illustrates a typical setup for BoKS domain running the network version of BoKS. In this example the domain comprises one master-server, one slave-server and three clients.

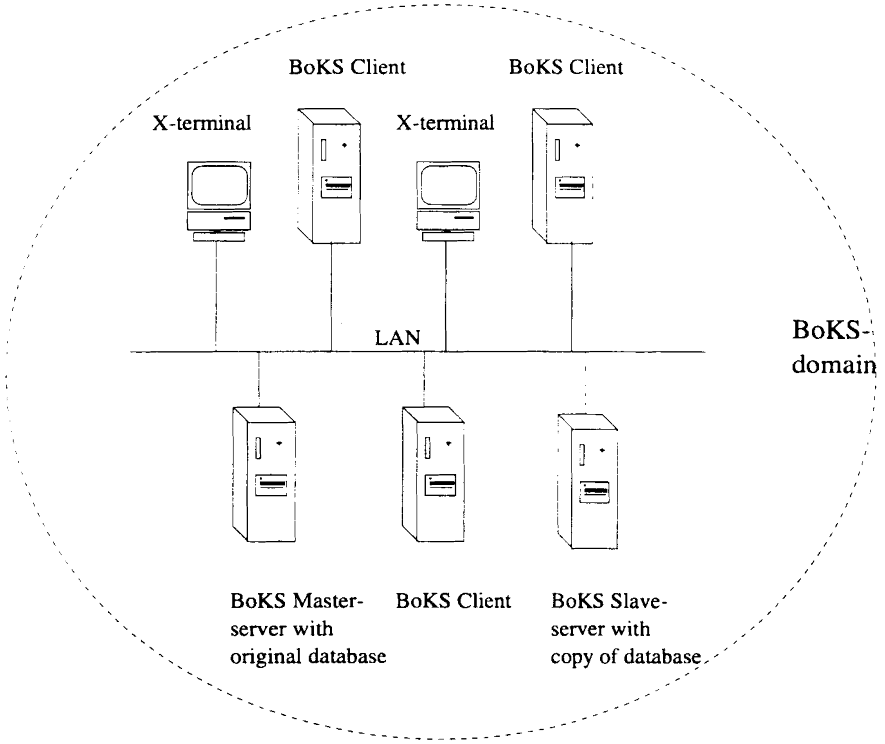

BoKS Client
BoKS Client
X-terminal
X-terminal
LAN
BoKS-domain
BoKS Master-server with original database
BoKS Client
BoKS Slave-server with copy of database

Figure 15.2. Sample BoKS Domain in the Network Version.

15.2.4 Configuring the Installation Procedure

BoKS has four standard configuration files which can be used at installation time. The configuration files are:

- STANDALONE
- MASTER
- SERVER
- CLIENT

These configuration files install the standalone, Master-server, Slave-server and Client components of BoKS respectively. The configuration files cover most machine requirements. However the configuration files can if necessary be configured either using the *Setup*(1B) program or editing the files directly.

NOTE *DynaSoft recommend that the Setup (1B) program be used because whilst the configuration files are shell scripts errors are more likely to occur if the files are edited directly.*

The Setup Program

The *Setup*(1B) program enables you to configure the way BoKS is installed and is located under the product directory. The program can be executed in one of two ways. If you enter:

```
# ./Setup
```

from the product directory ($APPLPATH) you are presented with a menu where you can select one of the following alternatives:

STANDALONE	BoKS Standalone module
MASTER	BoKS Master-server module
SERVER	BoKS Slave-server module
CLIENT	BoKS Client module

This then places you in the appropriate menu from where you are able to configure the installation procedure.

Alternatively you may enter (from the product directory $APPLPATH):

```
# ./Setup <module_name>
```

where `module_name` is the name of the module whose configuration procedure you wish to alter. For example:

```
./Setup STANDALONE
```

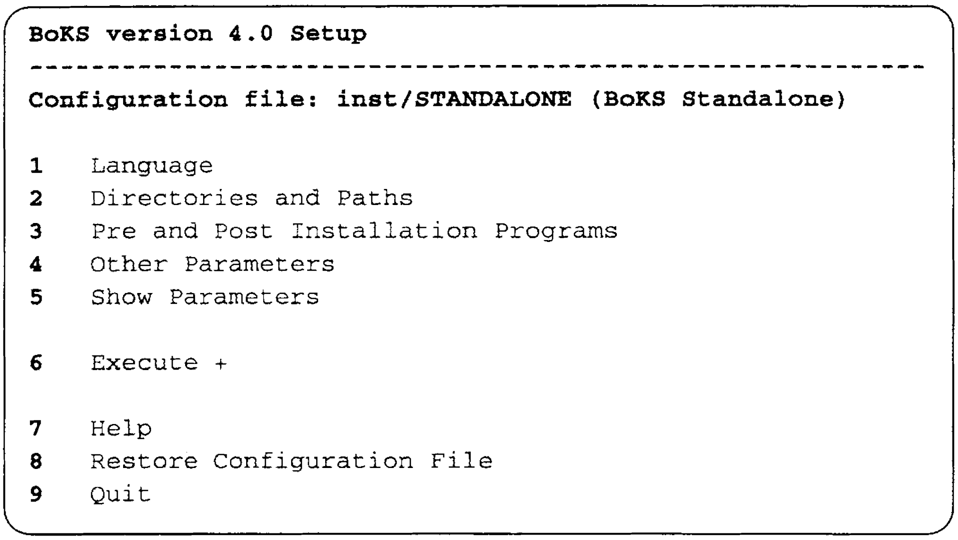
Setup(1B) is a menu driven program which enables you to alter a configuration file which belongs to a specific BoKS module.

To alter a module's installation configuration file, proceed as follows: (the STANDALONE module is used as an example here)

1. Enter the *Setup* command and the name of the configuration file you wish to alter. For example:

```
./Setup STANDALONE
```

2. The following menu appears:



```
BoKS version 4.0 Setup
---------------------------------------------------------
Configuration file: inst/STANDALONE (BoKS Standalone)

1    Language
2    Directories and Paths
3    Pre and Post Installation Programs
4    Other Parameters
5    Show Parameters

6    Execute +

7    Help
8    Restore Configuration File
9    Quit
```

3 The menu choices on the *Setup* menu enable you to specify the following:

`Language`

Language to use when running the following programs:

- *Install*
- *Uninstall*
- *Setup*

Once you have selected a language the *Setup*(1B) program is automatically restarted in the specified language.

`Directories and Paths`

Different locations for the different parts of BoKS. The locations that you can specify are: (Enter the new location when prompted if the location is to change, otherwise press **RETURN**)

- `Saved Database`

  This specifies where the BoKS database is to be saved when the program *Uninstall* is run. This setting can also be altered directly using the program *Uninstall.*

- `User Programs`

  Specifies where the program *boksadm*(1B) is to be located.

- `BoKS directory`

  Specifies where the BoKS system directory is to be located. Usually this directory is created as */boks.* If the "root" partition does not have enough disk space, it is appropriate to place it elsewhere.

- `X11 Programs`

  Specifies where the program *xdl*(1B) used by the BoKS display lock functionality is to be placed. This is only specified if the BoKS display lock module is specified.

`Pre and Post Installation Programs`

Programs to be executed before and after installation and before and after uninstallation. There are four fields: (Enter a program when prompted otherwise press **RETURN**)

- `Pre-Install Program`

  Specify a program to run before installation.

- `Post-Install Program`

  Specify a program to run directly after installation.

- `Pre-Uninstall Program`

  Specify a program to run before uninstalling BoKS.

- `Post-Uninstall Program`

  Specify a program to run directly after uninstalling BoKS.

`Other Parameters`

Miscellaneous parameters which comprise: (Make an entry when prompted otherwise press **RETURN**)

- Log File

  Name of the file to store the results of the install and uninstall procedures.

- Character set in boks

  Specifies which character set is used by the BoKSADM menus and for the login messages.

- Standard terminal type

  Default setting if the TERM variable is not set (only applies to new users).

- Automatic X locking (y/n)

  Specify **y** to enable X-display lock or **n** if it is to stay disabled. (Typically **n** is specified if you are not running BoKS in an X-Windows environment.)

- Modify X setup file(s) (y/n)

  Specify **y** if BoKS X display lock is to be enabled instead of your system's display lock program.

`Execute`

Enables you to execute the *Install, Upgrade* and *Uninstall* programs.

`Show Parameters`

Displays the current setup of the installation parameters.

`Help`

Help for the *Setup* menu.

`Restore Configuration File`

Restores the *Setup* configuration file which existed before you ran the *Setup* program this time. The file *<module_name>.BAK* is copied to the file *<module_name>*.

`Quit`

Enables you to quit from the *Setup* menu.

15.3 Stopping and Starting the BoKS Daemons

On every machine where BoKS is installed there are always a number of daemons running. These daemons are listed in table *15.1.*

15.3.1 BoKS Start Program Boot

The BoKS daemons are started automatically when the UNIX system is booted. The program */boks/etc/Boot*(1B) starts the BoKS daemons automatically when the UNIX system boots up into multi-user mode. The daemons started are those specified in table *15.1.*

Definition of how the */boks/etc/Boot*(1B) program is run is defined automatically during BoKS installation. This varies from machine type to machine type.

System V

The file *S99boksstart(4B)* is added to the directory */etc/rc2.d*

SUN OS and DEC ULTRIX

Method for starting */boks/etc/Boot*(1B) program is defined in */etc/rc.local*(8)

HP UX

Method for starting the */boks/etc/Boot*(1B) program is defined in */etc/rc*(8)

15.3.2 Stopping and Starting the Daemons Manually

The */boks/etc/Boot*(1B) program can be run directly from the system prompt.

Re-starting the Daemons

If the system directory is */boks* enter the following to start the daemons on your system:

```
# /boks/etc/Boot
```

Stopping the Daemons

If the system directory is */boks* enter the following to stop the daemons on your system:

WARNING **If the daemons are stopped on all BoKS servers no users are able to log in.**

```
# /boks/etc/Boot -k
```

15.4 Configuring the BoKS Menu System

The BoKS menu system (BoKSADM) is available for two different environments:

- X-Windows environment
- Character terminals

The major difference between the two environments is that the X-Windows version supports the use of a mouse and you are able to select which typeface is used to display the menus. In other respects BoKSADM has the same functionality in each environment.

This section explains how to:

- Select a language to run the menus and screens in
- Select a character set to display the language
- (Re)define the function keys
- (Re)define screen box characters
- Specify a type face if using BoKSADM in an X-Windows environment

BoKS is typically administered through the BoKSADM menu system. This needs the MENUETT menu handler to be installed and the *menuett*(1B) program needs to be located in a directory specified as part of the *$PATH* variable.

15.4.1 Different Languages and Character Sets

This section explains how to change and administer the different languages and character sets which BoKS supports.

Languages Supported by BoKS

To see which languages are supported in your version of BoKS do the following: (assuming that your product directory is */usr/dynprods/BOKS):* Enter:

```
# cd /usr/dynprods/BOKS
# ls -d mhelp.*
```

This lists the help directories. The three letter suffix after the "." denotes which language the mhelp directory supports.

Specifying a Language

To change the language that the BoKSADM menu system set the MLANG variable.

MLANG Variable

To set the MLANG variable for a superuser in the Bourne Shell enter:

```
# MLANG=<lang>
# export MLANG
```

at the prompt, where `<lang>` is the three letter suffix after the "." in the mhelp directory name.

To set the MLANG variable permanently for a superuser who uses the Bourne Shell, edit the superuser's *.profile* file. Add the lines specified above to the file.

To set the MLANG variable for a superuser in the C Shell enter:

```
# setenv MLANG <lang>
```

at the prompt, where `<lang>` is the three letter suffix after the "." in the mhelp directory name.

To set the MLANG variable permanently for a superuser who uses the "C" Shell, edit the superuser's *.login* file. Add the line specified above to the file.

Specifying a Character Set

Different languages need different character sets to be displayed correctly on the screen. The variable MENUASCII defines the character set in use. The different character available for BoKS are as follows:

MENUASCII Variable

- 7BIT

  Standard 7bit ascii character set.

- 8BIT

  ISO 8859-1 standard 8bit character set. This character set is used by VT200 terminals, for example.

- ROMAN8

  Hewlett Packard 8bit character set, used by HP terminals.

- IBMPC

  IBM 8bit character set (code page 850). This character set is used on IBM RS6000, RT and PC with DOS version 4 and later.

To set the MENUASCII variable for a superuser in the Bourne Shell enter:

```
# MENUASCII=<character set>
# export MENUASCII
```

at the prompt, where *<character set>* is one of the four listed above.

To set the MENUASCII variable permanently for a superuser who uses the Bourne Shell, edit the superuser's *.profile* file. Add the lines specified above to the file.

To set the MENUASCII variable for a superuser in the C Shell enter:

```
# setenv MENUASCII <character set>
```

at the prompt, where *<character set>* is one of the four character sets listed above.

To set the MENUASCII variable permanently for a superuser who uses the "C" Shell, edit the superuser's *.login* file. Add the line specified above to the file.

Terminal Specific Changes in the File envmake

To set the MENUASCII variable globally for a particular terminal type, edit the file *$MENUPATH/etc/envmake.* Enter:

```
# <terminal type>: MENUASCII=<character set>
```

In the above syntax `<terminal type>` is the terminal as denoted by the variable $TERM. `<character set>` is one of the four character sets listed above.

The file may contain the following type of entries:

```
vt1*: MENUASCII=7BIT
vt2*: MENUASCII=8BIT
hp*: MENUASCII=ROMAN8
```

15.4.2 Defining the Function Keys

Terminfo Database in MENUETT

MENUETT has a terminfo database which contains definitions of which keys produce the code required by the menu handler to operate the function keys. These definitions can be altered by editing the file *$MENUPATH/etc/term.ti.* This file contains the definitions for the symbols "kf1," "kf2," "kf3" and "kf4" *Go Back, Help, Menu Help* and *Execute* respectively.

The symbols "lf1," "lf2," "lf3" and "lf4" define the function key labels. For example the default definition for a Vt200 terminal sets kf1-kf4 to the code which the keys PF1-PF4 produce. The symbols lf1-lf4 are defined with the labels "PF1," "PF2," and so on.

Re-compiling the Terminfo Database

For new definitions to apply MENUETT's terminfo database must be recompiled. The easiest way of doing this is to reinstall MENUETT. If MENUETT is installed as */usr/dynprods/menuett* the following would be entered:

```
# cd /usr/dynprods/MENUETT
# ./Install
```

15.4.3 Defining the Box Set Characters

The boxes displayed on the screen are built in the following order of priority:

1. If the environment variable MENUBOX is set this value is used. This variable defines the box characters in the following order:
   - horizontal line
   - vertical line
   - top left corner
   - top right corner
   - bottom left corner
   - bottom right corner
2. If the current terminal type is defined in the file *$MENUPATH/bin/boxset*(1B) the MENUBOX variable is set to values specified for the current terminal type.
3. If the system supports specifying the box characters in terminfo.
4. If the terminal supports reverse video the box is displayed as if MENUBOX="(six spaces)".
5. If none of the above applies set MENUBOX as "-!++++".

NOTE *Graphics character are not supported by SUN's command tool and shell tool. The graphics characters are represented using 'normal' characters as explained in the last point.*

Defining Fonts

This section only applies if you are running BoKS in an X-windows environment.

NOTE *For BoKSADM to start correctly in an X-Windows environment the following must be the case:*

1. *The DISPLAY variable is set*
2. *The program "xterm" is available*

If one of these criteria is not met then mouse support is not enabled and the BoKSADM menu starts as it would on a character terminal

The different fonts files used are placed in different places on the different UNIX variants. Please check your X documentation to find out the correct location and name of the font file on your particular UNIX variant. Often you will find these files under the *fonts* directory.

NOTE *If 8-bit character support is required the font must support ISO-8859-1 so that 8-bit characters are*

The font can be specified by setting the variable MENUETT_XFONT. The list of available fonts can be listed using the command `xlsfonts`. In the Bourne shell enter:

```
MENUETT_XFONT='<font_name>' ; export MENUETT_XFONT
```

In the C-shell enter:

```
setenv MENUETT_XFONT '<font_name>'
```

Where *<font_name>* is the name of the font as listed by `xlsfonts`.

Adding to the Menu Tree

BoKSADM can be added to using the development module for the menu tree called MENUETT Development. The manual *MENUETT Development - Programming Manual* provides full information on this product.

15.5 Different Ways of Administering BoKS

The following section explains the different ways in which you can administer BoKS. BoKS can be administered through the BoKSADM menu system or from the system prompt. We recommend that you mainly use BoKS functions from the menu as there is much more powerful validation of the data passed to the different programs.

This section explains how to carry out the following:

- Start the BoKS menu system in debug mode so that the commands are displayed before they are executed.
- Start the BoKS shell so that BoKS administration programs can be run from the system prompt.

15.5.1 Starting BoKSADM in De-bug Mode

boksadm -d

By starting BoKSADM in de-bug mode each menu choice displays the program about to be executed. To start BoKSADM in de-bug mode enter:

```
 # boksadm -d
```

at the system prompt.

If BoKSADM is started in de-bug mode a pop-up box appears on the screen after each menu choice is selected displaying exactly what is being passed to the command line. This has two advantages:

1. You are able to learn more about the inner-workings of BoKS by using it in de-bug mode. This in turn enables you to manipulate BoKS in your environment.
2. You are no longer running BoKS "blind" and so you can understand what is occurring once you have executed a particular option. In this way you can work through any problems that might occur,

pinpointing the problem at source.

15.5.2 Running the Administration Programs from the System Prompt

boksadm -S

All the functions which are executed from BoKSADM are external programs. BoKSADM is a menu-driven front-end which enables you to execute these programs without worrying about the command line syntax.

All the commands executed through the menu system can be executed from the command line too, provided that the system environment is correctly setup.

The most simple way to make sure that the environment is setup correctly, is to use the BoKS shell. To execute a BoKS shell enter:

```
# boksadm -S
```

from the system prompt. Please see the *BoKS Reference Manual* and the *Reference* chapter in this manual for information on the individual BoKS programs.

To leave the BoKS shell, enter:

```
exit
```

15.6 Configuring the Functionality of BoKSADM

This section explains how to:

- Configure the backup functions available in BoKS
- Specify user startup files
- Specify which audit events are logged as alarms

15.6.1 Configuring the Backup Function

This section explains how to configure the backup functions available in BoKS.

Changing the Backup Program

The default program used to backup the BoKS database and BoKS logs is *tar*(1). To change this default, edit the *boks_bru*(1B) file located under the *bin* directory in the product directory. Replace the *tar*(1) command with the backup command of your choice.

Adding to the List of Backup Devices

To add to the list of devices that you can choose between when backing up the BoKS database and BoKS logs, edit the file *bdevlist*(4B) which is located under the *etc* directory in the product directory. Specify the device or devices you want to use.

15.6.2 Alarm Configuration

To specify which audit events are classified as alarms edit the file */boks/etc/alarmlogs*(4B). This file contains the labels for the messages defined in the files */boks/etc/mess.swe*(4B) and */boks/etc/mess.eng*(4B).

The menu choice for querying the logs also contains a field which enables you to specify if only alarm events are to be shown.

15.6.3 BoKS user Startup Files

This section explains :

- Functionality of a user startup file
- How to use a user startup file

User Startup File Functionality

In BoKS a user startup file is a file which is copied into the users' home directories when they are first created. The user startup files typically contains a list of actions to be carried out when the user logs in or starts an application. Typical user startup files are *.profile, .login* and *.mailrc*. These files are executed when the user logs into the system. The *.login* file is executed when logging into the C shell and the *.profile* file is executed when logging into the Bourne shell. The *.mailrc* file is used by the electronic mail system.

Defining a User Startup File

An arbitrary number of user startup files can be copied to the user's home directory when the user is created through BoKS. The files for copying are listed on a host/hostgroup basis, this means that each machine in BoKS has its own definition of which user startup files are to be used.

In BoKS there are two configuration files for specifying which files are to be copied. The first file is */boks/etc/host2profiles* defines which "profilelist" file a host is to use. The format of the */boks/etc/host2profiles* file is as follows:

```
<host1/hostgroup1>          <profilelist_file1>
<host1/hostgroup2>          <profilelist_file2>
```

host is the *hostname* for the machine in the network, *hostgroup* is a hostgroup that has been defined in BoKS. *profilelist_file* is the full pathname of the file which contains a list of user startup files for copying. The following shows typical contents for the */boks/etc/host2profiles* :

```
bigbox     /boks/etc/big_profiles
littlebox  /boks/etc/little_profiles
SALES      /boks/etc/SALES_profiles
```

The "profilelist" file is the second configuration file for configuring user startup file functionality. It has the following format:

```
# All lines not beginning with a '/' are assumed to be comments
#
# The /etc/stdprofile file is copied over as the .profile file
# in the user's home directory
/etc/stdprofile       .profile

# If the to-file is not defined the base-name of the from-file is
# used with a leading '.'. The file specified below is copied to .login
# /usr/dynprods/etc/login
/usr/dynprods/etc/login

# Sub directories to the users' home directories can also be specified.
# If the sub directory does not exist it is not created.
#
/usr/lib/X11/xdm/Xsession.std xdm/.Xsession
```

If the file */boks/etc/host2profiles"* does not exist a certain host is not mapped to "profile list" file, the file */boks/etc/def_profiles* is used instead. By default this file contains *$APPLPATH/etc/profile, $APPLPATH/etc/login* and *$APPLPATH/etc/cshrc.*

16

Troubleshooting

16.1 Overview

This chapter enables you to understand and solve problems that could potentially occur both during and after installing BoKS. The following types of problems occurring in the following circumstances are explained:

- BoKS installation
- Configuring and using BoKS
- BoKS networks and domains
- BoKS licencing
- BoKS error messages

The term *reason* is used in the sense of *probable reasons* for the problem. It is possible that these probable reasons do not apply to your system. This chapter is designed to help you solve any potential problems. If you are unable to solve the problems, please contact your BoKS help desk.

NOTE *In the different examples below BoKS, the system files are installed under /boks. This does not need to be the case as BoKS can be installed at any appropriate place in the file system.*

To check where BoKS is installed, enter the following at the system prompt:

```
# boksadm -S
BoKS > boksdir
```

There are different directories for programs, configuration files and data files. In the examples below these files are placed in the following directories: /boks/bin, /boks/etc and /boks/data. The files can be located in any appropriate place.

To check the locations of the files, enter the following at the system prompt:

```
# boksadm -S
```

You are now in the BoKS shell. From the BokS shell enter the following: In our example the following responses are also displayed:

```
BoKS > boksdir bin
/boks
BoKS > boksdir etc
/boks/etc
BoKS > boksdir data
/boks/data
```

The *boksadm*(1B) program can not be run on BoKS clients and BoKS slave servers. To find out where the *Boot*(1B) program is located, check the file /etc/nonstopconfig. The *Boot*(1B) program is located under the BOKS_etc directory. The location of the BOKS_etc directory is defined in /etc/nonstopconfig. Normally BOKS_etc is defined as /boks/etc.

16.2 Potential Problems when Installing BoKS

Below is a description and explanation of the types of problems that can occur during installation of BoKS and the appropriate action that can be taken.

Not Able to Read the Distribution Media

Reason

Incorrect restore command (normally this is *tar*(1)).

Action

Check the label on the media and make sure you are entering the correct command and syntax.

Reason

Incorrect media device.

Action

Check the type of media device on your machine. Please refer to your UNIX reference manual or UNIX help desk if you need help in finding the name of the media device. The device is typically a variant of `/dev/rmt`.

Reason

Insufficient disk space for BoKS to be loaded.

Action

Carry out some or all of the following:

- Clear out some disk space on the relevant partition

- Load BoKS onto another partition
- Acquire more disk space

Reason

Media contents are incorrect.

Action

Contact your BoKS supplier for new media.

Installation Program Aborts

Reason

The machine is not configured for the use of any or all of the following:

- semaphores
- message queues
- shared memory

To check whether your machine has been configured for the above enter the following at the shell prompt:

```
# ipcs
```

This specifies if shared memory, message queues and semaphores are configured.

Action

The machine's UNIX kernel needs to be reconfigured. Please refer to your UNIX support desk or UNIX manual reference pages for further information.

Reason

Not enough free disk space on the partition where the BoKS database is installed. (Typically the BoKS database is installed as */boks* and therefore is installed on the root partition.)

Action

There are several courses of action that can be taken in this situation:

- Empty out or increase the size of the partition. Please refer to your UNIX reference manual or help desk when increasing the size of the partition.
- Place the BoKS database and important BoKS programs on a different partition. Run the installation *Setup*(1B) program located in the $APPLPATH directory and change the *BoKS*-directory parameter. Change to a directory which is on a file system containing at least 2 Mbytes of free disk space.

NOTE

The partition where the BoKS programs and database are located must be automatically mounted when the machine is booted. On the BoKS master-server the partition must be mounted in single-user mode.

Please refer to the *Configuration* chapter for a detailed description of the *Setup*(1B) program.

16.3 Problems when Setting up BoKS

User ID Conflicts from Get User Data

Reason

When the menu choice *Get User Data* on the *User Admin* menu is executed there are one or more users who have the same user IDs as other users already existing in the database. The user(s) who have user IDs that are already allocated in the BoKS database are not created.

Action

Check which users have not been created using the *Log from Get User Data* menu choice on the *User Admin* menu.

For the users who have not been created, carry out the following actions:

1. Change the users' IDs in the */etc/passwd*(4) file to user IDs that are not already allocated. The user ID is located in the third field of the file.
2. Change the ownership on the users' files so that they are owned by the new user IDs.

   For example:

   If you change the user ID for the user `tracey` you could change the ownership on her files to the new user ID by entering the following command:

```
# find /home_dir -user <previous UID> -print %| xargs chown user_name
```

   Where `/home_dir` is the name of `tracey's` home directory, for example */home/tracey* and `user_name` is the name of the user, for example *tracey.*

3. Run the *Get User Data* menu choice again. The users who have already been created are ignored.

16.4 Problems when Starting/Using the BoKS Administration Menus

Cannot Find MENUETT

BoKS cannot find the menu handler MENUETT. This must be installed on the machine where BoKS is administered from.

Reason

MENUETT has not been installed.

Action

Install MENUETT. The menu handler comes with the BoKS licence and has probably not been loaded into a directory under the BoKS parent directory - (for example if the parent directory is */usr/dynprods* BoKS is loaded as */usr/dynprods/boks* and MENUETT is loaded as */usr/dynprods/menuett*). Change directory to where MENUETT has been loaded and run the installation program *Install.* To find out where MENUETT has been installed, enter the following at the shell prompt:

```
# find / -name menuett -type d -print
```

NOTE *This search can take several minutes if there is a lot of data on the system.*

For more information on how MENUETT is installed, please refer to the *BoKS - Getting Started* guide.

Reason

The startup script *menuett*(1B) is not in the current PATH.

Action

Check where the start script is located by moving to the directory where MENUETT is installed and enter *Setup*(1B) -program at the system prompt. For example normally the location is */usr/dynprods/menuett.* In this case enter the following:

```
# cd /usr/dynprods/menuett
# ./Setup MENUETT
```

Select the *Display Parameters* menu choice from the *Setup* menu. The *General Program* setting defines where the start program is located.

Check that the start program directory is in the current PATH setting. If the start program *menuett*(1B) is located under */usr/local/bin,* you would change the PATH setting as follows (in the Bourne Shell):

```
# PATH=$PATH:/usr/local/bin
# export PATH
```

Alternatively if using the C-shell you change the PATH as follows:

```
# setenv PATH $PATH:/usr/local/bin
```

In order to ensure that this is the PATH setting each time you log in, change your login startup file (*.profile, .login,* and so on. The easiest way to change the login startup file is to use the *Modify User* option on the *User Admin* menu in the BoKSADM menu system.

boksadm does not start - cannot initiate unknown terminal

Reason

Current terminal type is unknown or undefined.

Action

See the *Function Keys Do Not Work* section below.

Reason

The variable TERM has a setting for a terminal not supported by BoKS (or more correctly MENUETT).

Action

There are two possible courses of action:

1. Check if the terminal can emulate a vt100 or vt200. These terminal types are supported by BoKS. If this is possible change the TERM setting accordingly.
2. Define the function keys in the terminfo-database for this terminal type. Please refer to your UNIX reference material or help desk for further information on this course of action.

The *Configuration* chapter contains information on how to add to the MENUETT terminfo-database .

The Graphics Characters on the BoKSADM Screens are Missing or are Incorrect

The appearance of the BoKSADM screens are controlled by the variables MENUBOX and MENUBATTR. MENUBOX defines which box characters are used. MENUBATTR defines the attributes used. By combining these two variables in different ways, different problem situations can be solved.

For further details on MENUBOX and MENUBATTR please refer to the *Configuration* chapter.

Reason

MENUETT does not know how to display the graphical characters defined as the box characters.

Action

Check which characters the terminal uses in graphics mode to display the horizontal line, vertical line and the four characters used to display the top and bottom left and right characters. Check that the MENUBOX variable is set to these characters before the BoKSADM menu system is invoked.

For example:

```
# MENUBOX=qxlkmj
# export MENUBOX
# boksadm
```

To discover which graphics characters are used in graphics mode please refer to the manual for your terminal or your UNIX help desk.

Reason

The current terminal type does not support graphics characters.

Action

If the terminal supports reverse video, you can display the menu box by using reverse video. To achieve this, enter the following:

```
# MENUBOX="        "
# MENUBATTR=RRRRRR
```

The syntax means the MENUBOX variable specifies six spaces (with a backslash before each one to stop the shell interpreting them as field separators) and the MENUBATTR specifies that each space is to be displayed in reverse video (R).

16.5 Problems When Logging In

No Users Can Log In

Reason

All users have not been granted access routes to the system. This is the case typically directly after BoKS has been installed but before any initial configuration has been carried out.

Action

Log in as `root` on the console at the machine where BoKS is controlled from. Invoke the BoKSADM menu system and grant access routes to the users.

Reason

The authentication method is globally set to *locked.*

Action

Log in as `root` on the console at the machine where BoKS is controlled from. Initiate the BoKSADM menu system and change the authentication method with the menu choice *Default Specific Setup* and/or the menu choice *Define Specific Setup* on the *Authentication Methods* menu.

Reason

The program */boks/bin/boks_servc*(1B) is not running.

Action

Log in as `root` on the console on the machine where BoKS is controlled from. Start the */boks/bin/boks_servc*(1B) program by entering:

```
#  /boks/etc/Boot
```

A User Can Not Log In

Reason

The problem is usually that BoKS considers this user to be unauthorised for system access for some reason.

Action

Invoke the BoKSADM menu system and check the user setup using the menu choices *User Data* and *Full User Setup* on the *User Admin* menu. These reports display the setup information about users on the system including if they are blocked from system access, if their passwords have expired, the access routes that have they can use, and so on.

If this information does not provide you with enough information, set the login mode to *verbose.* Set the login mode by using the *Login Parameters* menu choice on the *Parameter Configuration* menu. When the login mode is set to verbose, the reason for system access denial is specified next time the user tries to log in. Take the appropriate action once you have discovered the reason for system access denial (for example adding access routes, extending the period of validity for a user account).

16.6 Problems in Using BoKS Programs When Identifying Authorised Users

NOTE *BoKS exchanges the original UNIX authentication programs for BoKS ones which refer to the BoKS database. This occurs during installation of BoKS and the original programs are moved to <filename>..org.*

Note that the location of these programs can vary from UNIX system to UNIX system. In the examples below the original programs are placed under "/usr/etc" and "/bin". To find out which programs have been replaced by BoKS ones, enter:

```
# cat /boks/etc/orgmodes
```

This command lists which files have been moved and their permission settings.

BoKS carries out user identification, using the following programs:

- */bin/login*(1B)
  Local login program
- *telnet* and *rlogin*
  Log in remotely over a network. Identification is normally carried out by the */bin/login*(1B) program in these cases.
- */bin/su*(1B)
  Adoption of another user's ID.
- *ftp*(1)
  File transfer (File Transfer Program). Identification is carried out by the program*ftpd*(1B).
- *net login, net use* and *net print*
  PCNFS programs executed on a PC. Identification is carried out by the program *rpc.pcnfsd*(1B).

- *xdm*(1B)

  Log in via an X-terminal or workstation running in an X-Windows environment.

- *rshd*(1B) or *remshd*(1B)

  Remote commands which use *rshd*(1B) or *remshd*(1B) include *rcp*(1).

Identification Does Not Work Using Any of the Programs

Reason

The program */boks/bin/boks_servc*(1B) is not running.

Action

Log in as `root` on the console connected to the machine where BoKS is controlled from and restart the */boks/bin/boks_servc*(1B) program by entering:

```
# /boks/etc/Boot
```

PCNFS net login Does Not Work

Reason

The program */usr/etc/rpc.pcnfsd*(1B) is not running. Restart the program by entering:

```
# /usr/etc/rpc.pcnfsd
```

General Problems with Identification and/or Communication Between BoKS Programs

Reason

One of the BoKS programs have stopped. The different programs running in the different configurations are defined in the *Configuration* chapter.

Action

Restart the BoKS programs by entering:

```
# boks/etc/Boot
```

on the machine where the BoKS programs are not functioning correctly. On the BoKS clients and BoKS slave-servers you can locate the *Boot*(1B) -program by consulting the file */etc/nonstopconfig.* The *Boot*(1B) -program is located in the BOKS_etc directory which is defined in the */etc/nonstopconfig* file. Typically BOKS_etc is defined as */boks/etc.* On the BoKS master-server and in the standalone version of BoKS the easiest way to discover the location of the *Boot*-program is to enter:

```
# boksadm -S
```

Now that you are in the BoKS shell, enter:

```
BoKS > boksdir etc
```

16.7 Network Related Problems

Changed Node Names on a Machine

If the node name has been changed for a particular machine all the users who are created for that machine are linked to the wrong host machine. As the network communication between these machines is based on IP-addresses, the user authentication still works.

Changed IP Address for a Machine

If the IP address is changed in the */etc/hosts*(4) file (or equivalent) this changed must also be made in the BoKS database. This is achieved by entering the following:

```
# boksadm -S
```

Once in the BoKS shell, enter:

```
BoKS > hostadm -hhostname -iIP-address
```

16.7.1 Licencing Problems

Too Many Users - Users Are Unable to Log In

Reason

The maximum number of concurrently logged in users has been reached.

Action

There are two possible courses of action:

1. Log out some of the users or log some of the users out of some of the windows if they are using a workstation or an X-terminal.
2. Upgrade your BoKS licence. Contact your BoKS supplier for further information if you wish to pursue this course of action.

Too Many Clients

Reason

Maximum number of clients in the BoKS domain has been reached.

Action

Upgrade your BoKS licence. Please refer to your BoKS supplier for further information on this course of action.

16.8 Integrity Check Warnings

This section explains the reason for the most typical warnings produced by the integrity checker function. These warnings are displayed in the *Integrity Check* report accessed from the *Integrity Check* menu.

4. A '+' entry in /hosts.equiv

Reason

If you are not running the BoKS versions of *login, rshd* and *rexecd* programs, the machine can be accessed without passwords from all other machines in the network.

Action

Install the BoKS versions of these programs or remove the line in */hosts.equiv*(4).

5. Non root entry in /.rhosts, machine users

Reason

Please refer to the warning above (warning number *4*). In this context, however, users on a particular machine are able to obtain `root` privileges.

Action

Install the BoKS versions of the *login, rshd* and *rexecd* programs. Alternatively remove this line in the */.rhosts*(4) file.

6. A '.' (current directory) is in root's path

Reason

When `root` executes a command the current directory is searched for that command. This is because the current directory is specified as part of the PATH setting. This can lead to the accidental execution of a Trojan horse program in a directory which can be written to by the entire user population.

NOTE

It is not fully secure to have the current directory specified as the last directory in the PATH setting. This is because Trojan horse programs can be hidden in files with the names using common misspellings of system programs.

Action

Put only trusted directories in the PATH setting for `root`. This means that directories which are able to be written to by the entire user community and the current directory must not be added to the PATH setting.

10. NFS file system is exported with no restrictions

Reason

The file system can be read and can be written to from users on all machines in the network. This includes personal computers running NFS programs (for example PCNFS).

Action

Export only the file systems to the machines which need access to them. To do this, modify the */etc/exports(4)* file or consult your UNIX documentation.

UNIX Reference Pages

exports(4)

20. The file <filename> (in system file) is world writable

A system process, for example *cron* or a file which is used when the machine is booted, starts a command which runs with `root` privileges. This command effects a directory with permissions that allow all users to write to it. If the process in some way retrieves the data or runs a command within the directory, this could cause a security threat.

Action

Check the lines in the file which have caused the warnings. In the *crontab*(1) file there are lines which purge the temporary directories. These lines do not pose a threat.

The syntax below enables to clear out old files in `/tmp`.

```
find /tmp -mtime +7 -exec rm -f }  ;
```

UNIX Reference Pages

cron(8)

crontab(1)

rc(8)

40. user <username>'s home directory <directory> is not a directory (mode 0nnn)

Reason

The user < >'s home directory <> is mode 0nnn.

Action

Change permissions for the directory in question. This is presumably an error.

UNIX Reference Pages

ls(1)

chmod(1)

login(1)

57. password file, <line number>, negative user id: from <file>

Reason

Usually only the user nobody (with UID -2) exists with a negative user ID. On some machines a negative user ID can be a security problem.

Action

Change the UID to a regular one for users other than `nobody`. Change the user ID of `nobody` to 32767-2.

59. password file, <line number>, <user> has id = 0 who is not root: remove from file

Reason

There is a user with user ID of `0`, with the exception of `root`.

Action

If the user is not a system administrator with the appropriate access restrictions, remove the user.

60. User user:filename is mode 0nnn

Reason

Files containing commands which are automatically executed when a user starts a shell (for example when the user logs in) can be written to by someone other than the user.

Action

Change the permissions on the relevant files.

UNIX Reference Pages

ls(1)

chmod(1)

70 . rexcd is enabled by /etc/inted.conf

Reason

The daemon *rexd*(8) is facilitates access from other machines with very little control.

Action

Comment out the line in */etc/inted.conf*(4) by placing a '#' at the beginning of the line beginning with *rexd*(8).

NOTE *On some machines rexd(8) is setup in a more secure manner. In this case it may not pose a threat to the system's security.*

UNIX Reference Pages

rexd(8)

inetd.conf(4)

72 . /usr/bin/uudecode is enabled in /usr/spool/aliases

Reason

The program *uudecode*(1) unpacks binary files which have been stored as text files. Binary files are typically stored in this manner so that they can be sent via electronic mail. *uudecode*(1) sets permissions on files as they are unpacked.

This message means that an email alias has been setup so that files can be created on other machines by email using *uudecode*(1).

Action

Comment out the line in */usr/spool/aliases*(4) by placing a '#' in front of the line which enables */usr/bin/uudecode*(1).

UNIX Reference Pages

sendmail(1)

uudecode(1)

74 . /usr/bin/uudecode creates setuid files

Reason

Please refer to the point above for warning number *72*. The version of *uudecode*(1) which is on this machine sets the setuid flag which means that if `root` unpacks a file this may result in the program having `root` executable privileges. This means that all files must be checked before users unpack files with *uudecode*(1). If the coded begins with four figure number (permissions mode) it is possible that this mode sets setuid permissions on the file when it is unpacked. For example :

```
begin 555 filename
```

Action

Remove the fourth number from the permissions mode before unpacking the file.

UNIX Reference Pages

uudecode(1)

chmod(1)

75 . tftpd is enabled on <machine>

Reason

This means that the daemon *tftpd*(8) is running and is able to retrieve files which are readable by all users on the machine. For example the */etc/passwd*(4) file can be retrieved in order to attempt to crack a machine's passwords. If there are no X-terminals or diskless machines which are to be started from this machine, there is probably no need for *tftpd*(8).

Action

Comment out the entry for *tftpd*(8) in the file *inetd.conf*(4). On certain machines *tftpd*(4) can be run with a certain amount of security.

UNIX Reference Pages

tftpd(8)

inetd.conf(4)

80 . <user> should be in /etc/ftpusers

Reason

A user with user ID of 0 permissions can log in via the program *ftp*(1). If you are using the BoKS version of *ftp* then access is controlled by the FTP access route.

Action

Add the user to the file */etc/ftpusers*(4) , so that no users with a user ID of 0 can use *ftp*.

UNIX Reference Pages

ftpd(8)

ftpusers(4)

81 . /etc/ftpusers should exist

Reason

Please refer to the explanation above for message number *80.*

Action

Please refer to the explanation above for message number *80.*

105 . <filename> could have a hole/bug (CA, year:no)

Reason

The specified program might contain a known problem, according to CERT (Computer Emergency Response Team). They provide a list of such problems "CERT Advisories" which are numbered with the year and the number. The warning points you to a CERT number.

Action

Obtain a new version of the program from the supplier.

120 . <filename> (or <directoryname>) is world (group) readable

Reason

The file or directory (or the parent directory) can be read by all users. You can elect to display this warning by altering the list of warnings in the *Warning Admin* sub menu on the *Integrity Check* menu.

Action

Change permissions on the files and directories, or modify the warning list in the *Warning Admin* sub menu.

UNIX Reference Pages

chmod(1)

16.9 BoKS Error Messages

!ERROR. No more shared memory. Run resetshm(1B) from the prompt!

Reason

BoKS uses shared memory to store indexes in the database. This is in order to facilitate quicker interrogation of the database. The message indicates that the shared memory is used up and needs to be reset.

Action

Reset the shared memory as follows. Enter the following at the system prompt:

```
boksadm -S
resetshm
```

WARNING

No one must log in or carry out an activity which uses the BoKS database whilst the shared memory is being reset. Resetting shared memory takes approximately 2 minutes.

!FATAL ERROR. No more shared memory and NOT resetable!

Reason

Shared memory has run out.

Action

Contact your BoKS support desk.

This page is intentionally left blank.

17

Reference Pages

17.1 Outlook

This chapter provides the essential man pages for the BoKS administration commands. This chapter has two functions:

- Helps system administrators familiarise themselves with the structure of BoKS commands.
- Enables system administrators to write customised system administration applications with BoKS commands.

Due to the fact that the BoKS administration functions are designed to be used through the BoKSADM menu system, there is very little need to use the commands outlined in this chapter in their raw state from the command line.

The main function of this chapter is to familiarise the system administrator with the commands that are called most frequently by the BoKSADM menu system. These are the commands you most frequently encounter when running BoKSADM in "debug" mode by entering **`boksadm -d`** at the command line.

The following commands are explained here:

- `bksdef`

This command enables you to set the system parameters. This is the command largely used by the menu choices in the *Parameter Configuration* menu. This command is responsible for setting such key features as authentication methods, length of password, period of inactivity, and so on.

- `boksadm`

  This command is the startup script for the BoKSADM menu system. Using this command also sets the environment required to run the BoKS administration commands.

- `des`

  This command is used to encrypt and decrypt files.

- `hostadm`

  This command is responsible for entering the host details into the BoKS database. This command is primarily called by the menu choices on the *Host Admin* menu and sets such key entries as default parent home directory, IP-address of the host, and so on.

- `lsbks`

  This command enables you to list the user setup and is used to list information about users stored in the BoKS database.

- `mkbks`

  This command enables you to create a user. The user details are stored in the BoKS database. This command is used by the *Create User* and *Get User Data* menu choices.

- `mkhome`

  This command is used to create a user's home directory, the various startup files which are added to the user's home directories including the *.boks_uenv* file.

- `modbks` This command is used to alter a user's setup. The user's name and access routes can not be altered with this command.

- `rmbks`

  This command is used to remove a user from the BoKS database. All BoKS information about the user is removed but the user's files and home directory are not.

- `ttyadmin`

  This command is used to set an access route. A user must have at least one access route specified to be able to access the system. This command is also used to remove an access route and to list access routes. The following *access methods* may be specified in a comma separated list:

TELNET	Access using the telnet protocol
RLOGIN	Login using the rlogin program
XDM	Login from a X-terminal
PCNFS	Disk access using PC NFS
RSH	Remote execution/copy using the rsh and rcp commands
REXEC	Remote execution using rexec
FTP	File transfer using ftp
LOGIN	Login through a standard tty
SU	Changing user id using the su command
*	All methods

In addition you must specify a location where an access method may be used from and where the access method enables access to.

- `xdladm`

  Command used by those running BoKS in an X-Windows environment. Enables you to alter the setup of the X-display locking facility for X-terminals and work stations.

17.2 Usage Examples

Below are simple examples of how the following access route is opened for all users on the machine `bigbox`. `RLOGIN,TELNET:colourbox->bigbox`

To set the correct environment to run BoKS programs, use the BoKS Shell as follows:

```
# boksadm -S
BoKS> for USER in 'lsbks | grep 'bigbox:''; do
> echo "Add access route to the $USER"
> ttyadmin -a -l $USER -zRLOGIN,TELNET:colourbox->bigbox
> done
BoKS>
```

In the same way other operations on multiple users be done in a simple way.

This page is intentionally left blank.

NAME

bksdef – manage system and default parameters

SYNOPSIS

bksdef -n *authentication method*

bksdef -n *auhtentication method* **-z** *access route*

bksdef -n *authentication method* **-z***access route* **-b** *start time* **-e** *end time* **-w** *weekday*

bksdef [**-vqup**]

bksdef -f *password format*

bksdef -d *days*

bksdef -r *tries*

bksdef -t *timeout*

bksdef -l *password length*

bksdef -H *password history*

bksdef -l *password frequency*

bksdef -C *days*

bksdef -E *user expire date*

bksdef -L *log language*

bksdef -O *log directory*

bksdef -S *log command*

bksdef -a *log ascii*

bksdef -D *options* [**-m**]

bksdef -s [gt12]

DESCRIPTION

Bksdef administers access route authentication methods and global BoKS data. *Bksdef* without arguments gives a list of global BoKS data and defined authentication methods for access routes. The option **-x** may always be used to set the debugging level. The debugging level may be set to a value in the interval 0 through 10.

OPTIONS

-n *authentication method*

authentication method can have the following values:

1	access route locked
2	system password
4	user password
6	system and user password
12	compatibility mode (e.g. use with uucp)
16	standard UNIX login (BoKS off)
36	Ask for one-time password
100	Must have one-time generator

If *access route* is given then *authentication method* is set for the given access route. If **-b** and **-e** are given it's assumed that time dependent authentication method should be set. If there are no access route given on the command line then system wide authentication method is set instead. When system authentication method is set to 1, the entire system is locked except for root at the console.

The actual authentication method is connected to a bit value, i.e, 1 = locked, 2 = system password.

-b *start time*

Specifies start time for time dependent authentication method. The format is *TT*[*MM*] or *TT*:[*MM*] where TT is hours (24 hour format) and MM is minutes.

-e *end time*

End time. See **-b** for a format description.

-w *weekday*
Day of week for time dependent authentication method. The format is a string with digits (1-7) without any space. 1 is Monday and 7 is Sunday. Example: -w12356 means Monday, Tuesday, Wednesday, Friday and Saturday. The default for week day is Monday to Friday (-w12345).

-z *access route*
The access route in the format *access method***:***from***->***too.*

-v Sets verbose login mode. Verbose login mode will make *login*(1B) verbose about why a user was denied login.

-q Quiet login mode. The opposite of **-v.** *login*(1B) will only say: "Login incorrect" whatever the problem was. This is the recommended setting for a secure system.

-u Activate updating of passwords in */etc/passwd.*

-p De-activate updating of passwords in */etc/passwd.* This will make BoKS to write '*no login*' in the password field in */etc/passwd* upon the next updating of passwords for a user by *passwd*(1MB).

-R Remove access route from the access route authentication method table.

-f *password format*
The *password format* is one of the following numbers:

0	no format restrictions
1	at least one letter and one digit
2	at least two letters and two digits
3	randomly chosen password
4	model password (part of password randomly chosen)

-d *days* Valid time for password is set to *days.*

-r *tries* System default number of login tries.

-t *timeout*
System default time out (inactivity time).

-l *password length*
System wide minimum length of password is set to *password length.*

-H *password history*
System wide length of password history is set to *password history* . A user may not use a password that is in the password history. Valid values are 0 to 20.

-F *password frequency*
System wide minimum time between password changes is set to *password frequency* .

-E *user expire date*
System wide exire date for newly created users is set to *user expire date* . Date should follow the format [YYMMDD].

-C *days*
If a users password has expired, and it's less than *days* days since expiration, *login*(1B) will call *chpwd*(1BM) to force password change.

-L *language*
Language to use when logs are written to the console.

-O *log directory*
Location of user log and system log. The logs are called *BoKS.LOG* and *BoKS.SYSLOG* and are placed in the specified log directory.

-S *log command*
Log messages beginning with '!' are piped to *log command*. Default is **cat > /dev/console**. If an empty log command is specified, log messages beginning with '!' will not be treated differently from other log messages.

-a *ascii* ASCII used in console logs and logs redirected with the **-S** option.

-D *options*
This option is used to display the value of other options. *option* can be one or more of the characters **fdrtlCOSLaqvupnsEHF**. The valued will be displayed one per line in the order specified in *options*.

-m Use with the **-D** option to display a descriptive message for each value.

-s g Print only global BoKS data

-s t Print only defined authentication methods

-s 1 Print a list of those access routes which have a time independent authentication method.

-s 2 Print a list of those access routes which have a time dependent authentication method.

-x *debug level*
Show debug info on execution. *Debug level* can be in the interval 0 (no debug info) to 10 (loads of debug info).

SEE ALSO

login(1B), mkbks(1B), passwd(1B), ENV(4B)

NAME

boksadm – startup script for BoKS Security Administration

SYNOPSIS

boksadm [**-v**]
boksadm -S [*commands*]

DESCRIPTION

Boksadm starts *BoKS Security Administration.* The script *boksadm* is created at installation by *Install*(1B), and is ususally placed in the directory */usr/bin* (the directory may be changed by using *Setup*(1B) before executing *Install*(1B).

Boksadm sets the environment used by BoKS administration programs and the Menuett menu handler. *Boksadm* then calls *menuett*(1).

Environment variables set by *boksadm* include:

APPLPATH	- BoKS home directory
MLANG	- language variable for BoKS and Menuett
PATH	

OPTIONS

-v Print licence information for the current *BoKS* licence. This includes release information, license number, and number of licenced users and hosts. Do not start *menuett.*

-S *commands*

With no commands, starts an interactive shell in BoKS environment, otherwise execute *commands* in a BoKS environment.

Other options

boksadm passes on all other options and arguments to *menuett.*

X-WINDOWS ENVIRONMENT

Boksadm starts an X-version of *menuett* that supports mouse-usage if the following two conditions are met:

1. The DISPLAY environment variable is set
2. An executable *xterm* is found (change $PATH if nessesary)

FILES

/usr/bin/boksadm - installed version of boksadm

SEE ALSO

Install(1), Setup(1), menuett(1)

NAME

des - DES file encryption

SYNOPSIS

des -el-d [-h] [-k key] [-b]

DESCRIPTION

des is a filter that encrypts or decrypts standard input to standard output with the Data Encryption Standard (DES). Either -e (encrypt) or -d (decrypt) must be specified. If the key is not given on the command line with the -k option the command will prompt for it twice, suppressing echo and comparing the two responses to guard against mistyping.

The -h flag controls how the key string is to be interpreted. Without the -h flag, the key is an ASCII string. Since DES ignores the low order bit of each key byte, the high order bit is set for odd parity, thus retaining the information contained in the low order bit. If the -h flag is set, the key string is interpreted as 16 hex/ASCII characters; the low order bit of each byte is again ignored as per the DES algorithm. This allows the use of any arbitrary 56-bit key, including bytes representing control characters that could not be typed if the -h option were not used.

By default, DES Cipher Block Chaining (CBC) mode is used, with an initial vector (IV) of all zeros; if the -b option is specified, Electronic Code Book (ECB) mode is used instead.

Except for the -h option, this command is compatible with the **des** command on the Sun Microsystems workstation.

SEE ALSO

Sun Microsystems DES(1) manual page, which describes in detail how the length of the file is encoded in the last block of ciphertext.

AUTHOR

Phil Karn, KA9Q

NAME

hostadm – Maintain BoKS host database table

SYNOPSIS

hostadm –a –h *name* **–i** *adress* [**–c** *comment*] [**–p** *homedir*] [**–f** *filehost:path*] [**–t** *type*] [**-x** *degug level*]
hostadm –d {**–h** *name* | **–i** *address*} [**-x** *degug level*]
hostadm –l [**–H** | **–F** | **–L** | **–T** | **–N**] [**–h** *name*] [**-x** *degug level*]
hostadm -k –h *name* [-x *degug level*]
hostadm { **-A** | **-D** } *flag* **–h** *name* [**-x** *degug level*]
hostadm -m –h *name* **–p** *homedir* [**-x** *degug level*]

DESCRIPTION

All hosts that should be used in a BoKS network environment must be present in the BoKS database. Hosts not present in the host database will be denied access to the *boks_servc*(1B) daemon. *Hostadm* maintains the BoKS host database (the database table HOST). Options exist to add/modify, delete, list and check host data. See also the *lh*(1B) manual page.

OPTIONS

-h *name*
Specifies the name of the host to be added or removed. Note that it is possible to have several hosts with the same name, but different IP-addresses in the database. Beware that this is not fully supported.

-c *comment*
When adding a new host to the database an optional comment may be entered using this option.

-i *address*
Specifies the internet (IP) address of the host to be added or removed. The address must be unique.

-p *homedir*
Specifies the name of the directory where the users homedirectories are located (homeprefix). If *homedir* is an empty string, the homeprefix will be removed.

-f *filehost:path*
Specifies the hostname and path to the directory on the fileserver where the homedirectory prefix for host is mounted. If *filehost:path* is an empty string, this attribute will be removed.

-t *type* Specifies the type of the host. Valid types are

UNIXBOKSHOST	Unix host with BoKS installed
PCBOKSHOST	PC host with PC-BoKS installed
NONBOKSHOST	Host with no BoKS installed

Default is **UNIXBOKSHOST.**

-A|D *flag*
Specifies if *flag* should be enabled (-A) or disabled (-D). Valid *flags* are

login	Root may login on this host
pswupdate	The password file should be updated on this host

-a Add/modify the entry for the host whose name is specified by the **-h** option and whose address is specified by the **-i** option to the BoKS-NonStop host database. If the host already exists in the database, the existing entry will be modified. If the **-p** and/or **-f** options are present, their arguments will be used to define homedirectory and physical homedirectory respectively.

-d Remove the host indicated by either the **-i** option or the **-h** option from the BoKS host database.

-l List contents of the host database to standard output. For each host the name, the address, the optional comment, homedirectory and physical homedirectory (i.e. directory on fileserver) will be printed.

-k Check that the *homedirectory-prefix* attribute exists for all hosts in the hostgroup named with the **-h** option. Exit status will be 1 if the homeprefix is missing for any of the hosts in the hostgroup.

-H With option **-l** print only the homedirectory prefix, if present.

-F With option **-l** only. Print the homedirectory prefix and physical homedirectory (on fileserver), if present.

-L With option **-l** only. Print the flag value.

-T With option **-l** only. Print the type value.

-N With option **-l** only. Print the number of currently logged in users for the host(s).

-x *debug level*
Show debug info on execution. *Debug level* can be in the interval 0 (no debug info) to 10 (loads of debug info).

SEE ALSO

lh(1B), hgrpadm(1B), boks_servc(1B), boks_master(1B)

NAME

lsbks – list user data

SYNOPSIS

lsbks [**-SHvsaTUMx**] [**-l** *user*] [**-t** *tty*] [**-V** *criteria*] [**-D** *options*]
lsbks -n [**-l** *user*] [**-V** *criteria*]
lsbks -p [**-l** *user*] [**-V** *criteria*]
lsbks -P [**-l** *user*] [**-V** *criteria*]
lsbks -u
lsbks -q -l *user*
lsbks -q -I *user id*

DESCRIPTION

Lsbks with options lists specific user data.

Lsbks without options lists all users in the BoKS domain.

OPTIONS

-H Write a header.

-v Verbose listing. The following columns with information are listed:

1: User name
2: Complete user name (comment field)
3: User id
4: Group id or group name
5: Password last valid date. If the user doesn't have
a password it's noted here (he's blocked).
6: User last valid date
7: Number of failed login tries
8: Inactivity time in minutes

-s Gives a list with last login/logout with terminal line.

-S Sorts output by user name.

-U Used with **-S** to ignore the hostname field in user names when sorting.

-l *user* By giving a user name output can be limited to only include information concerning *user.* The wildcards '*' and '?', as in *sh(1),* can be used to select a group of users. E.g., **-l '*:a*'** to list all users that begins with an 'a'.

-I *user id*
Used with **-q** to verify a user id.

-t *tty* When used together with **-s** lists info only for terminals matching *tty.* Analogous to **-l** for users.

-n Print serial number(s).

-p Print a user information in */etc/passwd* format. If no user is specified, *lsbks* prints user information about those users whose host prefix matches the host name of the host *lsbks* is running on.

-P Print user information in format easely used by Menuett. There is no guarantee that the behavior of this option will not change in future releases.

-a Print all known information about the indicated users in a very verbose format.

-T Used with **-a** to print all assigned terminals for each user.

-u Print the next available unique user id greater than 100. This corresponds to the value that *mkbks*(1B) will use when a new user is created unless an explicit user id is stated.

-m Print the mapping of hostgroupname:username to all hostname:usemame. E.g., if the host group *SALES* consists of the two hosts *sale1* and *sale2* the user created as *SALES:bill* is mapped to *sale1:bill* and *sale2:bill.* The mapping is for internal use only.

-D *options*

Show only selected information about each user. *Options* consists of a string of characters indicating what pieces of user data to display. All data will be printed one item per line without any headers or explaining texts.
Options consists of one or more of the following characters:

Character	*Displays*
l	Username
g	Numeric group ID
u	Numeric user ID
r	User's real name (comment)
h	Home directory
s	Shell
o	Timeout value
O	Time dependent timeout value
b	Start time for time dependent timeout
e	End time for time dependent timeout
w	Weekdays for time dependent timeout
p	Encrypted password
d	Password lifespan in days
E	Last date user is valid
T	Possible to SU to this user? Yields "yes" or "no" (for backward comp. only)
S	User may use SU? Yields "yes" or "no" (for backward comp. only)
X	Timeout depending on CPU time used (yes/no)
Y	Timeout depending on input from tty (yes/no)
Z	Timeout depending on screen updates (yes/no)
G	User must have a password generator to access the BoKS domain
(yes/no)	

-V *criteria*

Only list the users whose user data matches all of the criterias given in *criteria*. *Criteria* consists of one or more of the following characters:

Character	*Select users that...*
B	..are temporarily blocked.
P	..have invalid passwords.
0	..have user ID equal to zero.
F	..are blocked due to too many failed logins.
x	..have expired passwords.
X	..have expired.
L	..are denied to login.
T	..can't be SU:ed to.
S	..are denied to use SU.
Z	..have a valid zero length password.
g	..have expired passwords and grace period
O	..have time dependant timeout

Multiple **-V** options can be given to achieve an "or" effect. For example to list all users that are either temporarily blocked or have expired, specify **-VB -VX**.

valid passwords specify **-VP!** .

-q Used to verify the existance of *user* or a *user id*. If the user or user ID doesn't exist **lsbks** exits with a non zero status. No wildcards are allowed.

-M Show headers only.

-x *debug level*
Show debug info on execution. *Debug level* can be in the interval 0 (no debug info) to 10 (loads of debug info).

NOTE

An encrypted password with more than 0 but less than 13 characters is considered to be **invalid.**

SEE ALSO

mkbks(1B), modbks(1B), ttyadmin(1B)

NAME

mkbks – create user with BoKS

SYNOPSIS

mkbks [**-i**] **-l** *user* **-g** *gid* **-h** *home directory* [**-u** *uid*] [**-r** *name*] [**-s** *shell*] [**-o** *time limit*] [**-E** *date*] [**-p** *encrypted password*] [**-d** *date*] [**-x** *debug level*]

DESCRIPTION

Mkbks creates a user under BoKS. *Mkbks* updates */etc/passwd* and the BoKS database. */etc/passwd* is not directly used by BoKS, it is updated only to retain compatibility.

If a user is created without **-p** the user is blocked. To enable the user, he must be given a password.

If password updating is off (see *bksdef*(1B)) the password is always set to '*no login*' in */etc/passwd* instead of the real encrypted password.

A host prefix should be specified in front of the user name. The prefix specifies on which hosts the user is 'visible'. The host prefix can be a true host or a host group defined in the host group database. The predefined host groups **ALL** makes a user 'visible' on all hosts which have BoKS installed.

OPTIONS

-i Don't update */etc/passwd.*

-l *user* Specifies user name.

-g *gid* Group id. can be specified as a symbolic group from */etc/group* or as a number.

-u *uid* User id. Default is that *mkbks* creates the user with an unique user id.

-r *name*
The users full name (comment field). Default is empty

-h *home directory*
Users home directory. May be entered as a relative path. The users home directory is then built by merging the home prefix defined for the host in question and the relative path. E.g., if the user *sale1:bill* is created with the relative path *bill* and the home prefix for the host *sale1* is */home* the the Bill's homedir will be */home/bill.*

-s *shell* User login shell. Default is empty (which will be defaulted to */bin/sh* at login).

-o *time limit*
Timeout value (maximum in activity time in minutes). Default is definable with *bksdef*(1B).

-E *date* Users last login date. The default is definable with *bksdef*(1B).

-p *encrypted password*
An encrypted password can be given. This not used under normal BoKS administration. Passwords should be given with *passwd*(1B).

-d *date* Date when password expires. The default is definable with *bksdef*(1B).

-x *debug level*
Show debug info on execution. *Debug level* can be in the interval 0 (no debug info) to 10 (loads of debug info).

FILES

/etc/passwd

SEE ALSO

passwd(1B), modbks(1B), rmbks(1B), bksdef(1B), bksd(1B), createbks(1B)

NAME

mkhome – create users home directory

SYNOPSIS

mkhome -l *user* [**-u** *uid*] [**-g** *gid*] [**-d** *directory*] [**-U** *umask*] [**-P** *path*] [**-S** *start program*] [**-E** *env=val*] [**-h** *host*] [**-p**] [**-v**]

mkhome -d *directory* [**-u** *uid*] [**-g** *gid*] [**-U** *umask*] [**-P** *path*] [**-S** *start program*] [**-E** *env=val*] [**-p**] [**-v**]

DESCRIPTION

Mkhome creates a users home directory and creates the file *.boks_uenv* and various shell profiles in the users home directory.

User or directory must be specified.

OPTIONS

-l *user* Take the information needed about the home directory to create from the BoKS database. The information taken from the database is *uid*, *gid* and *home directory.*

The home directory is created on the host (or an all hosts belonging to hostgroup) specified by *user* as the user is specified as *host(group):username.*

A configurable number of user login profiles (e.g., *.profile* , *.login)* may be copied to the users home directory as defined by the files *$BOKSDIR/etc/defprofiles* and *$BOKSDIR/etc/host2profile.*

-g *gid* Group ID. Must be specified as a number.

-u *uid* User ID as a number.

-d *directory*
An absolute or relative pathname specifying the directory to create.

If the directory is specified as relative pathname, and the home prefix (parent homedir) for the host(s) in question, then the home prefix will be prepended to the directory name to form the full home directory path. The home directory prefix is defined by using *hostadm (1B).*

-P *path* Path to be appended to the standard path at login.

-U *umask*
Umask to be set at login.

-S *startprog*
Startprogram to be run after login.

-E *env=var*
Set environment variable *env* to *var* at login.

-v Display human readable information about the users login *path*, *umask* and *start program.*

-p Print information about *umask*, *path* and *start program* on three separate lines in this order.

-x *debug level*
Show debug info on execution. *Debug level* can be in the interval 0 (no debug info) to 10 (loads of debug info).

NOTES

The option **-l** have lower precedence than the options **-u**, **-g** and **-d**.

FILES

$HOME/.boks_uenv
$HOME/.profile
$HOME/.login
$BOKSDIR/etc/host2profiles
$BOKSDIR/etc/defprofiles

SEE ALSO

mkbks(1B), hostadm(1B), Chapter 15 in BoKS Adminstration Manual

NAME

modbks – modify a BoKS user

SYNOPSIS

modbks **-l** *user* [**-u** *uid*] [**-g** *gid*] [**-r** *name*] [**-h** *home directory*] [**-s** *shell*] [**-E** *date*] [**-d** *days*] [**-o** *timeout*] [**-O** *timeout*] [**-b** *start time*] [**-e** *end time*] [**-w** *weekdays*] [**-A** *allow*] [**-D** *deny*] [**-L** *days*] [**-C** *concurrent logins*] [**-n** *serial*] [**-x** *debug level*] [**-N**] [**-t**] [**-B**] [**-U**] [**-H**] [**-S**]

DESCRIPTION

BoKS users can be modified with *modbks*. The user name cannot be modified.

OPTIONS

-l *user* Specifies user name.

-g *gid* Group id. can be specified as a symbolic group from */etc/group* or as a number.

-u *uid* User id.

-r *name*
The users full name (comment field).

-h *home directory*
Users home directory.

-s *shell* User login shell.

-o *time limit*
Timeout value (maximum inactivity time in minutes).

-E *date* User's last login date.

-d *days* Number of days password is valid after change.

-O *timeout*
Used together with options **-b**, **-e**, and **-w** to specify a time dependent timeout.

-b *start time*
Specifies a starting time for time dependent timeout.

-e *end time*
Specifies a ending time for time dependent timeout.

-w *weekdays*
Specifies which weekdays the time dependent timeout will be used.

-A *allow*
allow is a comma separated list of attributes to allow for the user. The attributes are *login*, *suto*, *sufrom*.

-D *deny*
deny is a comma separated list of attributes to deny. The attributes are *login*, *suto*, *sufrom*. When a new user is created with a non zero uid, all attributes are allowed. When a super user is created, the attribute *login* is denied, allowing only console logins.

-n *serial number*
Serial number of smart card or one-time password generator.

-L *days* Set password last change date back *days* days.

-C *concurrent logins*
Number of allowed logins with the same name. Default is no restriction but the licenced number of logged in users.

-n *serial number*
Serial number of smart card or one-time password generator.

-N Clear serial number.

-t Authorize new login tries for the user.

-B Block user. Both login and su prohibited.

-U Unblock user.

-H Set the one-time user password option (hard spin).

-S Unset the one-time user password option (soft spin).

-x *debug level*
Show debug info on execution. *Debug level* can be in the interval 0 (no debug info) to 10 (loads of debug info).

FILES

/etc/passwd
data/bks

SEE ALSO

mkbks(1B), rmbks(1B), bksdef(1B), bksd(1B)

NAME

rmbks – remove a BoKS-NonStop user

SYNOPSIS

rmbks [**-k**] *users*

DESCRIPTION

Rmbks removes one or more users from the BoKS database. All information concerning login/logout dates, blocked menus and login terminals will be removed. Log entries will not be removed.

The users home directory and private files are not affected.

OPTIONS

-k Keep password file entries. If this option is given users will not be removed from the password file(s).

-x *debug level*
Show debug info on execution. *Debug level* can be in the interval 0 (no debug info) to 10 (loads of debug info).

SEE ALSO

mkbks(1B), modbks(1B), bksdef(1B)

NAME

ttyadmin – administration of user access routes

SYNOPSIS

ttyadmin -a|**-r -l** *user* **-z** *AccessMethods:FromHost->ToHost* [**-b** *start time*] [**-e** *end time*] [**-w** *days of week*] [**-x** *debug level*]

ttyadmin -y[v] **-z** *AccessMethods:FromHost->ToHost* [**-x** *debug level*]

ttyadmin -P [**-l** *user*] [**-x** *debug level*]

ttyadmin -s [**-l** *user*] [**-x** *debug level*]

ttyadmin -T [**-l** *user*] [**-x** *debug level*]

ttyadmin -N [**-l** *user*] [**-x** *debug level*]

ttyadmin -A [**-x** *debug level*]

DESCRIPTION

Ttyadmin administers access routes for BoKS users. A BoKS user must have an *access route* allocated by *ttyadmin* to be able to access the system through BoKS.

A user may be authorized to access the system from any number of access routes. A user may also have several authorizations per route. At access time all the entries are scanned for a possible match.

OPTIONS

-r Revoke authorization.

-s List authorizations. This is the default if neither **-r** or **-a** is present.

-a Authorize a user to access the system using the specified *access route.* The user must previously have been created by *mkbks*(1B).

-T List *access routes* through which a user is authorized to access the system. If no *access route* is specified, all routes which at least one user is authorized to access are shown.

-N The negation of **-T.**

-A Show all known terminals. This is done by scanning the /dev directory for possible terminals.

-l *user* Specify user.

-z *AccessMethods:FromHost->ToHost*

This option is used to specify a full *access route* with one option. The following *access methods* may be specified:

TELNET	Access using the telnet protocol
RLOGIN	Login using the rlogin program
XDM	Login from a X-terminal
PCNFS	Disk access using PC NFS
RSH	Remote execution/copy using the rsh and rcp commands
REXEC	Remote execution using rexec
FTP	File transfer using ftp
LOGIN	Login through a standard tty
SU	Changing user id using the su command
*	All methods

Methods may be entered either upper or lower case letters. The wildcard '*' may be used.

If the *access method* is **SU** or **LOGIN** the *FromHost* part should be a valid terminal name instead of a host. If the access method is **SU** *ToHost* should be the name of the user (only username).

-b *start time*
: Specifies the start time, since midnight, for access through the specified route. The format is *TT*[*MM*] or *TT*:[*MM*] where TT is hours (24 hour clock) and MM is minutes.

-e *end time*
: End time. See **-b** for a format description.

-w *days of week*
: Day of week for access through the specified route. The format is a string with digits (1-7) without any spaces. 1 is Monday and 7 is Sunday. Example: -w12356 means Monday, Tuesday, Wednesday, Friday and Saturday. The default for *days of week* is Monday through Friday (-w12345).

-P Print access route/user information in format easely used by Menuett. There is no guarantee that the behavior of this option will not change in future releases.

-y Used to check if a access route entered together with the -z option is valid. Use -v option for verbose mode.

-x *debug level*
: Show debug info on execution. *Debug level* can be in the interval 0 (no debug info) to 10 (loads of debug info).

EXAMPLES

To enable user **host1:bill** to login through terminal **tty34** between **8am** and **5pm** from Monday through Wednesday:

```
ttyadmin -a -l host1:bill -z LOGIN:tty34->host1 -b 0800 -e 1700 -w 123
```

ttyadmin supports multiple access route entries. So if user **host1:bill** only work in the afternoon on Thursdays and Fridays the following should also be entered:

```
ttyadmin -a -l host1:bill -z LOGIN:tty34->host1  -b 1300 -e 1700 -w 45
```

To revoke user **host1:bill**'s authorization on terminal **tty34:**

```
ttyadmin -r -l host1:bill -z LOGIN:tty34->host1
```

The following authorizes the user **balder:tom** to always access the host **balder** from the host **foo** through the ftp server:

```
ttyadmin -a -l balder:tom -z FTP:foo->balder -w 1234567
```

SEE ALSO

mkbks(1B), login(1B)

NAME

xdladm – administration of the X Display Locking facility

SYNOPSIS

xdladm [-h *host*][-H|-d]
xdladm [-u|-r *display*]
xdladm [-h *host*] [-X *on|off*][-z *seconds*]
xdladm [-h *host*] [-s|-S|-v]
xdladm [-h *host*] -m *parameter:value ...*

DESCRIPTION

xdladm can be used to unlock or reset locked displays, and to view or modify parameters concerning automatic X locking. With no options, *xdladm* shows a list of locked displays.

OPTIONS

–r|-u *display*
Reset or unlock a display.

-h *host* Specify which host or host group to operate on. Doesn't apply to unlocking or resetting displays. Default is **ALL .**

–X *on|off*
Turn the X-locking daemon on or off. You may specify the words "on" and "off" as their equivalents in the current language. Only one at a time, though.

–z *seconds*
Specify sleep interval for the daemon.

–s Show some values. The ones that may be set from inside *boksadm.*

–S Show more values — all of them, in fact.

–v Be verbose about it.

–H Show a header when listing locked displays. Used together with -v to show locked displays.

–d List only the display names when listing locked displays.

–m *parameter:value ...*
Modify some values. Anything after the **–m** is interpreted as *parameter:value* pairs. There must be no whitespace in any of the fields. Any parameters may be added or modified. Parameters shown in italic are settable from with in *boksadm* and are the ones shown with *xdladm -s*

Timeout, Warntime, BeepInterval, FastBeep, Volume, Transparent, Log, Retries, Wait, Font, Ascii, xrdbPath, Sensitive, Access, IgnoreMotion

For each parameter, there is a corresponding "Override" parameter, that, if set to "yes," prohibits users to customise the parameter. E.g. the override parameter for *Timeout* is *TimeoutOverride.* In some cases the user setting for a parameter is ignored anyway.

WARNINGS

It is recommended that this script is only used from the X screen lock administration functions in *boksadm (1B).*

FILES

$BOKS_DIR/etc/Xdefaults

SEE ALSO

xdl(1B), boksadm(1B)

This page is intentionally left blank.

I

Index