Appendix A

Extended Boot Protection

- For Safety
- Running the Extended Boot Protection (EBP) Programs
- Passwords
- Installing EBP
- Boot Dialogue
- Re-configuring EBP
- De-installing EBP
- Protect Options

FOR SAFETY

DO NOT INSTALL EXTENDED BOOT PROTECTION

- if you use remote booting across a network
- if you use non-IDE removable hard disks
- if you have a non-DOS/Windows 95 operating system
- if your hard disk is controlled by a device driver which makes calls directly to the hardware rather than addressing it through the BIOS. Examples include OnTrack's 32-bit FASTDISK driver and Adaptec's ASPI4DOS.SYS. You can still use Adaptec's driver however if you specify the 'I' option (this re-enables BIOS and hence EBP compatibility).
- if you have not already installed Stoplock

BEFORE RUNNING ANY OF THE PROGRAMS

- check the Product Release Documentation
- disable any anti-virus monitor (Memory resident & BIOS)
- boot from a floppy disk

RUN FROM PRODUCT DISK 1, NOT A COPY

- for re-configuration or de-installation, use the same disks you used for installing EBP

BEFORE INSTALLING OR DE-INSTALLING

- back up the hard disk
- be aware how long encryption/decryption may take
- use a mains adapter rather than battery power

DO NOT INTERRUPT ENCRYPTION OR DECRYPTION !

Introduction

This chapter tells you how to install Extended Boot Protection (EBP), re-configuration and de-installation of EBP.

EBP encrypts all or part of the hard disk. When the PC is booted from a floppy, the presence of Extended Boot Protection ensures that the hard disk is not accessible.

EBP checks that Stoplock is loaded in a proper fashion. At boot time, EBP is initialized and starts a timer. If the time expires before the Stoplock kernel has been loaded, a message is displayed (**Kernel VxD not found**). The PC is then automatically shut down.

The EBP resident code takes up approximately 3K of system memory.

If full disk encryption is selected, users may notice a slight degradation in performance since there is some overhead involved in decryption or encryption each time a disk sector is read or written.

DO NOT INSTALL EXTENDED BOOT PROTECTION BEFORE READING THE SAFETY REQUIREMENTS ON THE PREVIOUS PAGE.

Do not boot the PC in Safe Mode once EBP has been installed - remove EBP before you activate Windows 95 Safe Mode. Safe Mode does not load any device drivers, including the Stoplock device driver, causing a ‘Kernel VxD not found’ error to occur and the PC to be shut down.

EBP may also be installed via a full or partial ‘hands-free’ installation procedure. See the ‘Protect Options’ section at the end of this chapter for details on achieving this.

Running the EBP Programs

Do the following before running any of the EBP programs:

- Disable any anti-virus monitor that may be present in memory or BIOS, as this could prevent any of the programs from running successfully. You can enable any such monitor again as soon as you have completed installation, de-installation, or re-configuration.
- Boot from a DOS/Windows 95 system floppy disk that does not contain a CONFIG.SYS or AUTOEXEC.BAT file.
- If you used foreign keyboard settings during the installation of Stoplock then make sure the appropriate keyboard drivers are loaded before running either UNPROT or EBPCONF.
- Back up your hard disk: if anything happens to interrupt the installation or removal of EBP, you will be left with an unusable system.
- Make sure the PC is plugged into the mains when you install/ de-install EBP. Do not rely on battery power as full encryption or decryption may take several hours.
- When you de-install EBP, make sure that you use the same product disk that was used to install it.

You can cancel out of any of the EBP programs by means of the **D** key, **but do not do this during encryption or decryption**.

Passwords

Two passwords are used during installation and removal of EBP:

- **EBP program password**
  This is chosen at installation time, and it never changes. You have to supply this password before you can re-configure or remove Extended Boot Protection. Knowledge of this password should be restricted to you, as administrator, plus whoever will deputize in your absence.

- **Boot password**
  This is optional and can be chosen at installation time or subsequently. If a boot password is enabled, any user who boots the PC needs to know this password. This is different from the user's personal password, which he/she enters when logging on.

  The boot password must be different from the EBP program password - you will be asked to enter a new boot password if it is the same as the program password.

You will be asked to repeat both passwords in order to verify them.

Installing EBP

Use the PROTECT program to install EBP. Command line options for the PROTECT program can be used to bypass some or all of the installation screens - see ‘Protect Options’ later in this chapter.

Boot off a DOS system disk that does not contain a CONFIG.SYS or AUTOEXEC.BAT file - the following instructions assume that the floppy drive is **A:**

Replace the boot disk with Stoplock disk 1. At the A:\ prompt type:

protect

and press Q .

The **Introduction** screen is displayed. To continue with installation, type *Y* and press Q . The **Program Password Explanation** screen is displayed.

Program Password Entry Screen

Type a password of up to 16 characters in length and press Q .

The program password is used to form an encryption key for the disk and you will need to supply it again in order to re-configure or remove Extended Boot Protection.

Boot Password Choice Screen

This asks you to choose whether you want to implement a boot password. If you select this option, then every time you reboot the PC you will be asked to enter this password.

You can implement a boot password retrospectively, so you are not making a permanent choice at this point.

To implement a boot password, type *Y* and press Q. The **Boot Password Explanation** screen is then displayed.

If you type *N*, and press Q, no boot password is implemented and the **Select Encryption** screen is displayed instead.

Boot Password Entry Screen

This screen requires you to enter a boot password. So long as a boot password is enabled, the password must be supplied correctly when booting from the hard disk: otherwise, start-up does not take place.

Type a password of up to 16 characters in length and press Q. The **Select Encryption** screen is displayed.

Select Encryption Screen

Here you choose the amount of encryption to be performed.

You should make your choice by using the ↑↓ keys to position the selection bar and pressing Q.

- **Whole physical disk**
  This offers the greatest protection as the whole of the disk is encrypted. The only drawback is the length of time taken by encryption and decryption as this is directly proportional to the size of the disk. All sectors of the disk are encrypted regardless of whether or not they contain data. It takes approximately a maximum of 1 minute to encrypt 10MB.
- **System area of the hard drive**
  This encrypts the first few sectors: the File Allocation Table and Directory (Folder) Listing. Encryption and decryption take a matter of seconds or minutes.

Whichever is chosen, the **Timeout Value** Screen is displayed.

Timeout Value Screen

This screen asks you to specify the timeout value: *Seconds to wait for Stoplock to load*.

WARNING!
THE ENCRYPTION PROCESS BEGINS AS SOON AS YOU PRESS ENTER!
This is the final configuration screen. Encryption will begin as soon as you press **Q** in response to this screen, and this could take several hours. This is your final opportunity to terminate the program by using the **D** key.

Timeout Value

This feature is built in, not optional, but what you can choose is the time interval, which can be any value up to 999 seconds (which is a little over 15 minutes).

When the timeout occurs the following message is displayed:

Kernel VxD not found

and the PC will automatically shut-down.

If you choose an unnecessarily high value there is always the risk (albeit a small one) of a security breach before shut-down occurs. If you choose too low a value then shut-down will occur during a normal start-up, preventing legitimate users from working. You should time start-up and set the timeout value accordingly. The default is 120 seconds, which is a good starting point.

Press **Q** to initiate encryption.

Encryption

This process may take several minutes or hours depending on whether you chose system area or full disk encryption.

⚠

WARNING!
DO NOT INTERRUPT THE ENCRYPTION PROCESS!
You risk losing your data if you interrupt encryption.

While encryption is in progress a message remains on screen warning you that the program is protecting the disk and that the process should not be interrupted. A thermometer bar is displayed to inform you of progress.

Once encryption is complete the message changes to ‘Protection complete. Press any key to reboot your PC’. You should remove the product disk and press any key: the PC automatically reboots.

EXTENDED BOOT PROTECTION IS NOW INSTALLED.

Boot Dialogue

The information in this section only applies when the PC is booted from the hard disk. When booted from a floppy, the presence of Extended Boot Protection ensures that the hard disk is not accessible.

During start-up, Extended Boot Protection signifies its presence by two messages which appear on the command line in the usual way:

Stoplock EBP bootstrap V*n.n*
Loading Stoplock EBP V*n.n*

If the option has been taken to use a boot password then these messages are immediately followed by a request for the boot password. This takes the form of a red and white box in the center of the screen entitled ‘Initializing Encryption Key’ and containing a single field in which the user should type the boot password, pressing **Q** afterwards.

If the password is accepted, the box disappears immediately and normal start-up continues with logon to Stoplock.

If the password is incorrect, the field in the box is replaced by the message:

Incorrect Boot Password

This disappears after a few seconds and password entry is invited once again. There is no limit on the number of attempts allowed.

Re-configuring EBP

You can re-configure EBP by running the EBPCONF program. This allows you to change certain configuration options that were chosen during installation – the timeout value, whether a boot password is required, and the boot password itself.

Boot off a DOS system disk, then insert Stoplock disk 1 in **A:** At the A:\ prompt type:

EBPCONF

Press Q : the **Program Password Entry** screen is displayed.

Program Password Entry Screen

This screen requires you to enter the password that was chosen at installation time.

Type the program password and press Q . You will be asked to repeat this password to verify it. Providing the passwords match and are correct, the **Re-configuration** screen is displayed.

Re-configuration Screen

This screen tells you what options are currently in effect. Typically, it might say:

Timeout is currently 120 seconds
Boot password dialogue is currently Disabled

A selection box allows you to control these options. These might appear as:

Set timeout
Enable boot password
Save changes and Exit

In order to change the timeout value, use the ↑↓ keys to position the selection bar over *Set timeout* and press Q . The **Timeout Value** screen is displayed and here you can alter the timeout value.

In order to implement a boot password if it is shown as Disabled, use the ↑↓ keys to position the selection bar over *Enable boot password* and press Q . You will be asked to enter this password on saving and exiting.

In order to suspend the boot password if it is shown as Enabled, use the ↑↓ keys to position the selection bar over *Disable boot password* and press Q .

If a boot password is already implemented and you just want to change the password itself, use the ↑↓ keys to position the selection bar over *Save changes and Exit* and press Q . The **Boot Password Explanation** screen is displayed.

When you are happy that you have made the correct choices, use the ↑↓ keys to position the selection bar over *Save changes and Exit* and press Q . What happens next depends on whether a boot password is shown as Enabled. If it is, the **Boot Password Explanation** screen is displayed and then the **Boot Password Entry** screen.

You are required to enter a boot password, which may be the same as or different from the existing one. On entering and repeating the password correctly, the EBPCONF program terminates.

If the boot password was shown as Disabled, the program terminates. Remove the product disk and reboot the PC in order for the changed options to come into effect.

De-installing EBP

Use the UNPROT program to de-install EBP. The procedure is very similar to installation and the same precautions apply, but there are no options to choose and the disk is decrypted rather than encrypted. It is vital that nothing interrupts this operation.

De-installation

Boot off a DOS system disk then insert Stoplock Disk 1 in **A:**

At the A:\ prompt type:

UNPROT

and press **Q** . The Introduction Screen is displayed. To continue with de-installation, type *Y* and press **Q** .

The Program Password Explanation Screen is displayed.

Program Password Entry Screen

This screen requires you to enter the password which was chosen at installation time. Type the **program** password and press **Q** . You will then be asked to repeat this password.

WARNING!
THE DECRYPTION PROCESS BEGINS AS SOON AS YOU PRESS ENTER!
This is your final opportunity to terminate the program by using the **D** key.

If the two passwords match and are correct then decryption commences immediately.

Decryption

This process takes as long as encryption did at installation time – anything from a few seconds to several hours.

WARNING!
DO NOT INTERRUPT THE DECRYPTION PROCESS!
You risk losing your data if you interrupt decryption.

While decryption is in progress a message remains on screen warning you that the program is unprotecting the disk and that the process should not be interrupted. A thermometer bar is displayed to inform you of progress.

Once decryption is complete the message changes to ‘Unprotection complete. Press any key to reboot your PC’. You should remove the product disk and press any key: the PC automatically reboots.

EXTENDED BOOT PROTECTION IS NOW REMOVED.

Protect Options

The purpose of the options described here is to enable full or partial ‘hands-free’ installation of Extended Boot Protection. In this way, you (as administrator) could safely delegate installation by setting up the required options within a small batch file.

The effect of each option is to cause one or more screens to be bypassed by providing the relevant information on the command line instead of in response to a prompt. If you take all the available options, only the final screen is ever presented. The options are:

-q

Specify this switch to bypass the initial confirmation screen.

-k*program-password*

Use this option to specify a program password.

Specifying -k also causes the boot password screens to be bypassed.

-b*boot-password*

Use this option to specify a boot password.

If you do this, all the relevant screens are bypassed as described above, regardless of whether -k is also specified.

-r*x*

Use this option to specify the extent of encryption.

Specify **-rf** for full disk encryption or **-rp** to encrypt just the system area.

-t*n*

Use this option to specify the timeout value. Specify the value *n* as a number of seconds, up to a maximum of 999.

-v

Specify this switch to get access to the encryption range form (useful for Compaq diagnostic partitions) and for other engineering purposes.

Please contact the PCSL Help Desk should you require advice on using any of the protect options.

Examples of use

In the first example the program password is ‘bomb-proof’, a boot password is not implemented, and the whole disk is to be encrypted. Manual interventions are retained for initial confirmation and timeout value.

```
protect  -kbomb-proof  -rf
```

In the second example the program password is ‘hyphenate’, the boot password is ‘logical’, only the system area of the disk is to be encrypted and the timeout value is 20 seconds. No manual interventions are required.

```
protect  -q  -khyphenate  -blogical  -rp  -t20
```