

Encryption Plus[®] Hard Disk

Windows NT/2000/XP

Data Security for Notebooks & Desktops

User Guide

Enterprise-Version 7.0

Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of PC Guardian.

©2002 PC Guardian. All rights reserved.
1133 E. Francisco Blvd.
San Rafael, CA 94901-5427
415.459.0190

Encryption Plus is a registered trademark of PC Guardian.

All product names mentioned in this guide may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

Rev. 09/20/02

End User License Agreement

THIS IS A LEGAL AGREEMENT BETWEEN YOU AS THE END USER AND PC GUARDIAN. THIS IS A LICENSE AGREEMENT AND THE PC GUARDIAN SOFTWARE PROGRAM THAT ACCOMPANIES IT ("the SOFTWARE") IS LICENSED FOR USE ONLY PER THE TERMS SET FORTH HEREIN. PLEASE READ THIS LICENSE AGREEMENT. BY INSTALLING THE SOFTWARE, YOU ARE AGREEING TO THE TERMS OF THIS LICENSE AGREEMENT. IF YOU DO NOT AGREE WITH THESE TERMS, UNINSTALL THE SOFTWARE.

GRANT OF LICENSE. PC GUARDIAN grants you a nonexclusive, non-transferable license to: (i) use the SOFTWARE, in executable form only, on a single computer or CPU; and, (ii) make one copy the SOFTWARE for backup and archival purposes. The copy shall be subject to all terms, conditions, and obligations of this Agreement.

RESTRICTIONS. You may not: (i) modify, translate, or merge the SOFTWARE with another program; (ii) reverse-engineer, disassemble, decompile, or make any attempt to discover the source code of the SOFTWARE; or (iii) sublicense, rent, transfer, or lease any portion of the SOFTWARE.

COPYRIGHT. All title, right and interest in the SOFTWARE and related trademarks, trade names, and other intellectual property rights are owned by PC GUARDIAN and the SOFTWARE is protected by United States and international copyright laws and international trade provisions. You must treat the SOFTWARE like any other copyrighted material.

GOVERNMENT LICENSE. If you are acquiring the SOFTWARE on behalf of any unit or agency of the United States Government, the following provisions apply:

The Government acknowledges PC GUARDIAN'S representation that the SOFTWARE was developed at private expense and no part of it is in the public domain.

The Government acknowledges PC GUARDIAN'S representation that the SOFTWARE is "Restricted Computer SOFTWARE" as that term is defined in Clause 52.227-19 of the Federal Acquisition Regulations (FAR) and is "Commercial Computer SOFTWARE" as that term is defined in Subpart 227.471 of the Department of Defense Federal Acquisition Regulation Supplement (DFARS). The Government agrees that: (i) if the SOFTWARE is supplied to the Department of Defense (DoD), the SOFTWARE is classified as "Commercial Computer Software" and the Government is acquiring only "restricted rights" in the SOFTWARE as that term is defined in Clause 252.227-7013 (c) (1) of the DFARS; and, (ii) if the SOFTWARE is supplied to any unit or agency of the United States Government other than DoD, the Government's rights in the SOFTWARE will be as defined in Clause 52.227-19 (c) (2) of the FAR.

Restricted Rights Legend. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013. Micro Security Devices, Inc. DBA PC Guardian 1133 E. Francisco Blvd. San Rafael, CA 94901.

LIMITED WARRANTY. PC GUARDIAN warrants that for a period of 90 days from the date of original purchase: (i) the SOFTWARE will perform substantially in accordance with the

End User License Agreement

documentation; and, (ii) any media disks enclosed with the SOFTWARE will be free from defects in materials and workmanship under normal use. This limited warranty is void if the SOFTWARE or media disk failed due to accident, abuse, or misapplication. Your sole and exclusive remedy and PC GUARDIAN'S entire liability during this 90 day warranty period shall be, at PC GUARDIAN'S option: (i) repair and replacement of SOFTWARE or documentation that do not meet PC GUARDIAN'S limited warranty; or, (ii) refund of the purchase price paid for the license. To make a claim under this limited warranty, you must uninstall the SOFTWARE and notify PC GUARDIAN within 10 days of expiration of the warranty period.

PC GUARDIAN does not warrant that the SOFTWARE will meet your requirements, or that the operation of the SOFTWARE will be uninterrupted or error free, or that all SOFTWARE errors will be corrected. PC GUARDIAN is not responsible for problems or non-conformities caused by the use of the SOFTWARE with non PC GUARDIAN software or by changes in the operating methods of computer hardware or computer operating systems which are made after the release of the SOFTWARE.

THE ABOVE WARRANTIES ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESSED OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY PC GUARDIAN, ITS EMPLOYEES, DISTRIBUTORS, DEALERS, OR AGENTS SHALL INCREASE THE SCOPE OF THE ABOVE WARRANTIES OR CREATE ANY NEW WARRANTIES.

SOME STATES MAY NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. IN THAT EVENT, ANY IMPLIED WARRANTIES ARE LIMITED IN DURATION TO NINETY (90) DAYS FROM THE DATE OF DELIVERY OF THE SOFTWARE. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

LIMITATION OF LIABILITY. REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL PC GUARDIAN BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE OR ANY DATA SUPPLIED THEREWITH EVEN IF PC GUARDIAN OR ANYONE ELSE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR FOR ANY CLAIM BY ANY OTHER PARTY. PC GUARDIAN'S CUMULATIVE LIABILITY TO YOU OR ANY OTHER PARTY FOR ANY LOSS OF DAMAGES RESULTING FROM ANY CLAIMS, DEMANDS OR ACTIONS ARISING OUT OF OR RELATING TO THIS AGREEMENT SHALL NOT EXCEED THE PURCHASE PRICE PAID FOR THE LICENSE.

SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

EXPORT LAW ASSURANCES. You acknowledge and agree that the SOFTWARE is subject to restrictions and controls imposed by the United States Export Administration Act (the "Act") and the regulations thereunder. You agree and certify that neither the SOFTWARE nor any direct product thereof is being or will be acquired, shipped, transferred, or re-exported, directly

End User License Agreement

or indirectly, into any country prohibited by the Act and the regulations thereunder or will be used for any purpose prohibited by the same.

TERMINATION. This Agreement to use the SOFTWARE will terminate automatically if you violate any part of this Agreement. In the event of termination, you must immediately remove all installed copies of the SOFTWARE and destroy all copies of the SOFTWARE. GENERAL. This Agreement is governed by the laws of the State of California and you consent to the jurisdiction and venue of the courts of the State of California. Should any term or condition of this Agreement be declared void or unenforceable by any court of competent jurisdiction, such declaration shall have no effect on the remaining terms hereof. The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.

YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS. FURTHER, YOU AGREE THAT IS THE COMPLETE AND EXCLUSIVE STATEMENT OF THE AGREEMENT BETWEEN YOU AND PC GUARDIAN WHICH SUPERSEDES ANY PROPOSAL OR PRIOR AGREEMENT, ORAL OR WRITTEN, AND ANY OTHER COMMUNICATION BETWEEN YOU AND PC GUARDIAN RELATING TO THE SUBJECT MATTER OF THIS AGREEMENT. If you have any questions regarding this Agreement, please write: PC Guardian 1133 E. Francisco Blvd. San Rafael, CA 94901 USA.

Table of Contents

END USER LICENSE AGREEMENT	3
INTRODUCTION TO EP HARD DISK.....	8
ABOUT THIS PUBLICATION	8
DOCUMENTATION CONVENTIONS.....	8
PROGRAM OVERVIEW.....	8
WHAT'S NEW IN THIS VERSION	9
INSTALLATION AND SETUP.....	10
CONSIDERATIONS BEFORE INSTALLATION AND ENCRYPTION	10
REMOTE INSTALLATION—OVERVIEW	11
REMOTE INSTALLATION—SETUP AND INITIAL ENCRYPTION	11
LOCAL INSTALLATION—OVERVIEW	14
LOCAL INSTALLATION—STANDARD INSTALLATION AND SETUP	14
PRE-ENCRYPTED DRIVES—OVERVIEW	16
PRE-ENCRYPTED DRIVES—SETUP	16
SETTING UP AUTHENTI-CHECK	17
EP HARD DISK INTERFACE	19
LOGGING ON	20
LOGGING ON WITH SINGLE SIGN-ON.....	20
LOGGING ON WITH THE SINGLE SIGN-ON PASSWORD SYNCHRONIZATION FEATURE ENABLED.....	21
MAIN MENU	21
BASIC NAVIGATION.....	22
INITIAL ENCRYPTION AND DECRYPTION	24
ENCRYPTING A DRIVE	24
DECRYPTING A DRIVE	26
CHECKING THE DRIVE STATUS	27
PERFORMANCE MONITOR.....	28
RECOVER PROGRAM.....	29
FORGOTTEN PASSWORDS.....	31
USING AUTHENTI-CHECK.....	32
USING THE ONE-TIME PASSWORD PROGRAM.....	33
UPDATE SETTINGS.....	34
UPDATING YOUR USER NAME.....	35
UPDATING YOUR USER PASSWORD	36
UNINSTALLING	37
APPENDIX A	38
GLOSSARY	38
APPENDIX B.....	41
TABLES OF PARAMETERS	41
APPENDIX C	42
GUIDELINES FOR CREATING AUTHENTI-CHECK QUESTIONS	42
APPENDIX D	43
TECHNICAL SUPPORT	43

Table of Contents

Table of Figures

FIGURE 1—WELCOME AND KEYBOARD LAYOUT	11
FIGURE 2—CREATE USER NAME AND PASSWORD	12
FIGURE 3—AUTHENTI-CHECK SETUP	13
FIGURE 4—ENCRYPT DRIVES	13
FIGURE 5—PRE-WINDOWS LOGON	20
FIGURE 6—MAIN MENU	22
FIGURE 7—ENCRYPT DRIVES	25
FIGURE 8—DECRYPT DRIVES	26
FIGURE 9—DRIVE STATUS	27
FIGURE 10—PERFORMANCE MONITOR	28
FIGURE 11—AUTHENTI-CHECK QUESTION	32
FIGURE 12—UPDATE USER SETTINGS	35

Chapter One

INTRODUCTION TO EP HARD DISK

About this Publication

The Encryption Plus® Hard Disk User Guide will provide you with:

- An overview of EP Hard Disk User Program features
- Step-by-step instructions on how to use features in the EP Hard Disk User Program.

This documentation was written with the assumption that you have a basic knowledge of Windows, including using a mouse, navigating the Windows interface, restarting and logging on to your computer, and, if applicable, installing software.

Documentation Conventions

The following conventions were used in creating this documentation:

- The shortened name EP Hard Disk is used throughout this User Guide in place of the formal product name, which is Encryption Plus® Hard Disk.
- Each chapter begins with a basic, conceptual introduction. Step-by-step instructions then explain how to perform the related tasks in the EP Hard Disk User Program.
- Shortened terminology, such as using program administrator to refer to any one of the three administrator type, is defined in the Glossary.
- All parameters for password length, Authenti-Check, and other settings are included in *Appendix B—Parameters*.

Program Overview

Encryption Plus® Hard Disk is designed to encrypt all of the data or up to eight partitions on a computer's hard disk, using the Advanced Encryption Standard (AES, or the Rijndael algorithm). Since EP Hard Disk operates at the pre-DOS level, access is controlled via a logon that is required before Windows starts up. After the initial encryption, EP Hard Disk works

Introduction to EP Hard Disk

transparently with other applications to encrypt data as it is created on the hard disk. When files are accessed by the user, the data is decrypted and then re-encrypted on-the-fly. Encryption on-the-fly should have no impact a computer's normal operation.

A variety of settings are available in the EP Hard Disk Administrator Program to define User Program elements such as password settings, corporate and local administrators, password recovery options, and initial encryption speed. These settings are saved to User Program Setup files that can be deployed locally or over a network. A majority of user settings can also be updated over a network with logon scripts.

What's New in this Version

- Keyboard layout support added for English (UK), French, German, Italian, Portuguese, Portuguese (Brazil), and Spanish (Spain).
- AES algorithm with a 256-bit key.
- Corporate administrator role added. This role can access large installation groups that have multiple local administrators.
- Authenti-Check password recovery, which uses a self-service question/answer format.
- Administrators can select initial encryption settings based on desired speed and existing hardware.
- Completely redesigned interface. Wizard structure streamlines linear processes.
- Background encryption—users can continue to work at their computers during initial disk encryption and decryption.
- Turning off Master Boot Record protection in anti-virus programs is no longer required.
- Synchronization of the EP Hard Disk User Password with the Windows user password.

Chapter Two

INSTALLATION AND SETUP

This chapter describes how you or a program administrator can install and set up the EP Hard Disk User Program on your computer.

The EP Hard Disk Administrator Program generates the EP Hard Disk User Program Setup files. You or a program administrator can install the EP Hard Disk on your computer in three different ways. With a remote installation, the EP Hard Disk Administrator will install the software over the company's network. With a local installation, a technician will install the software directly on your computer by using files from an accessible network drive or on removable media. In addition, you could receive a workstation that has been set up for you with a complete installation and a pre-encrypted drive.

Considerations Before Installation and Encryption

The following issues should be considered before you complete the installation and encryption:

- If the computer has a previous version of EP Hard Disk installed, decrypt the drive and uninstall the older version before initiating an upgrade.
- All partitioning, formatting, and resizing should be completed before EP Hard Disk is installed.
- Do not modify encrypted partitions in any way—including partitioning, formatting, and resizing—with Partition Magic or any other utility.
- After the EP Hard Disk User Program installation, a recover disk should be made. See the [Recover Program](#) section for information on how to create a recover disk.
- To optimize the initial encryption speed, run Chkdsk and defragment the hard drive before encryption.
- EP Hard Disk does not support the encryption of Volume Set partitions. If such a partition is selected for encryption, it may not be fully encrypted.

Remote Installation—Overview

If the EP Hard Disk Administrator chooses Remote Installation, the installation takes place over the network. Windows administrator rights are required to perform and complete the installation. You will not be required to take part in any of the installation process except for the standard User Program setup, which includes setting your password and creating your Authentic-Check password recovery questions, if required.

Remote Installation—Setup and Initial Encryption

To set up EP Hard Disk and encrypt your drives

1. After the program has completely installed and Windows completely starts up, the EP Hard Disk User Program will launch and display a Welcome screen that may require you to select a keyboard layout.

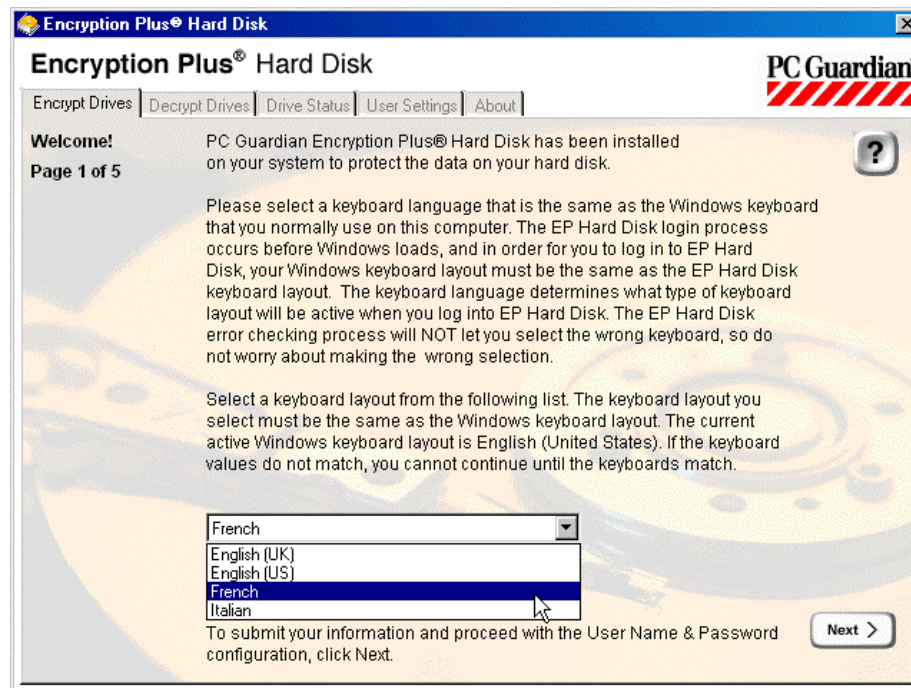


Figure 1—Welcome and Keyboard Layout

2. Select your keyboard layout, if required. This allows EP Hard Disk to recognize user names, passwords, and other text that you type in your preferred language. The keyboard layouts must match or you will not be allowed to continue the setup process. US English is the default language.

Note: The EP Hard Disk Administrator can have EP Hard Disk determine and configure this setting automatically, require a specific keyboard layout, or let you choose your keyboard layout from a list.

Installation and Setup

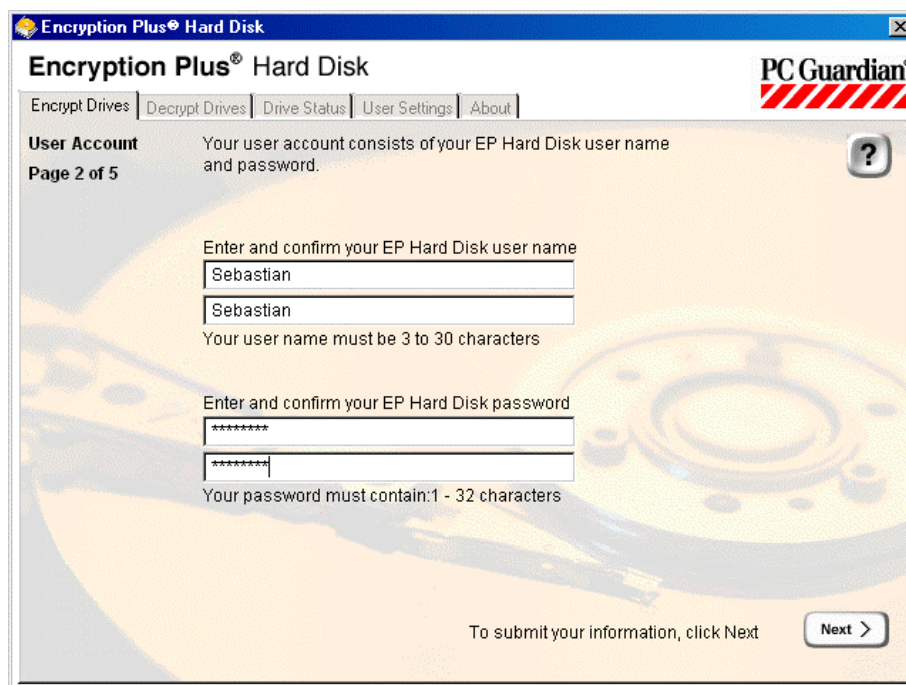


Figure 2—Create User Name and Password

3. If the EP Hard Disk Administrator enabled Single Sign-On, enter your Windows User Name and Password.

Note: The Windows Name and User Password must already be set up on your computer.

4. Enter and confirm your User Name. The User Name must be 3-30 characters in length and is not case sensitive.

Note: Characters from the character map will not display in your primary logon because Windows will not yet be launched. The characters that you can use for your User Name and Password are: letters A through Z, numbers 0 through 9, and the following special characters:

\$ # @ % & * () + ? !

5. Enter and confirm your User Password. The User Password must be 6-32 characters in length, though the EP Hard Disk Administrator may set the minimum length to be lower than six. The User Password is case sensitive. Additional password restrictions chosen by the administrator are listed below the text field. Click Next.

Note: See the Note on entering the User Name, above, for recommended characters.

6. If your EP Hard Disk Administrator has chosen Authenti-Check as a password recovery method, enter the required answers or question and answer pairs.

Installation and Setup

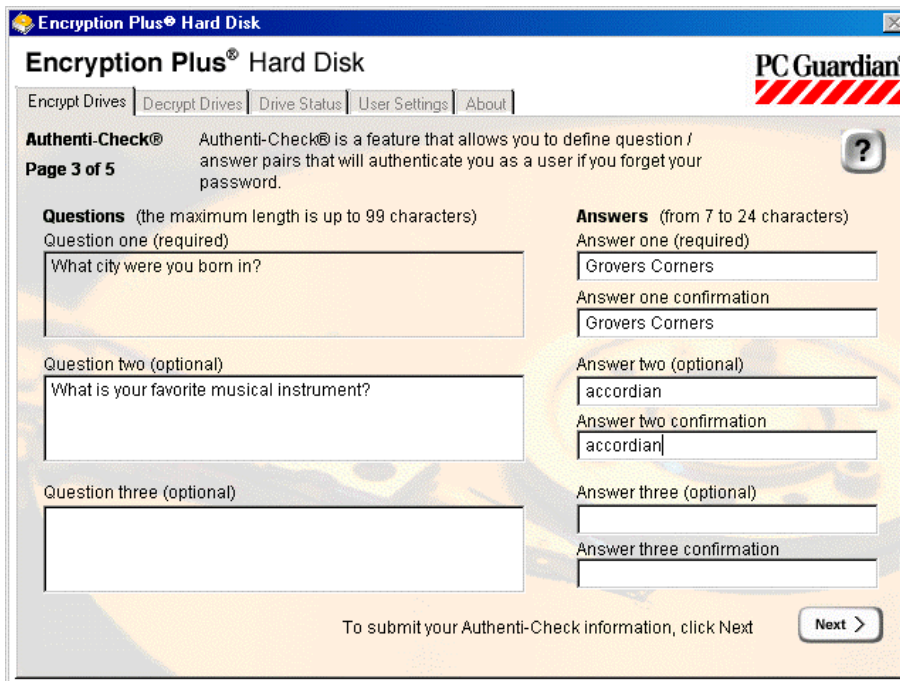


Figure 3—Authenti-Check Setup

Up to two questions may be optional. For more detailed information and guidelines, see the [Setting Up Authenti-Check](#) section. Click Next when you have completed entering your questions and answers.

7. The Encrypt Drives screen will display.



Figure 4—Encrypt Drives

Installation and Setup

Select the partition or partitions on your hard drive that you want to have encrypted. The EP Hard Disk Administrator may have designated automatic selection of all partitions, and can set a default encryption speed. If the EP Hard Disk Administrator has set the encryption speed to Fast, your computer may run more slowly than usual. If the EP Hard Disk Administrator has set the encryption speed to Slow, your computer will not run as slowly, but encryption will take longer. You can change the speed while encryption is in progress.

Note: You can encrypt up to eight partitions with a combined size of up to one terabyte.

If desired, change the speed setting and click Next. The encryption process will begin. You will not be able to exit this screen or the encryption process until the encryption is complete.

Notes: To minimize the EP Hard Disk User Program screen during encryption, click Next. To maximize the screen, double-click the EP Hard Disk icon in the status area.

If you will be using encryption in the background while working in other applications, save a backup copy of your work in a network folder.

The partition size and the EP Hard Disk encryption settings may cause the progress bar to remain at a certain percentage for a long period of time. Check the [Performance Monitor](#) if you want to make sure that the process is running.

8. When the encryption process has been completed, a success screen will display.

From this point on, EP Hard Disk will continue to protect your drives in the background. An icon will continually display in the status area. You can double-click the icon, right-click the icon and select Open, or launch the program through the Windows Start menu at any time to access the EP Hard Disk User Program interface.

Local Installation—Overview

If the EP Hard Disk Administrator chooses a local installation, a technician will need to be at your workstation in order to install the EP Hard Disk User Program. The software will be available through removable media, network access, or a network logon script. Windows administrator rights are required to perform and complete the installation.

Local Installation—Standard Installation and Setup

Note: You will need Windows administrator rights to complete the installation process.

1. Browse to the location of the Setup.exe file for the EP Hard Disk User Program.
2. Double-click the Setup.exe icon and follow the InstallShield prompts. Click Finish to restart the computer.

Note: You should not shut down the computer to complete the installation at a later time.

3. When the computer restarts, log on to Windows as an administrator. EP Hard Disk will continue to install. After Windows completely starts up, the EP Hard Disk User Program will launch. At this time, you can shut down the workstation to allow the user to complete the setup process.

Installation and Setup

4. At the EP Hard Disk Welcome screen, enter a keyboard layout, if required. This allows EP Hard Disk to recognize user names, passwords, and other text that you type in your preferred language. The keyboard layouts must match or you will not be allowed to continue the setup process. US English is the default language.

Note: The EP Hard Disk Administrator can have EP Hard Disk determine and configure this setting automatically, require a specific keyboard layout, or let you choose your keyboard layout from a list.

5. If the EP Hard Disk Administrator has enabled Single Sign-On, enter your Windows User Name and Password.

Note: The Windows Name and User Password must already be set up on your computer.

6. Enter and confirm your User Name. The User Name must be 3-30 characters in length and is not case sensitive.

Note: Characters from the character map will not display in your primary logon because Windows will not yet be launched. The characters that you can use for your User Name and Password are: letters A through Z, numbers 0 through 9, and the following special characters:

\$ # @ % & * () + ? !

7. Enter and confirm your User Password. The User Password must be 6-32 characters in length, though the EP Hard Disk Administrator may set the minimum length to be lower than six. The User Password is case sensitive. Other password restrictions chosen by the administrator will be listed below the text field. Click Next.

Note: See the Note on entering the User Name, above, for recommended characters.

8. If your EP Hard Disk Administrator has chosen Authenti-Check as a password recovery method, enter the required question and answer pairs. Up to two questions may be optional.

Click Next when you have completed entering your questions and answers. For more detailed information and guidelines, see the [Setting Up Authenti-Check](#) section.

9. At the Encrypt Drives screen, you can select the partition or partitions that you would like to encrypt. The EP Hard Disk Administrator may have set parameters that automatically select all partitions, and can set a default encryption speed. If the EP Hard Disk Administrator has set the encryption speed to Fast, your computer may run more slowly than usual. If the EP Hard Disk Administrator has set the encryption speed to Slow, your computer will not run as slowly, but encryption will take longer. You can change the encryption speed while encryption is in progress.

Note: You can encrypt up to eight partitions with a combined size of up to one terabyte.

If desired, change the speed setting and click Next. The encryption process will begin. You will not be able to exit this screen or the encryption process until the encryption is complete.

Notes: To minimize the EP Hard Disk User Program screen during encryption, click Next. To maximize the screen, double-click the EP Hard Disk icon in the status area.

If you will be using encryption in the background while working in other applications, save a backup copy of your work in a network folder.

Installation and Setup

The partition size and the EP Hard Disk encryption settings may cause the progress bar to remain at a certain percentage for a long period of time. Check the [Performance Monitor](#) if you want to make sure that the process is running.

10. When the encryption process has been completed, a success screen will display.

From this point on, EP Hard Disk will continue to protect your drives in the background. An icon will continually display in the status area. You can double-click the icon, right-click the icon and select Open, or launch the program through the Windows Start menu at any time to access the EP Hard Disk User Program interface.

Pre-Encrypted Drives—Overview

The EP Hard Disk Administrator can choose a process that will install EP Hard Disk and pre-encrypt workstations before the computers are sent to users.

Because encryption has already taken place, only part of the normal setup will need to be completed.

Pre-Encrypted Drives—Setup

1. After you switch on the power and Windows completely starts up, the EP Hard Disk User Program will launch and display a Welcome screen.

Note: You might see an EP Hard Disk screen flash briefly right after you turn your workstation on; this is normal.

Select your keyboard layout, if required. This allows EP Hard Disk to recognize user names, passwords, and other text that you type in your preferred language. The keyboard layouts must match or you will not be allowed to continue the setup process. US English is the default language.

Note: The EP Hard Disk Administrator can have EP Hard Disk determine and configure this setting automatically, require a specific keyboard layout, or let you choose your keyboard layout from a list.

2. If the EP Hard Disk Administrator has enabled Single Sign-On, enter your Windows User Name and Password.

Note: The Windows Name and User Password must already be set up on your workstation.

3. Enter and confirm your User Name. The User Name must be 3-30 characters in length and is not case sensitive.

Note: Characters from the character map will not display in your primary logon because Windows will not yet be launched. The characters that you can use for your User Name and Password are: letters A through Z, numbers 0 through 9, and the following special characters:

\$ # @ % & * () + ? !

Installation and Setup

4. Enter and confirm your User Password. The User Password must be 6-32 characters in length, though the EP Hard Disk Administrator may set the minimum length to be lower than six. The User Password is case sensitive. Other password restrictions chosen by the administrator will be listed below the text field. Click Next.

Note: See the Note on entering the User Name, above, for recommended characters.

5. If your EP Hard Disk Administrator has chosen Authenti-Check as a password recovery method, enter the required answers or question and answer pairs.

Up to two questions may be optional. For more detailed information and guidelines, see the [Setting Up Authenti-Check](#) section. Click Next when you have completed entering your questions and answers.

6. When the setup process is complete, a success screen will display.

EP Hard Disk will continue to protect your drives in the background. An icon will continually display in the status area. You can double-click the icon, right-click the icon and select Open, or launch the program through the Windows Start menu at any time to access the EP Hard Disk User Program interface.

Setting Up Authenti-Check

For all installations, part of the setup process is setting up Authenti-Check, if your EP Hard Disk Administrator has enabled this password recovery method.

Authenti-Check is a question-response authentication method that verifies your identity by prompting you to answer questions. You will be providing your answers to pre-determined questions set by the EP Hard Disk administrator, your own questions and answers, or both.

If you forget your password at some later point in time, you can answer your Authenti-Check questions and set a new user name and password. This will allow you to regain access to your computer and your files.

The Authenti-Check setup screen

The Authenti-Check setup screen contains a number of data entry fields to create and verify up to three question and answer pairs. You must create at least one question and answer pair. See Appendix C—Guidelines for Setting Up Authenti-Check Questions if you would like to see examples of secure questions.

Types of Authenti-Check question and answer pairs

There are three types of question and answer pairs:

An **administrator defined** question is a question that the EP Hard Disk Administrator defined when creating the User Program Setup. You will be required to answer this question in order to complete the Authenti-Check setup process.

Installation and Setup

A **required user defined question** is a question that your EP Hard Disk Administrator has chosen for you to set up. You will be required to create and answer this question in order to complete the Authenti-Check setup process.

An **optional user defined question** is a question that your EP Hard Disk Administrator did not require and you are not required to create a question and answer pair. However, setting up optional questions will make your workstation less vulnerable to unauthorized access.

To set up your Authenti-Check question and answer pairs

You cannot modify Authenti-Check question and answer pairs in any way after you create them. The only way to change them will be to decrypt your drive and re-install the EP Hard Disk User Program.

1. Type your question (if applicable) in the first data entry field.
2. Type and confirm your answer in the two data entry fields to the right of the question.

Note: Characters from the character map will not display in Authenti-Check because Windows will not yet be launched. The characters that you can use for the answers are: letters A through Z, numbers 0 through 9, and the following special characters:
\$ # @ % & * () + ? !

3. Repeat steps One and Two for the second and third Authenti-Check question and answer pairs, if required. You can also create your own optional user-defined question and answer pairs at this time
4. Click Next to confirm your Authenti-Check question and answer pairs and continue the setup process.

Chapter Four

EP HARD DISK INTERFACE

This chapter describes how to navigate the EP Hard Disk User Program interface, including logging on to the program and accessing the program features.

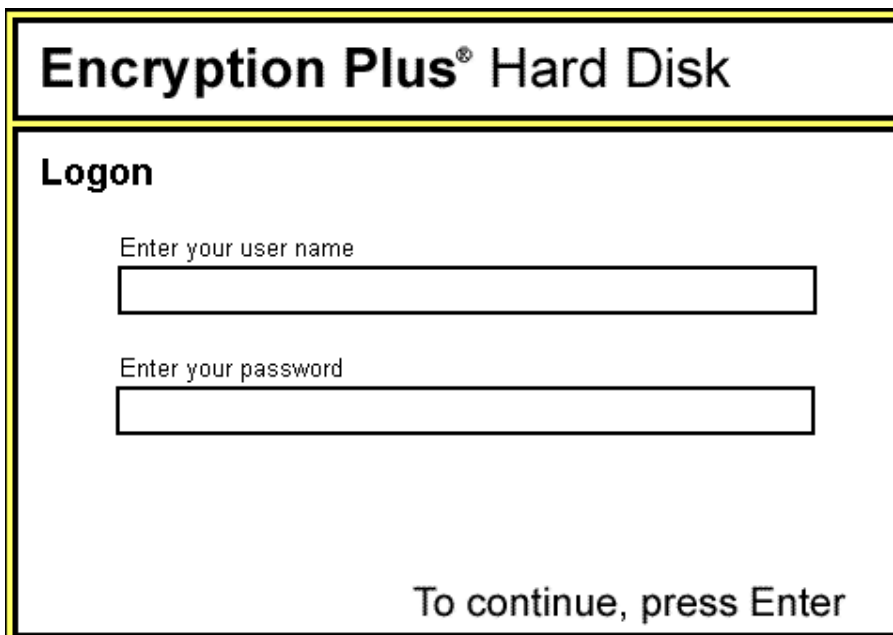
There are two different EP Hard Disk screen types that will display, depending on the Windows operating system startup status. The first screens display before Windows has completely started, or is in the “pre-boot” stage. The other type of screen displays when the EP Hard Disk User Program has been started after Windows has “launched” and you can see your Windows desktop.

The EP Hard Disk Administrator may have chosen to enable Single Sign-On, which allows you to log on to EP Hard Disk and Windows at the same time. If the EP Hard Disk Administrator has not enabled Single Sign-On, you will log on to EP Hard Disk and Windows separately.

Logging On

If the EP Hard Disk Administrator has not enabled Single Sign-On, you will need to log on to EP Hard Disk and Windows separately.

To log on, enter your EP Hard Disk User Name and Password at the EP Hard Disk Logon screen.



Encryption Plus® Hard Disk

Logon

Enter your user name

Enter your password

To continue, press Enter

Figure 5—Pre-Windows Logon

This screen will occur before the Windows logon screen, which you can complete as usual. Your User Name and User Password for Windows and EP Hard Disk can be different.

Tip: Press Tab to go to the next field, or Shift + Tab to go back to the previous field. Press Enter when you have completed the screen.

If you cannot remember your EP Hard Disk User Password, enter incorrect responses. After you reach the Lockout number set by the EP Hard Disk Administrator, this will launch Authenti-Check, One-Time Password, or both recovery methods. See Chapter Six—Forgotten Passwords for more details and step-by-step instructions.

Logging On with Single Sign-On

To log on to EP Hard Disk and Windows with Single Sign-On, enter your User Name and User Password at the EP Hard Disk Logon. Because the EP Hard Disk Administrator has enabled Single Sign-On and the EP Hard Disk logon process occurs before Windows has launched, you can log on to both EP Hard Disk and Windows at the same time.

Tip: Press Tab to go to the next field, or Shift + Tab to go back to the previous field. Press Enter when you have completed the screen.

EP Hard Disk Interface

If you cannot remember your EP Hard Disk User Name, User Password, or both, you should submit incorrect responses. After you reach the Lockout number set by the EP Hard Disk Administrator, this will launch Authenti-Check or One-Time Password recovery methods. See Chapter Six—Forgotten Passwords, for more details and step-by-step instructions.

Logging On with the Single Sign-On Password Synchronization Feature Enabled

To log on to EP Hard Disk and Windows with Single Sign-On, enter your Windows User Name and User Password at the EP Hard Disk Logon. Because the EP Hard Disk Administrator has enabled Single Sign-On with Password Synchronization and the EP Hard Disk logon process occurs before Windows has launched, you can log on to both EP Hard Disk and Windows at the same time. Password synchronization changes your EP Hard Disk user account to match any changes to your Windows user account.

Tip: Press Tab to go to the next field, or Shift + Tab to go back to the previous field. Press Enter when you have completed the screen.

If you cannot remember your Windows User Name, User Password, or both, you can submit incorrect responses. After you reach the Lockout number set by the EP Hard Disk Administrator, this will launch Authenti-Check or One-Time Password recovery methods. See Chapter Six—Forgotten Passwords, for more details and step-by-step instructions.

Notify your program administrator that you had to change your user account with Authenti-Check, as this will affect how password synchronization works.

Main Menu

The EP Hard Disk Main menu is the basic starting point for navigating through all features in the program. The tabs at the top will allow you to go to the following user tasks. Each task is fully described in its associated chapter.

To launch the main menu, double-click the icon in the status area of the Windows taskbar, or right-click and select Open.

EP Hard Disk Interface

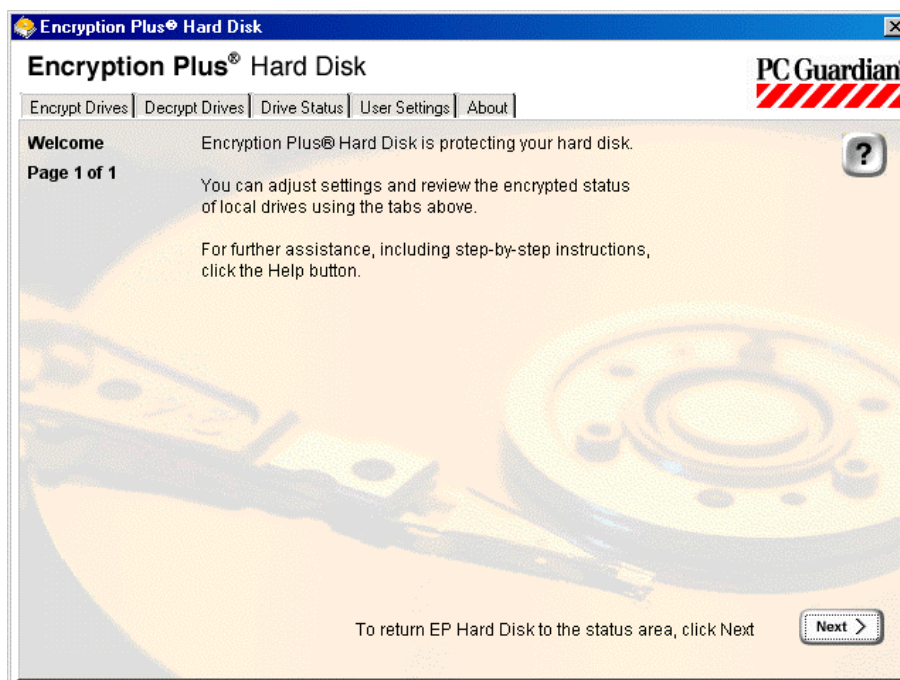


Figure 6—Main Menu

Encrypt Drives—This tab allows you to encrypt any partition or partitions on your hard drive that are not already encrypted. A logon is required.

Decrypt Drives—This tab allows you to select partitions for decryption. Your EP Hard Disk Administrator may have restricted your access to this tab. A logon is required.

Drive Status—This tab allows you to see if your drives are encrypted, being encrypted, decrypted, or being decrypted.

User Settings—This tab allows you or a program administrator to change your User Name and Password, if the EP Hard Disk Administrator has permitted changes. A logon is required.

After successful completion or canceling out of any of these processes, EP Hard Disk will return you to this main menu or will minimize to the status area.

To minimize the main menu, click Close. It is important to note that after EP Hard Disk is installed, the program is always open in the background. As long as EP Hard Disk remains installed, the icon in the status area will always display.

Basic Navigation

To navigate, or get around in, the EP Hard Disk interface after the full program has started, click the appropriate tab at the top of the EP Hard Disk User Program main screen. Depending on the function, EP Hard Disk may prompt you to provide your User Name and Password.

Each screen has common elements:

EP Hard Disk Interface

The top, left corner of the screen will have a title, page number, and a total number of pages. If there are multiple screens in the process that you are using, the page number will display, for example, as “Page 1 of 3.” It is important to note the title and page number if you will be calling your help desk or an administrator for support.

The text at top center in the screen describes the last successful step that you took in EP Hard Disk. This section may also welcome you to a function or confirm that you have successfully completed a user function in the program.

The text in the middle center of the screen will contain fields and text that will allow you to complete a specific task in EP Hard Disk. At other times, this section will describe useful information, such as a list of drives and their status. If you are typing information, use the Tab key to complete a field entry and go to the next field. An error message will display if you press Tab, click the mouse, or press Return before required fields are completed.

The text next to the navigation buttons describes where you will be directed if you click the Back, Next, or Finish button.

The Back button will take you back to the previous screen if you would like to make changes to entries you have made. If you do go back to a previous screen, EP Hard Disk will preserve the information on the screen that you just left. If you are in the first screen of a process, or cannot go back, the Back button will not display.

The Next button will take you to the next screen in the particular process. In certain cases, clicking the Next button will prompt EP Hard Disk to complete a procedure and take you to a success screen. You may need to wait for your computer to complete a process.

The Help button will lead you to specific instructions for a particular procedure or step. In some cases, the Help contents topic will display instead of a specific topic. If this occurs, use the Help contents or index to locate the information that you need.

Chapter Five

INITIAL ENCRYPTION AND DECRYPTION

This chapter describes how to encrypt and decrypt your drives, as well as how to check the encryption status of the partitions on your drive.

You will only be able to decrypt drives if your EP Hard Disk Administrator has authorized you to do so.

Encrypting a Drive

Encryption is a process by which an algorithm is used to render data unreadable to anyone who does not have the proper key to read or decrypt the information. When you encrypt a drive, you are prompting EP Hard Disk to perform that process.

After a drive is encrypted, you will be able to access your data as usual after you have logged on with the correct EP Hard Disk User Name and Password. When you access data that is saved on the encrypted drive, EP Hard Disk will decrypt the data on-the-fly so that you can read it, and then re-encrypt the information when you close the file. This allows only the information or files being accessed at the time to be readable. At the same time, all of the other data on your hard drive is still encrypted. Information that you create on the hard drive will be automatically encrypted.

To encrypt a drive

1. Launch the EP Hard Disk User Program by double-clicking the icon in the status area of the Windows task bar, right-clicking the icon and selecting Open, or by launching through the Windows Start menu.
2. The EP Hard Disk User Program Main menu will display. Click the Encrypt Drives tab.
3. At the prompt, type your EP Hard Disk User Name and Password. Click Next.
4. The Encrypt Drives screen will display.

Encryption and Decryption

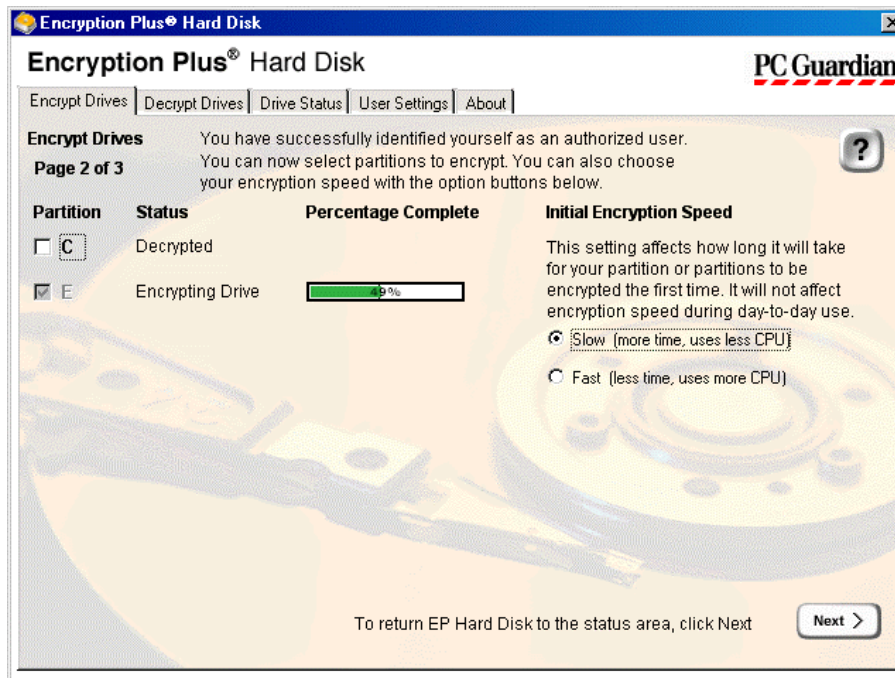


Figure 7—Encrypt Drives

Select the partition or partitions to encrypt by clicking the checkbox next to the drive letter.

Note: You can encrypt up to eight partitions with a combined size of up to one terabyte.

The EP Hard Disk Administrator will have set a speed of Fast or Slow. If the EP Hard Disk Administrator has set the encryption speed to Fast, your computer may run more slowly than usual. If the EP Hard Disk Administrator has set the encryption speed to Slow, your computer will not run as slowly, but encryption will take longer. You can change the encryption speed while encryption is in progress.

If desired, change the speed setting and click Next. The encryption process will begin.

Notes: Click the Next button to minimize the EP Hard Disk User Program screen during encryption. To maximize the screen, double-click the EP Hard Disk icon in the status area.

If you will be using encryption in the background while working in other applications, save a backup copy of your work in a network folder.

The size of the partition designated for encryption and the EP Hard Disk encryption settings may cause the progress bar to remain at a certain percentage for a long period of time. Check the [Performance Monitor](#) if you want to make sure that the process is running.

If you would like to exit and not encrypt any partitions at this time, click on any other tab at the top of the screen.

6. When encryption has been completed, you will see a Success screen. From this point on, EP Hard Disk will protect your newly encrypted partition or partitions in the background.

Decrypting a Drive

Decryption is a process by which an algorithm is used to return data to its normal state if the correct decryption key is provided. The data will be accessible to anyone who can access the computer. When you decrypt a drive, you are prompting EP Hard Disk to perform that process.

To decrypt a drive

1. Launch the EP Hard Disk User Program by double-clicking the icon in the status area of the Windows task bar, right-clicking the icon and selecting Open, or by launching through the Windows Start menu.
2. The EP Hard Disk User Program Main menu will display. Click the Decrypt Drives tab.

Note: If the tab is gray, either your EP Hard Disk Administrator has not allowed you to decrypt your drives or there are no encrypted partitions on your hard drive.

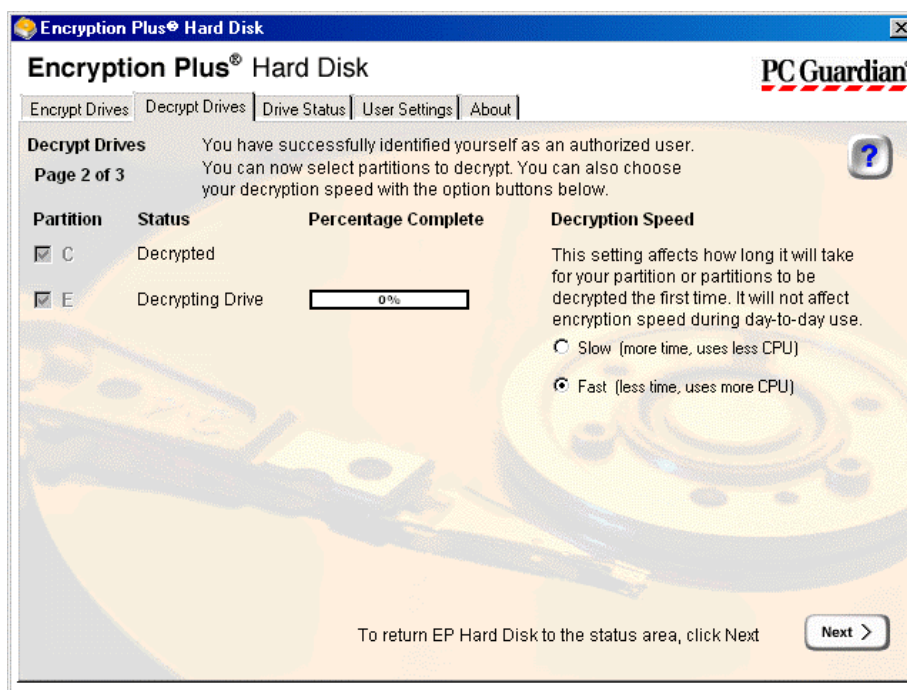


Figure 8—Decrypt Drives

3. At the prompt, type your EP Hard Disk User Name and Password. Click Next.
4. The Decrypt Drives screen will display. Select the partition or partitions that you would like to decrypt by clicking the checkbox next to the drive letter. The EP Hard Disk Administrator will have set a speed of Fast or Slow. If the EP Hard Disk Administrator has set the decryption speed to Fast, your computer may run more slowly than usual. If the EP Hard Disk has set the decryption speed to Slow, your computer will not run as slowly, but decryption will take longer. You can change the decryption speed while decryption is in progress.

If desired, change the speed setting and click Next. The decryption process will begin.

Encryption and Decryption

Notes: Click Next to minimize the EP Hard Disk User Program screen during decryption. To maximize the screen, double-click the EP Hard Disk icon in the status area.

If you will be using decryption in the background while working in other applications, save a backup copy of your work in a network folder.

The partition size and the EP Hard Disk decryption settings may cause the progress bar to remain at a certain percentage for a long period of time. Check the [Performance Monitor](#) if you want to make sure that the process is running.

Important: Selecting all partitions for decryption will not remove the EP Hard Disk User Program from your computer.

5. When the decryption process is complete, you will see a Success screen. EP Hard Disk will no longer protect the decrypted partition or partitions.

Checking the Drive Status

The Drive Status screen will display the encryption status for up to eight partitions.

To check the drive status

1. Launch the EP Hard Disk User Program by double-clicking the icon in the status area of the Windows task bar, right-clicking the icon and selecting Open, or by launching through the Windows Start menu.
2. Click the Drive Status tab. The Drive Status screen will display.

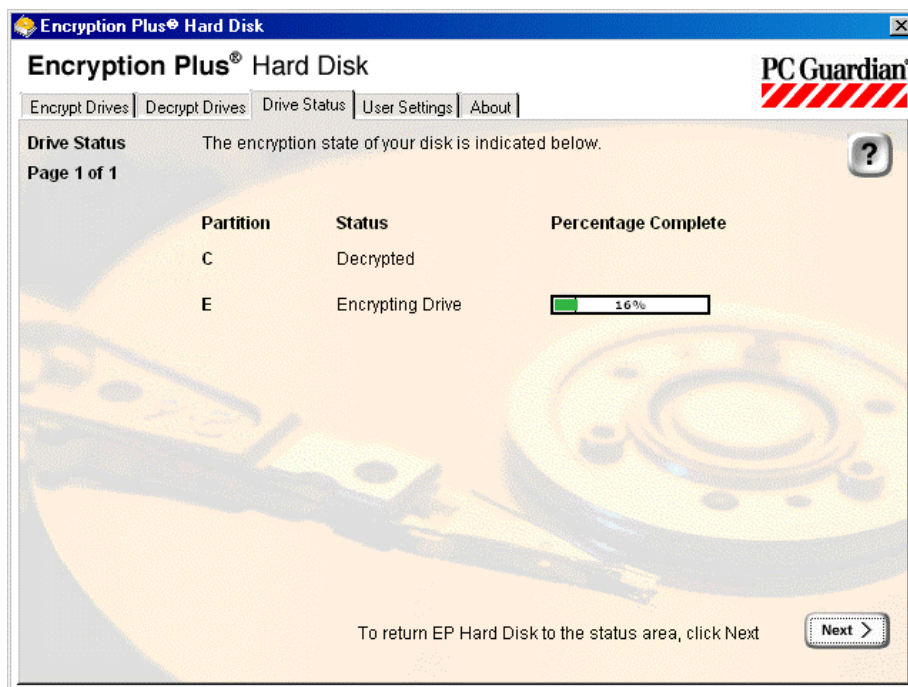


Figure 9—Drive Status

Encryption and Decryption

- Each partition on your hard drive will be listed as encrypted or decrypted. If you are checking the drive status while encryption or decryption are taking place, the Drive Status screen will indicate that encryption or decryption are in progress and a progress bar will display the percentage completed.

Note: The size of the partition that is being encrypted or decrypted and the EP Hard Disk encryption settings may cause the progress bar to remain at a certain percentage for a long period of time. Check the [Performance Monitor](#) if you want to make sure that the process is running.

- Click Close to go back to the EP Hard Disk User Program Main menu.

Performance Monitor

The Performance Monitor is a utility that provides a detailed visual reference of the encryption and decryption processes. If the progress bar stays on a certain percentage for a long time, or you just want to make sure that EP Hard Disk is performing the specified process, the Performance Monitor will provide confirmation.

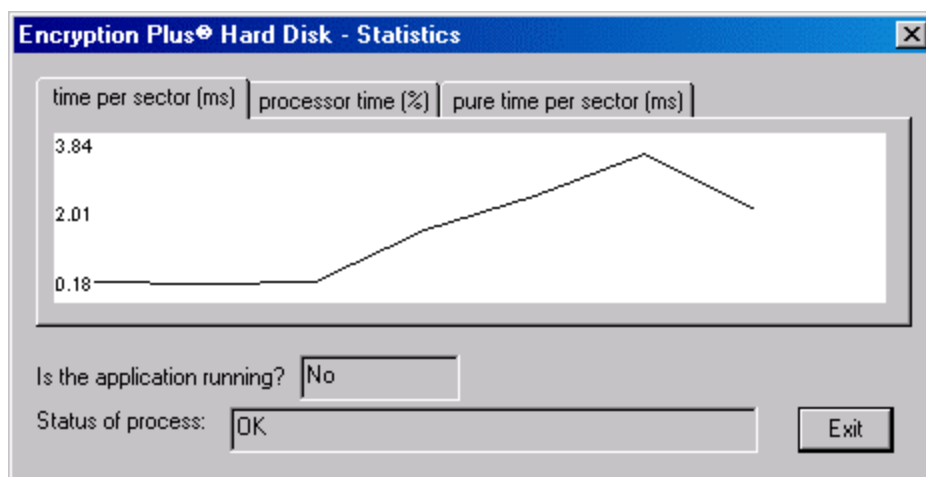


Figure 10—Performance Monitor

To access the Performance Monitor, right-click the EP Hard Disk icon in the status area and select Performance.

There are three tabs on the Performance Monitor. Each graph shows a different technical aspect of the process; but all of the graphs indicate that EP Hard Disk is encrypting or decrypting the partition or partitions. About every five seconds, the graph will extend to the next point. The field next to *Is the application running?* indicates that, at that moment, EP Hard Disk is encrypting or decrypting part of your hard drive. It is normal for the field to display "No" intermittently. The field next to *Status of process* will indicate "OK" unless an error has occurred during the encryption or decryption process.

Recover Program

If power is lost during the encryption or decryption process, or an error prevents access to your workstation, the Recover Program should be run. There are two options: to try to gain emergency access to the computer, or to gain access to the computer and perform emergency decryption of the entire hard drive.

Important: Contact a program administrator for assistance with the Recover Program.

Creating a Recover Disk

Make a recover disk before completing the encryption process, if possible. If your computer has encountered a serious error and cannot load windows, the recover disk serves as a bootable disk and allows you to use the EP Hard Disk recover process to access your hard drive or start emergency decryption.

You must have a blank floppy disk and a disk label in order to complete this procedure.

Important: The recover disk cannot be made on a CD-ROM. A floppy disk must be the initial bootable disk.

1. Insert the floppy disk into the A:\ drive.
2. Double-click the MakeRecoverFloppy.exe in:

[Path]\Recover, where Path is the location of the User Program Setup files, or

C:\Program Files\Encryption Plus Hard Disk Administrator.
3. Follow the on screen prompts. The program will format the disk and copy two EP Hard Disk files to complete the process.
4. To verify that all of the files you need have been copied, in Windows Explorer, browse to the A:\ drive. The following files should be included: Command.com, Ephdxlat.bin, Io.sys, Msdos.sys, and Recover.exe.
5. Label and date your recover disk so that you can find the disk quickly if you experience a problem.

You can use the recover disk on any computer that has the same version number of EP Hard Disk installed.

Encryption and Decryption

Running the Recover Program

If your computer has encountered a serious error and you cannot load Windows, use the following instructions to regain access to data on your hard drive or perform an emergency decryption of the entire hard drive.

Important: Users should contact a program administrator for assistance with the recover process.

1. Insert the recover disk into the disk drive and, using the Reset button on the workstation, restart your computer.
2. At the A:\ prompt, type recover

Example: A:\recover

3. The following instructions will display:

You have activated the recover program for EP Hard Disk. To regain access to the files on your hard drive through Windows, type Recover.exe /A after the A:\ prompt. If you have been unable to access your workstation in previous attempts, want to perform an emergency decryption of your hard drive, or both, type Recover.exe /D after the A:\ prompt.

4. At the A:\ prompt:

Type Recover.exe/A to regain access to your computer; or

Type Recover.exe /D to perform an emergency decryption of all encrypted partitions on your hard drive.

5. The process will launch. Follow any additional instructions that display. These instructions will vary depending on which process you are running, as well as whether or not you need to use a password recovery method.
6. If you are able to regain access to your computer, be sure to change your user name and password.

If you have performed an emergency decryption, the EP Hard Disk User Program should be uninstalled from your computer. The User Program can then be re-installed and the partitions re-encrypted.

Chapter Six

FORGOTTEN PASSWORDS

This chapter describes the two different methods you can use if you have forgotten your EP Hard Disk User Name or User Password, or both.

Authenti-Check uses question and answer pairs that you created during the initial EP Hard Disk Program setup. If you answer the questions correctly, you will be able to assign yourself a new EP Hard Disk User Name and Password and log on to your computer.

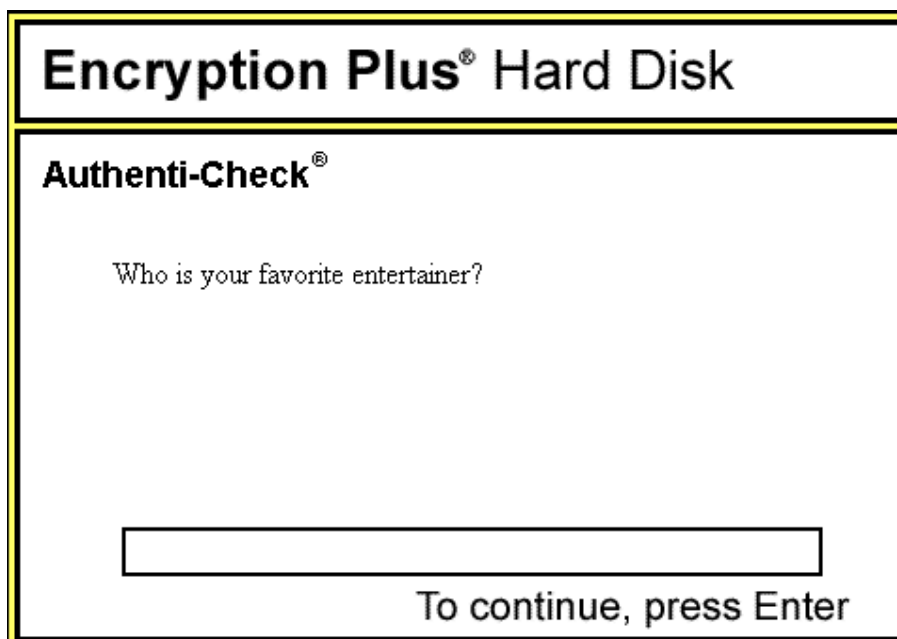
One-Time Password is a recovery method that requires you to communicate with a program administrator or a Help Desk technician. When One-Time Password activates, EP Hard Disk will display a series of numbers that you will give to the technician. The technician will then use those numbers to generate a key that will temporarily authenticate you to EP Hard Disk, which will allow you to create a new User Name and Password.

If the EP Hard Disk Administrator has enabled both Authenti-Check and One-Time Password, Authenti-Check will be the first password recovery method displayed.

Using Authenti-Check

If you cannot enter your User Name and Password successfully after the number of attempts set by the EP Hard Disk Administrator for lockout, the Authenti-Check process will begin on the next screen.

1. After an introductory screen, the first Authenti-Check question will display.



Encryption Plus® Hard Disk

Authenti-Check®

Who is your favorite entertainer?

To continue, press Enter

Figure 11—Authenti-Check Question

Enter your answer to the question.

2. Depending on how the questions were originally set up, Authenti-Check will display one to three questions. Type the answers to the questions exactly the same way that you did when you set up Authenti-Check. After you type an answer, press Enter to go to the next question
3. Once you have answered all of your questions correctly, EP Hard Disk will prompt you to enter and confirm a new User Name and Password, which will replace the password that you have forgotten.
4. If you are unable to successfully answer all of the Authenti-Check questions, and your EP Hard Disk Administrator has also enabled this function, the One-Time Password Process will start. If the EP Hard Disk Administrator did not enable One-Time Password, a screen will instruct you to restart your computer and contact a program administrator.

Notes: To restart your computer, you will need to press the reset button on the computer itself. Turning the computer off and on with the power button is not recommended. Ask your Help Desk or program administrator for assistance if you do not know the location of the reset button.

Forgotten Passwords

Completing the Authenti-Check process may affect Single Sign-On. Contact your program administrator after you have successfully changed your user name and password and use Single Sign-On.

Using the One-Time Password Program

The One-Time Password Program generates unique numbers each time EP Hard Disk activates it. When the numbers are entered in an administrative program, a process called Elliptical Curve Cryptography is used to generate a One-Time Password.

To use the One-Time Password Program

1. If you are unable to answer your Authenti-Check questions successfully, or the EP Hard Disk Administrator did not enable Authenti-Check, the One-Time Password Program will display a message that will designate a person to contact.
2. Contact the designated person and let the technician know that you need assistance with the EP Hard Disk One-Time Password Program.
3. The technician will ask you to read the series of numbers that appears on your screen.
4. After you have finished reading the numbers, click OK to go to the next screen, which will contain a number of blank data entry fields.
5. Listen carefully and type the series of numbers the technician will read to you in the blank data entry fields.
6. The administrator may ask you to read a “checksum” number that displays under each data field. There is also a checksum for the entire number series, which displays near the bottom right corner of the screen. A checksum is another way of confirming that the numbers are correct and does not represent the sum of the numbers you typed.
7. If all of the numbers have been entered correctly, after you click OK, you will be prompted to enter and confirm a new User Name and User Password, which will replace the User Name and Password that you have forgotten.
8. If you did not enter the numbers correctly, you should contact a program administrator and restart your computer.

Note: To restart your computer, you will need to press the reset button on the computer itself. Turning the computer off and on with the power button is not recommended. Ask your Help Desk or program administrator for assistance if you do not know the location of the reset button.

Chapter Seven

UPDATE SETTINGS

This chapter will show you how to update your User Name and User Password settings in the EP Hard Disk User Program, if your EP Hard Disk Administrator has allowed you to change them. If changing the settings is not allowed, the Update Settings tab will be gray and you will not be able to access the Update Settings screen. The EP Hard Disk Administrator can also choose to allow you to change only one of these settings. In this case, the Update Settings tab will be accessible, but the checkbox for the disallowed setting will not be available.

Only a program administrator can update all other settings.

Updating Your User Name

Following these instructions will change your User Name. Your User Name is updateable at any time.

- ❑Important:** If you use Single Sign-On, contact your program administrator before changing your user password.

To update your user name

1. Click the User Settings tab. Type your current user name and password at the prompt and click Next.

The screenshot shows the 'Encryption Plus Hard Disk' application window. The 'User Settings' tab is selected, displaying a confirmation message and two sections for updating user information. The 'Change EP Hard Disk User Name' section has two input fields, both containing 'Nick', with a note 'Your user name must be 3 to 30 characters'. The 'Change EP Hard Disk Password' section has two input fields, both containing '****', with a note 'Your password must contain: 1 - 32 characters'. A 'Next >' button is located at the bottom right, and a note 'To submit your settings, click Next' is positioned above it.

Figure 12—Update User Settings

2. Click the checkbox next to the Change User Name heading.
3. Type and confirm your new User Name.
4. If allowed, you can [update your User Password](#) at the same time.
5. To confirm your changes, click Next. A success screen will display.
6. Click Next to return to the EP Hard Disk User Main menu.

Updating Your User Password

Following these instructions will change your User Password. Your User Password is updateable at any time.

- Important:** If you use Single Sign-On, contact your program administrator before changing your user password.

To update your user password

1. Click the User Settings tab. Type your current user name and password at the prompt and click Next.
2. Click the checkbox next to the Change User Password heading.
3. Type and confirm your new User Password.
4. If allowed, you can [update your User Name](#) at the same time.
5. Click Next to confirm the change to your User Password.

Note: If allowed, you can change the User Name and User Password at the same time.

Chapter Eight

UNINSTALLING

Following these instructions will remove the EP Hard Disk User Program from your computer.

Note: Decrypting all of your partitions will not uninstall EP Hard Disk.

Important: You should make sure that all of your partitions were decrypted. Check the Drive Status screen.

1. From the Start menu, select Settings then Control Panel.
2. In the Control Panel window, double-click Add/Remove Programs.
3. At the Install/Uninstall tab, select EP Hard Disk from the list of programs and click the Add/Remove button.
4. EP Hard Disk will be removed from your computer.

APPENDIX A

Glossary

Administrator Program	Installed by the EP Hard Disk Administrator, this portion contains all of the administrative functions of EP Hard Disk, including: create User Program Setup, create Corporate Administrator, create Local Administrator(s), and change user settings. Encryption/decryption processes do not take place in the Administrator Program.
Authenti-Check	A password recovery method that uses a question/answer format for users to authenticate themselves and regain access to their computer.
Corporate Administrator	Has the ability to log on to any users' workstation and access all functions.
Decrypt Drive	Reverses the encryption process on one or more drives. EP Hard Disk no longer protects the data.
Drive	A portion of the entire hard disk, also known as a partition. EP Hard Disk can encrypt up to eight partitions that, in any combination, total one terabyte in size.
Drive Status	An EP Hard Disk screen that allows users to see which drives are encrypted or not encrypted on their computer.
Encrypt Drive	Begins the encryption process on one or more drives.
Encryption Speed	<p>A setting that regulates the amount of the computer's resources allocated to encrypting/decrypting drives.</p> <p>If set to "Fast," the encryption/decryption process will take less time, but the process takes up more of the computer's processing ability. Other programs may run more slowly while the encryption/decryption process runs in the background.</p> <p>If set to "Slow," the encryption/decryption process will take more time, and less of the computer's processing ability will be taken up by the encryption/decryption process. Other programs can be used more easily while the encryption/decryption process runs in the background.</p>
EP Hard Disk Administrator	Is responsible for installing the Administrator Program and creating the User Program Setup. Is also able to define the Corporate Administrator password and any Local Administrator names and passwords. Has the ability to modify User Settings.

Glossary

Local Administrator	Is able to log on to and access all functions on any users' computer within the limits placed by the EP Hard Disk Administrator.
Local Installation	A standard installation, requiring either the user or a technician to be physically present at the computer to install EP Hard Disk. The user can choose which partitions to encrypt.
One-Time Password	A challenge-response password recovery method that requires users to contact an administrator or help desk. The user provides a set of numbers to the technician, who then generates a One-Time Password key and returns it to the user. The user will be able to change their password and regain access to their computer.
On-The-Fly Encryption/Decryption	The encryption/decryption process that occurs after initial encryption. When you access data on an encrypted partition, only that part of the hard drive is decrypted and then re-encrypted when the file is closed.
Password Management	Settings that the EP Hard Disk Administrator can use to set users' password parameters. These include password length, password reuse, expiration, required special characters, and number of invalid logon attempts before lockout occurs and activates Password Recovery.
Password Recovery	If a user forgets the password, EP Hard Disk allows the user to regain access to their computer with Authenti-Check, One-Time Password, or both.
Password Synchronization	An additional setting for Single Sign-On that synchronizes the EP Hard Disk password to match changes made to the Windows password. The setting allows the user to only have to remember one password.
Program Administrator	A shortened term that, when used, means the EP Hard Disk Administrator, Corporate Administrator, or Local Administrator.
Remote Silent Installation	Allows the EP Hard Disk Administrator to use a network script to install the User Program (via the User Program Setup) without being physically present at the computers.
Single Sign-On	Combines the logon process for Windows and EP Hard Disk.
Status Area	The area on the Windows task bar that contains the system time and various icons. Also known as the system tray.
Update Settings	Allows the EP Hard Disk Administrator to change user settings and create an update file without creating a new User Program Setup. The following settings are modifiable: Corporate and Local Administrator passwords, password management, user settings, and user program messages.
User Program Messages	Messages that display for the user after installation, at logon, or when One-Time Password Recovery activates. The EP Hard Disk Administrator can use a customized message or choose the default.

Glossary

User Name	Associated with the user password, the name selected by the user for logon.
(User) Password	Associated with the user name, the password selected by the user for logon. May be required to fit certain parameters, such as minimum length and special characters, set by the EP Hard Disk Administrator.
User Program	This portion of EP Hard Disk is where—depending on parameters set by the EP Hard Disk Administrator—the user can encrypt/decrypt drives, check the encryption status of their drives, and change selected settings.
User Settings—Administrator Program	When defined by the EP Hard Disk Administrator during creation of the User Program Setup, includes the user's ability to change their password, decryption rights, Single Sign-On, and default encryption speed. After installation of the User Program Setup, the EP Hard Disk Administrator can use update settings to change these and other parameters.
User Settings—User Program	If allowed by the EP Hard Disk Administrator, allows the user to change their EP Hard Disk user name and password.
User Program Setup	Installs the User Program with the parameters set by the EP Hard Disk Administrator. Created by the EP Hard Disk Administrator in the Administrator Program.

APPENDIX B

Tables of Parameters

Password and Name Parameters

Password/Name	Minimum Length	Maximum Length
User name	3	30
User password (if set by administrator)	1-24	32
User password (if not set by administrator)	6	32

Password Recovery Parameters

Type	Minimum Length	Maximum Length
Authenti-Check question	1	99
Authenti-Check answer	set by administrator†	24
One-Time Password fields	5‡	5

†—if the administrator does not define a number, the default is seven

‡—only the last One-Time Password field can be less than five digits

APPENDIX C

Guidelines for Creating Authenti-Check Questions

Creating authentication questions can be challenging. There is often a real conflict between creating questions to which you can provide unique answers, and, at the same time, creating questions to which you will *remember* the answers. To that end, the following examples represent questions that are relatively secure, as well as questions that could compromise your company's system security by being easy for an intruder to guess or find the information.

Tips: Select questions to which the answers are not public information, easily guessed, or easy to research. For example, "What is your spouse's name?"

Try to choose questions to which there could be many answers. For example, "What day of the week do you go grocery shopping?" has only seven possible answers.

Relatively Secure Questions

- What was your first pet's name?
- What is your Employee ID Number?
- What is your favorite novel?
- Who is your favorite entertainer?
- What is the street name where your favorite relative lived?
- Who was your childhood hero?

Risky Questions

- What is your mother's maiden name?
- What is your Social Security Number?
- What is your spouse's/child's/pet's name?
- Where were you born?
- What is your birthday?
- What kind of car do you drive?

APPENDIX D

Technical Support

If you need assistance or have any questions about Encryption Plus® Hard Disk, please contact your help desk or the appropriate program administrator.