DiskGuard 2

User Manual

http://www.intego.com

DiskGuard for Macintosh

Intego.

www.intego.com

TABLE OF CONTENTS

INTRODUCTION

Welcome to DiskGuard™! We hope this software will give you complete satisfaction.

OVERVIEW

Nearly all Macintosh users are confronted daily with security problems. Although the data on your computer is not always confidential, it is very often valuable information. You just can't imagine losing your financial records and customer files to your competitor, sharing all of your correspondence with your colleagues at work, or having your latest project trashed by your six-year old. Not to mention burglars who like Macintosh as well…

DiskGuard has been developed to keep your work safe without getting in your way. With DiskGuard, you can protect any hard disk connected to your Macintosh and prohibit unauthorized access.

TWO LEVELS OF PROTECTION

If you are the only person working on your Macintosh, you can protect your computer by typing in one password. That's all there is to it. If your computer is shared with other people, give them a second password which limits the access, according to your own requirements, to certain days of the week or to specific hours during the day or prevents them from inserting disks into your Macintosh, etc.

PERMANENT SECURITY

At start-up, DiskGuard requests a password. No one will be able to access the Macintosh without supplying the proper password, even if he tries to start up with a System disk or if he holds the Shift key down. DiskGuard also keeps a close watch on your computer while you are at work: leave your desk for a few minutes and DiskGuard automatically hides your screen from prying eyes. As soon as somebody tries to access the computer, DiskGuard requests the password. DiskGuard also keeps track of valid and invalid access attempts to your hard disk so you can see at any time if somebody used the computer during your absence.

TECHNICAL SUPPORT

If you experience any problems, do not hesitate to contact the customer support department of your local representative. You will find his name and address on the DiskGuard program diskette (“Support” file). Before contacting them, please make sure you have returned your Registration Card and have your User Card by hand as well as the following information:

• **Version and serial numbers of the software you are using:** Click the DiskGuard logo in the DiskGuard screen. The version and serial numbers should also be on the User Card.

• **The type of Macintosh you are using.**

• **Version number of the System software you are using:** You can find this information under the Apple menu by selecting About This Macintosh…

Note for DiskGuard users over the network:

If you want to protect the hard disks of networked Macintosh computers, we recommend you use **DiskGuard™ Remote.** This application allows you to remotely install, remove, modify and update the protection, instantly lock hard disks over the network, etc.

DiskGuard Remote is fully compatible with DiskGuard. If you previously protected some of your computers with DiskGuard, you will also be able to access and configure them with DiskGuard Remote over the network. DiskGuard Remote is available in office packs and site licenses.

For further information on DiskGuard Remote, please contact
your local distributor (See “Support” file).

You can contact our support team by e-mail at **Support@intego.com**

DOCUMENTATION CONVENTIONS

The following conventions are used in this manual:

- **Bold typeface** is used to indicate button, pop-up menu and checkbox names.
- *Italic* typeface is used to indicate notes, warnings and important information.
- ***Bold italic*** *typeface* is used to indicate introductory sentences that guide you through the configuration process.

  These sentences typically begin with, “So far you have…You must now…”.

Note: *The graphics in this manual have been created using a specific software and hardware environment. As a result, they may differ slightly from the ones you see on your screen.*

CHAPTER ONE - INSTALLATION

REQUIRED CONFIGURATION

DiskGuard requires a Macintosh equipped with System 6.0.7 or later, 4 megabytes of RAM and at least one hard disk. See the Read Me file on the DiskGuard program floppy for up-to-date details on system requirements and compatibility.

INSTALLING DISKGUARD

Note: *Before installing DiskGuard 2.0,remove all older components remaining from a previous version.*

Read this section if you are installing DiskGuard for the first time:

1.1 How to install DiskGuard 2.0

Step 1

- **Web version installation**

Once you have downloaded the program (if you own the web version), you should see a small Stuffit (from Aladdin Software) icon. It is a compressed file that looks like one of the following two pictures.

Or

Double-click on the icon or open this file using Stuffit Expander which is located on your hard-drive then proceed to step 2.

- **CD-Rom version installation**

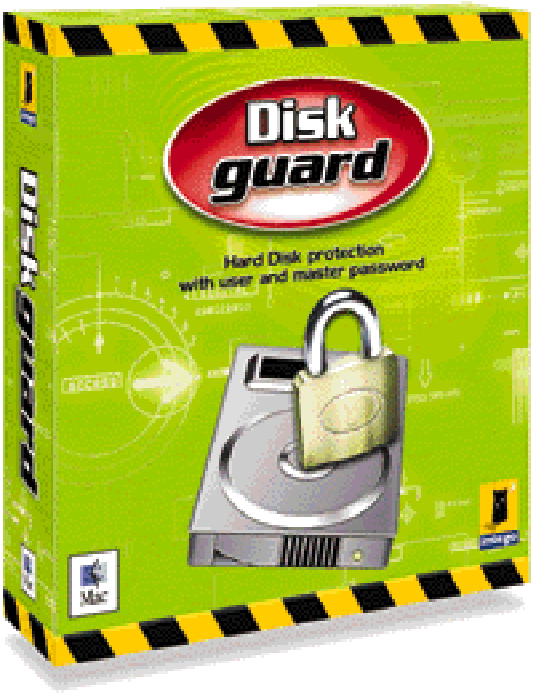
Insert the CD-Rom in your computers's CD-Rom drive. Proceed to step **2.**

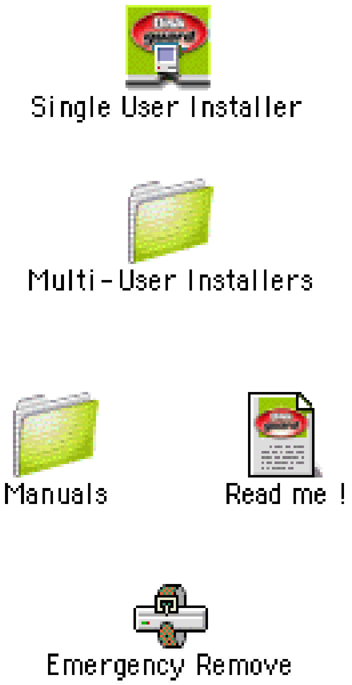
Step 2

The following icon will appear on your desktop :

DiskGuard 2.0

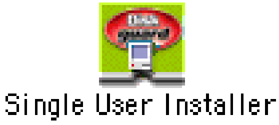
Double-click on it. A window will open containing the installer icon, Two PDF manual icons and a read me icon.



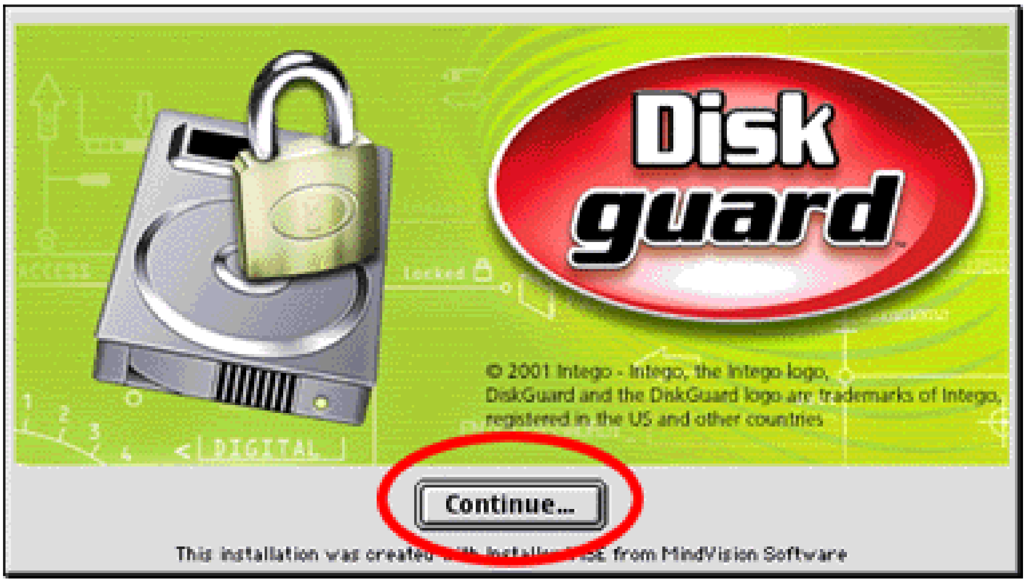


Double-click on the DiskGuard installer icon **(1)**.

When you see this splash screen **(2)**,click continue.



(1)



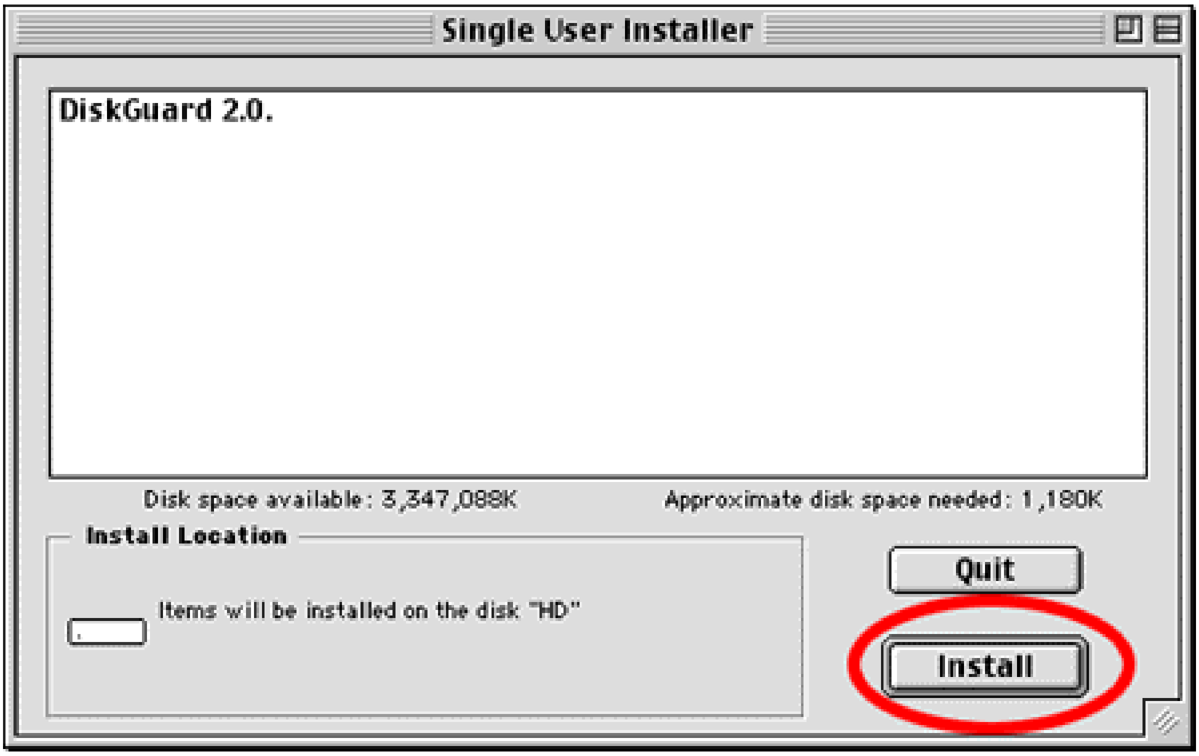
© 2001 Intego - Intego, the Intego logo, DiskGuard and the DiskGuard logo are trademarks of Intego, registered in the US and other countries

This installation was created with Installer VISE from MindVision Software

(2)

The Diskguard license will appear. Read this license carefully, and, if you accept it, click on accept.

You will now see the following window. You can select the easy install which installs DiskGuard 2.0.



Single User Installer

DiskGuard 2.0.

Disk space available: 3,347,088K

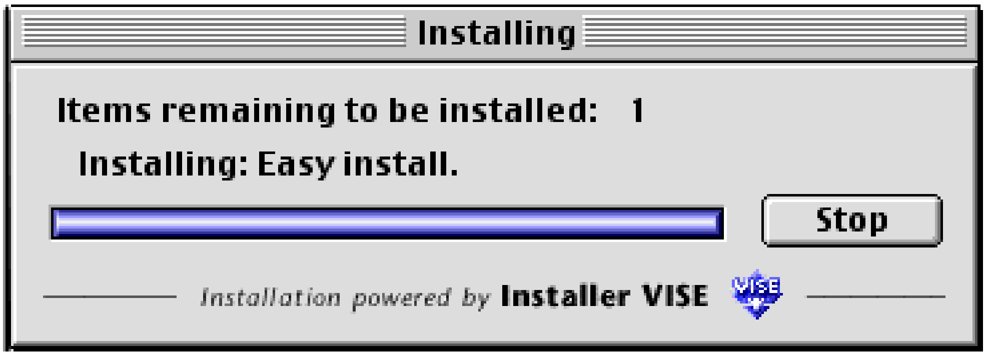
Approximate disk space needed: 1,180K

Install Location

Items will be installed on the disk "HD"

Click install to start the installation process.

During the installation process, a progress bar will be displayed.

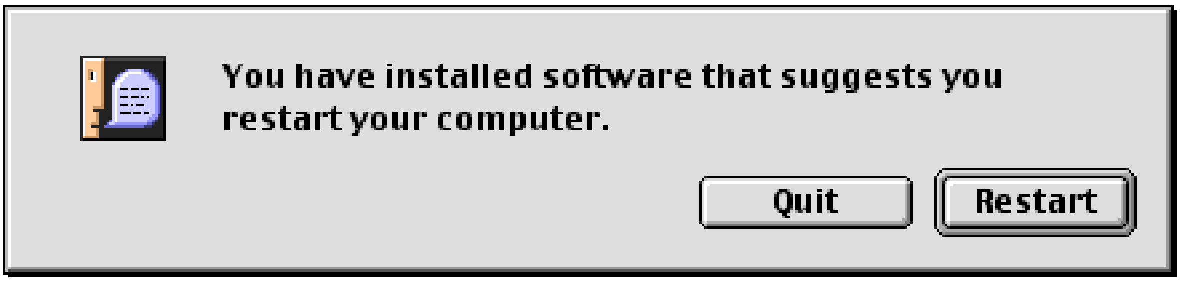


Installing

Items remaining to be installed: 1

Installing: Easy install.

When the installation is finished, you will be asked to restart the computer in order to be able to use the new software.



You have installed software that suggests you restart your computer.

Once you have restarted and your desktop appears, you can open your new software by selecting it in the control panels folder. You will be asked to register the program.

The serial number can be located on the **back of your CD jewel case** for the CD version or appears on your **purchase confirmation E-mail** for the web version.

You do not need the CD or the Archive after installing. Store it in a safe place together with your serial number for future installation.

Upgrading DiskGuard

Note: *Before upgrading your program, please remove all protections and DiskGuard extensions.*

For further details,please read our Quick install report or see the **Chapter One** in this manual.

Removing DiskGuard

For detailed instructions on the appropriate way to remove this version of DiskGuard, please consult the Read Me file located in the DiskGuard Installer.

Note: *Individual Idems, like Hard-drive and documents remain protected even after removing DiskGuard.*

You should remove the protection before uninstalling DiskGuard .

1) To Uninstall DiskGuard extensions, open your Control Panels folder and select the DiskGuard control panel. You may also want to remove the DiskGuard folder located into your hard drive.

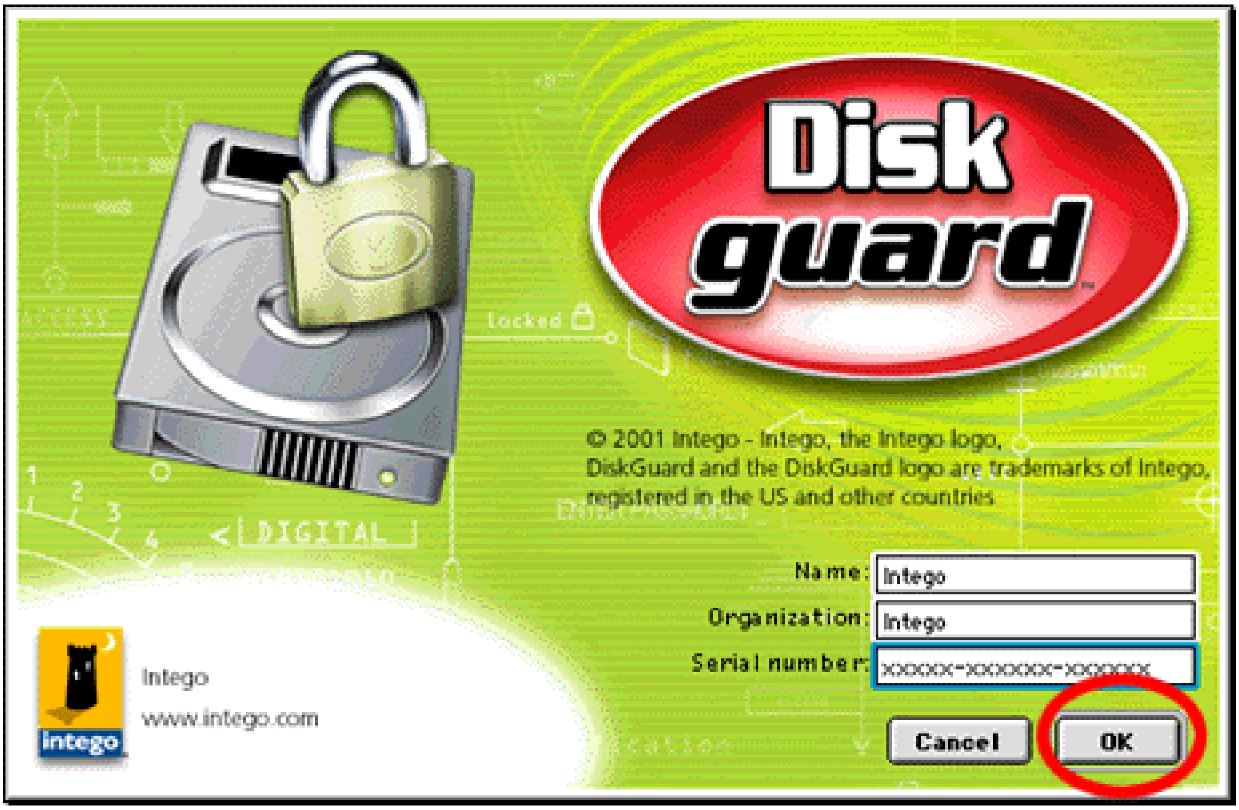
2) Drag them into the trash.

3) Restart your Macintosh.

4) Empty the trash once your computer has restarted.

Registering the program.

4. Enter your name, organization and the serial number you received with the program, then click OK.



© 2001 Intego - Intego, the Intego logo, DiskGuard and the DiskGuard logo are trademarks of Intego, registered in the US and other countries

Name: Intego

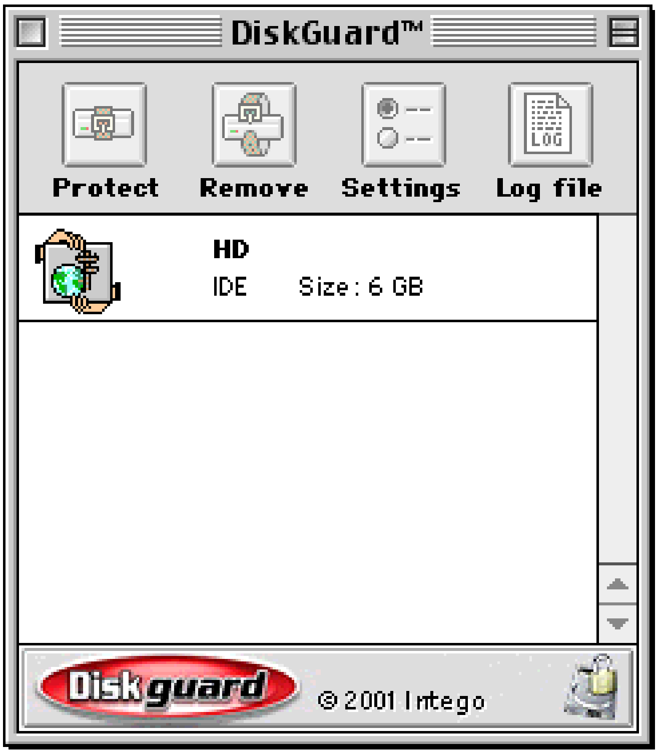
Organization: Intego

Serial number: xxxxx-xxxxxx-xxxxxx

6. If you are using System 6, open the desk accessory Control Panel under the Apple menu. In the left column, select the DiskGuard icon.

If you are using System 7 or upper, open the Control Panels folder and double-click the DiskGuard icon.

The DiskGuard control panel appears:



HD
IDE Size : 6 GB

The DiskGuard screen consists of two parts. The upper part shows the control buttons allowing you to protect, modify or remove the protection and to consult the log file.

The lower part lists all the hard disks connected to your Macintosh.

By clicking on the DiskGuard logo, a screen appears informing you of the version number of the software, your license number and our address.

CHAPTER TWO - PROTECTION

This chapter describes the protection procedure. It explains how to configure the Master password, screen lock, User password and user restrictions.

BEFORE PROTECTING A DISK

Before protecting a hard drive or a partition, we recommend you take the following precautions:

1. Make a backup copy of your data on another HFS volume (floppy disks, external hard disk, server, ...).

2. Check your hard disk.

A hard disk can contain minor defects that may cause problems when you try to protect it. Before protecting a disk, we recommend you check the state of your hard disk with a utility called Disk First Aid 1 . This utility is included on one of the System disks that comes with your Macintosh. For System 6 on the disk “Utilities 1”, for System 7 on the disk “Disk Tools”.

3. Remove all driver level compression utilities.

DiskGuard, like most other volume protection programs, cannot protect disks compressed with driver level compression utilities like Stacker®, Times Two®, … Therefore, we recommend you remove these utilities before attempting to protect a disk. File level compressors such as AutoDoubler™ and SpaceSaver™ should present no problem.

4. Remove all protection utilities.

To ensure proper access to your disk, we recommend you remove all other protection utilities you may have installed.

PROTECTION CONFIGURATION

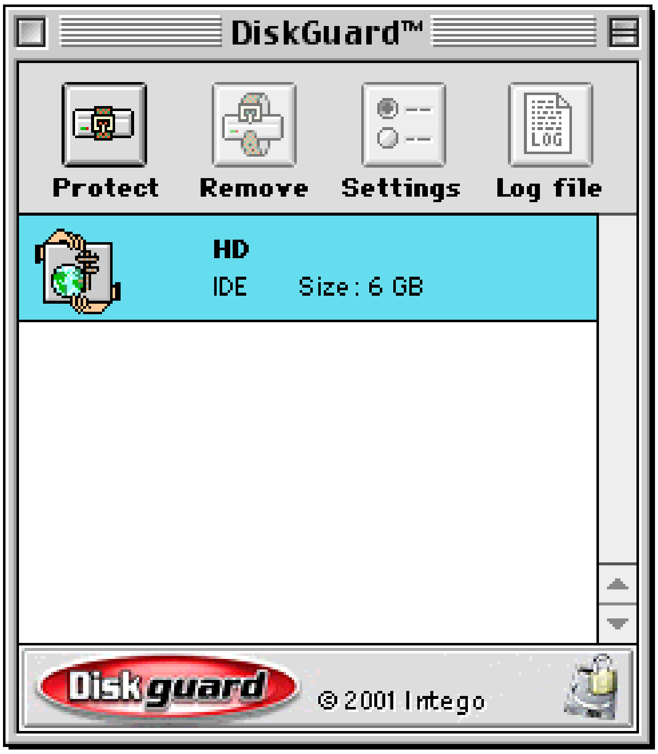
ABOUT PASSWORDS

DiskGuard offers two-level protection using two different passwords. The first password is the **Master password** which gives entire access to the protected hard disk(s) and DiskGuard's configuration (See below). If your Macintosh is shared with other people, give them a second password which limits the access to your disk(s). The second password or **User password** is optional (See page 21).

MASTER PASSWORD

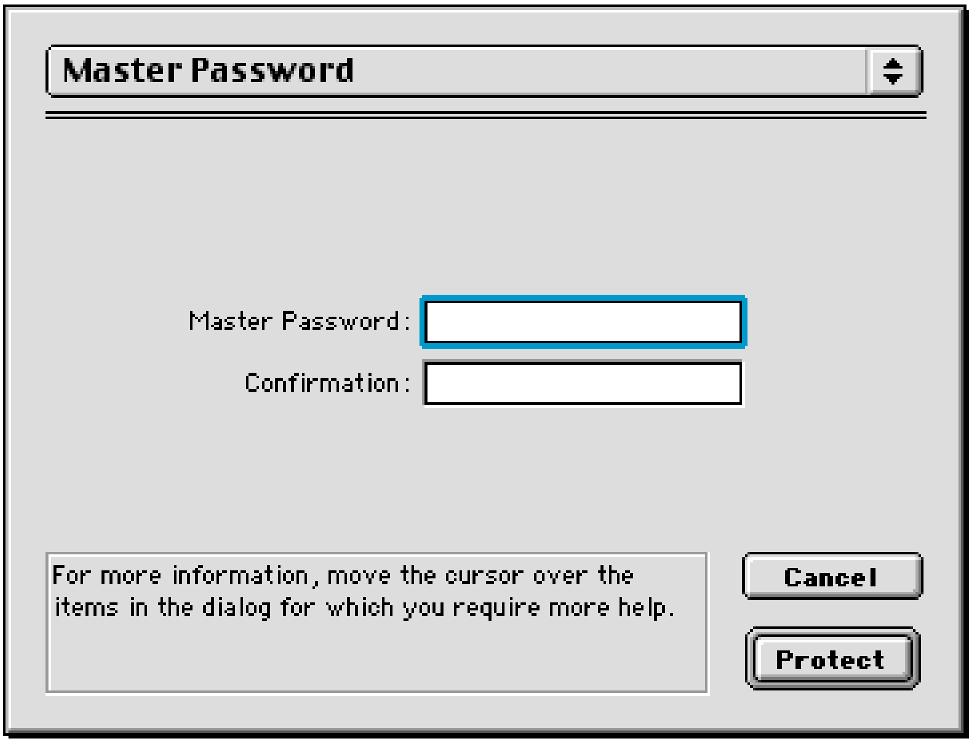
The hard disk is protected as soon as the Master password has been defined. Proceed as follows:

1. In the DiskGuard screen, select the disk you wish to protect and click the Protect button or double-click the selected disk.



To select multiple hard disks, hold down the Shift key (for consecutive disks) or the Command key (for non-consecutive disks).

The following screen appears:



For more information, move the cursor over the items in the dialog for which you require more help.

2. Enter the Master password in the first text box.

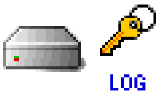
• The password may contain up to 31 characters. For security reasons, we recommend you define a password at least 4 characters long.

• Passwords are case sensitive (for example, “Secret”, is different from “secret” and “SECRET”). When defining a password, you may use odd capitalization to make it more difficult for others to guess your password (for example, “SeCreT”).

• Avoid using passwords which are easy to guess such as the name of the hard disk, names or birthdays of close relatives, … Opt for a celebrity’s name, an important event, your secret bankcode or a combination of letters and figures. Be creative!

3. Press the Tab key and type the password a second time to confirm it.

4. Click the Protect button or press the Return key to validate the protection of the hard disk.

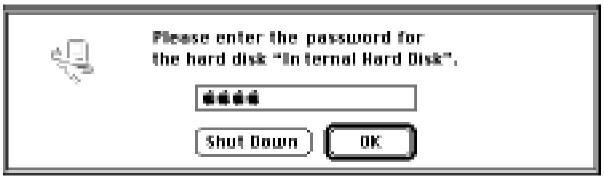


A key appears to the right of the protected hard disk icon in the DiskGuard screen indicating the disk is now protected with a Master password. The word “LOG” indicates that a log file is available. It registers all protection events of the disk and lists all valid and invalid access attempts (See “The Log file”, page 34).

USING PROTECTED VOLUMES

• From now on, DiskGuard will prompt for the **password** at each start-up.

- In the case of the start-up volume, DiskGuard will display the following window:

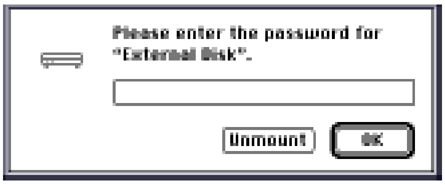


Please enter the password for the hard disk “Internal Hard Disk”.

Anyone not knowing the password will have no other choice but to shut down the Macintosh by clicking the Shut Down button.

Note: *Some types of Macintosh computers will shut down after three invalid attempts or after having displayed the above message for more than five minutes to avoid the Macintosh from remaining on unnecessarily.*

- For any other volume, DiskGuard shows the following window:



Please enter the password for “External Disk”.

Anyone not knowing the password can click the Unmount button to access the start-up volume or any other disk for which he does know the password.

Note: *A common mistake users make is attempting to enter a password with the Caps Lock key in the wrong position. To help you avoid any possible confusion, DiskGuard includes a small indicator to the right of the password box when the caps lock key is active (⇪).*

• As soon as a volume is protected, the screen lock settings become active to secure your data from prying eyes while the Macintosh is switched on.

Read more on the screen lock features on the following pages.

PROTECTING REMOVABLE VOLUMES

DiskGuard enables you to securely protect any mountable volume, including floppies and other removable media like SyQuest, Bernoulli, Zip, Jaz and magneto-optical cartridges. When a protected removable volume is inserted into a Macintosh running DiskGuard, it will immediately demand that disk’s password.

If the recipient is not a DiskGuard user, the volume will show a single file labeled “Open Me”. All other contents will be securely locked and invisible. Double clicking the Open Me file will inform the user that the disk is protected. It will then allow him to install a small extension enabling his Macintosh to read volumes protected by DiskGuard. After restarting, that user will be able to access the contents of any DiskGuard protected disk, as long as the correct password is known.

SCREEN LOCK

By using the screen lock feature, you can prevent access to your hard disk when you are away from your Macintosh while the computer is switched on.

After a predefined period of idle time or upon request, DiskGuard displays a security screen that hides the data. When somebody tries to access the computer, DiskGuard will request the password for all protected hard disks.

As soon as a hard disk is protected, the default settings of the screen lock will apply. To alter the settings or configure a screen lock keyboard shortcut:

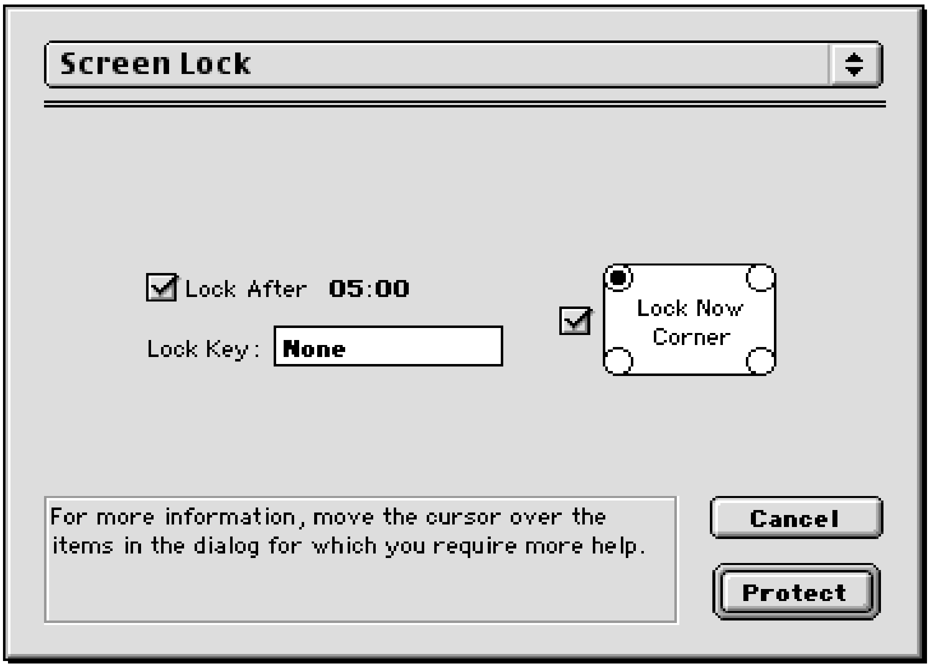
1. Select a protected hard disk in the DiskGuard screen and click the Settings button or double-click the hard disk’s icon.

To select multiple hard disks, hold down the Shift key (for consecutive disks) or the Command key (for non-consecutive disks).

You will be prompted to enter the password.

2. Enter the Master password and click the OK button.

The following screen appears:



For more information, move the cursor over the items in the dialog for which you require more help.

- **Lock After:** By default, the screen lock becomes active after five minutes of keyboard and mouse inactivity. To modify the settings, click on the minutes or seconds and enter another value.
  Except in some specific cases (for instance, if the Macintosh is consulted regularly in a public area), we recommend that you do not deactivate this feature because there is no use in protecting a hard disk if it can be accessed as soon as the user takes a moment's leave.

Note: *If several disks are connected to the same Macintosh and the period of idle time is defined differently for each hard disk, DiskGuard will automatically choose the smallest value.*

- **Lock key:** You can instantly lock the screen by using a lock key. To define this key, type any key combination with one or several special keys (Control, Option or Command) and a character (letter, figure, arrow, ...).

The function keys can be used separately or in combination with a special key. The Shift key can be used in combination with a special key or function key.

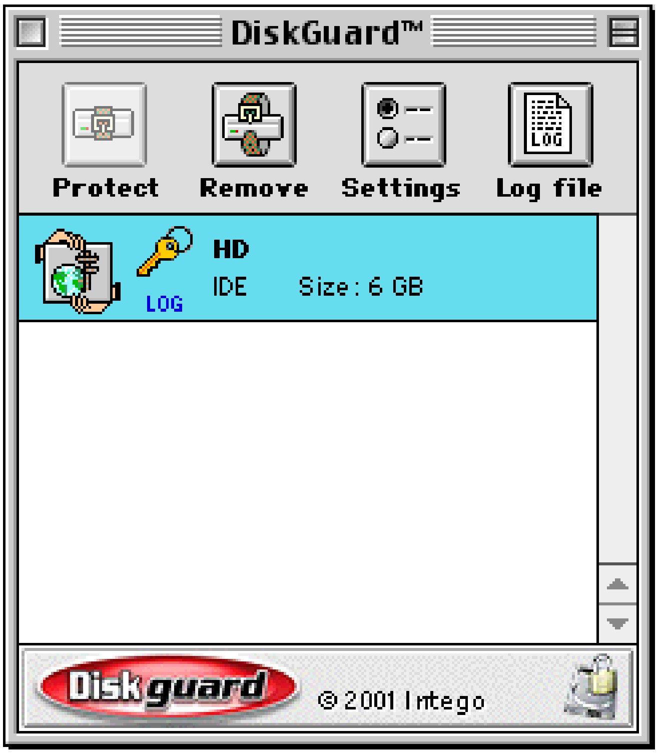
- **Lock now corner:** The screen lock may also be instantly activated by placing the cursor in a corner. The default lock corner is the upper left corner of the screen. You can define another corner or deactivate this feature.

Note: *You can use the After Dark ® screen saver together with DiskGuard's access protection. When you check the Lock after box, the password will always be required, even if After Dark is set to kick in before DiskGuard's screen lock.*

USER PASSWORD

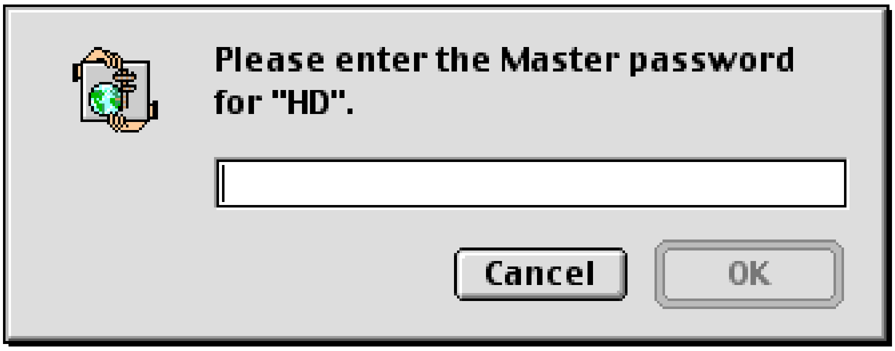
If you share your computer with other people, you can give them a second password. It will allow them to access the computer without being able to remove or change the hard disk protection. With this second password, you can also set up restrictions to limit access to the computer, for instance, prohibiting access after work hours or during the weekend, forcing a change of password after a predefined time of use, etc.
To configure the user password:

1. Select a protected hard disk in the DiskGuard screen and click the Settings button or double-click the hard disk.



You will be prompted to enter the Master password.

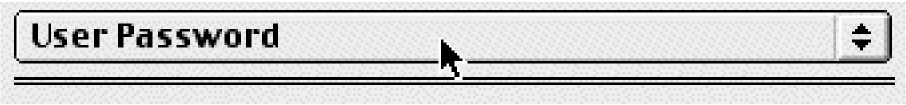
2. Enter the Master password and click the OK button.



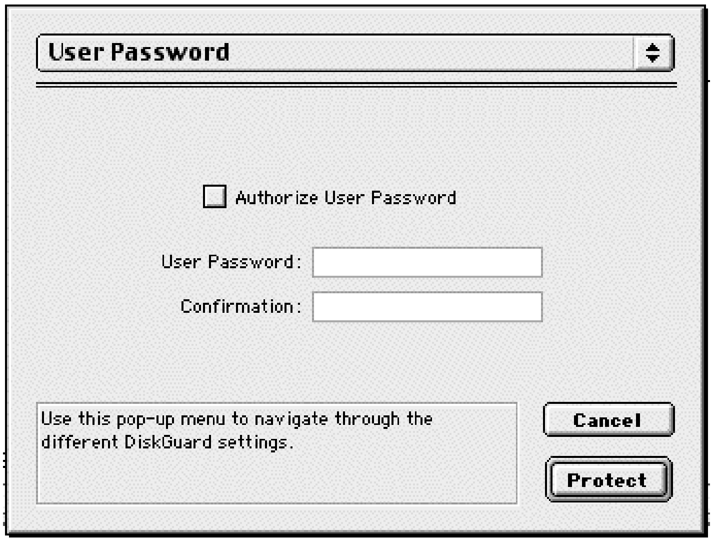
Please enter the Master password for "HD".

3. In the pop-up menu, select User Password.

You can also use the arrow keys to navigate through the pop-up menu.



The following screen appears:



☐ Authorize User Password

User Password:

Confirmation:

Use this pop-up menu to navigate through the different DiskGuard settings.

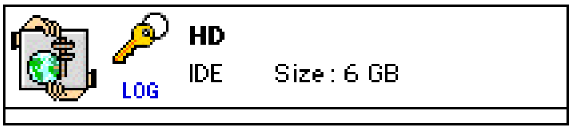
4. Check the box Authorize User Password.

5. Enter the User Password.

6. Press the Tab key and confirm the password.

7. Validate the User password by clicking the Save button or pressing the Return key.

A second key appears to the left of the hard disk icon in DiskGuard's screen indicating the hard disk is now protected with a Master password as well as with a User password.



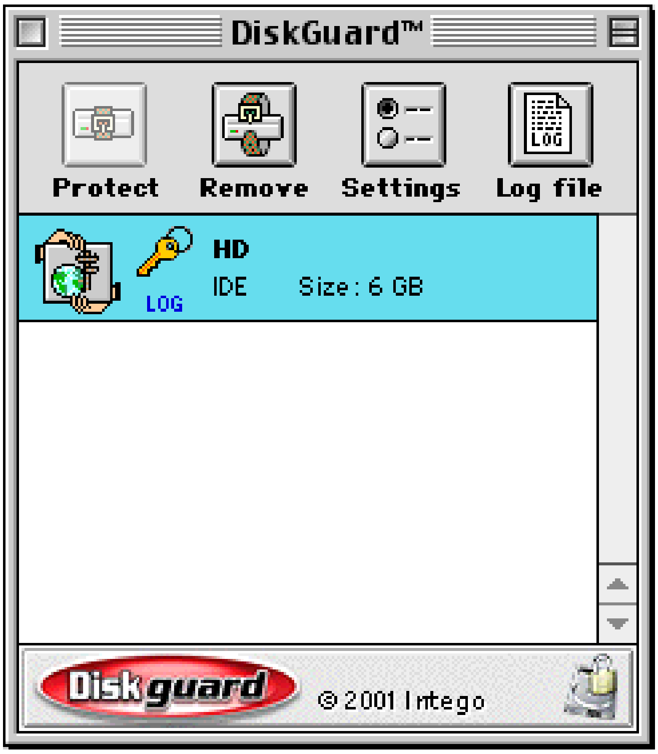
8. Give the User password to all potential users.

You also need to provide them with information on the screen lock settings so that they know how to lock the screen (idle-time period, lock corner, lock key) (See also page 15).

USER RESTRICTIONS

With DiskGuard, it is possible to restrict the privileges of the User and his password. You can, for example, limit the use of the User password in time, write-protect your hard disk, prevent diskette insertion, etc.
To configure these restrictions:

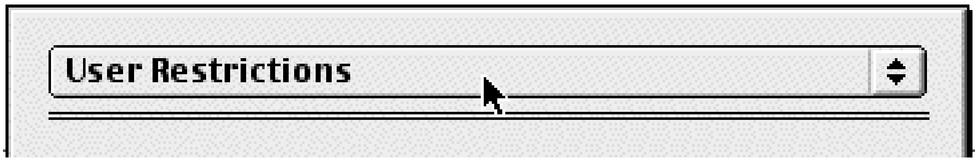
1. Select a protected hard disk in the DiskGuard screen and click the Settings button or double-click the hard disk.



You will be prompted to enter the Master password.

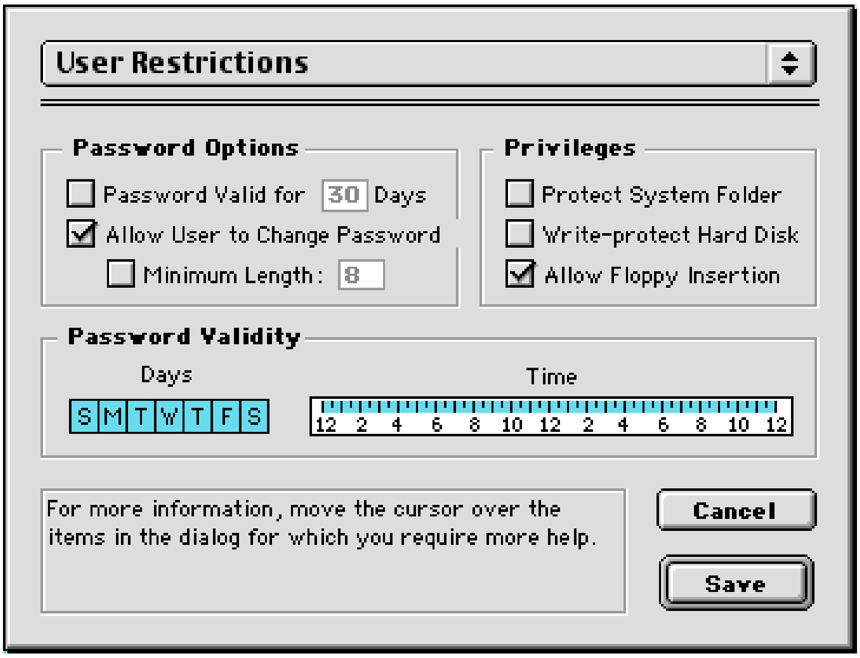
2. Enter the Master password and click the OK button.

3. In the pop-up menu, select User Restrictions.



You can also use the arrow keys to navigate through the pop-up menu.

The following screen appears:



User Restrictions

Password Options

□ Password Valid for 30 Days

☑ Allow User to Change Password

□ Minimum Length: 8

Privileges

□ Protect System Folder

□ Write-protect Hard Disk

☑ Allow Floppy Insertion

Password Validity

Days: S M T W T F S

Time: 12 2 4 6 8 10 12 2 4 6 8 10 12

For more information, move the cursor over the items in the dialog for which you require more help.

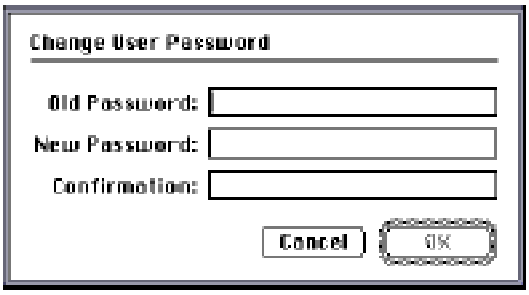
PASSWORD OPTIONS

- **Password Valid for ... Day**s: When this feature is active, the User password is valid only for the defined number of days. With this option the user can be forced to modify his password regularly, provided he has the privilege to do so (see “Allow User to Change Password”). To activate this option, check the box on the left and enter the number of days after which the user must define a new password on the right.

Note: *Once this option is checked, DiskGuard will remember all User passwords and prohibit the use of old passwords.*

- **Allow User to Change Passwor**d: For security reasons, we recommend you force the user to change his password regularly.

When this option is checked, the user can change the User password. He can do so after the password validity period has expired (See Password Valid for … Days, page 20) or each time the password is requested by clicking the Password button. The following screen appears:



Change User Password

Old Password:

New Password:

Confirmation:

Note: *In some cases, it may be useful not to allow the user to change the User password and to limit the validity of the User password to a certain number of days. For example, if a Macintosh is rented, the user will not be able to use the computer beyond the validity period of the User password. If you work with temporary personnel, they will not be able to access the computer once the User password has expired, …*

- **Minimum Lengt**h: When this box is checked, the User password must not be shorter than the defined number of characters. We recommend to define a User password that is not shorter than 4 characters. Short passwords are more easily guessed. To modify the required minimum length, type in another value.

PRIVILEGES

- **Protect System Folder**: All folders on a protected hard drive, including the System Folder, can be protected via the Protect Folder command in the File menu (See “Protection is removed”, page 27). Protecting the System Folder prevents any modification of its contents.

Note: *Unlike other protected folders, the System Folder’s icon remains visible to users even when protected.*

- **Write-protect Hard Disk**s: By default, a user can save or copy files onto the protected hard disk. When this box is checked however, the user will only be able to read the data on the hard disk but will not be allowed to change the hard disk contents. Each time the user wants to save or copy a file onto the hard disk, a message will appear informing the user he does not have the privilege to do so.

Important: *If you want to write-protect a start-up hard disk or a hard disk containing applications, we would advise you to make some preliminary tests before making the disk accessible to the users. The System and some applications may need to write temporary or preferences files to the hard disk in order to function properly. If this is the case, the hard disk must not be write-protected.*

- **Allow Floppy Insertio**n: This option is checked by default to enable the user to insert diskettes. If you do not want the user to insert diskettes in the disk drive, uncheck this option. This feature can be useful if you do not wish your files to be copied. It is also an efficient method of preventing virus introduction. Each time the user tries to insert a disk, a message will appear informing him he does not have the privilege to do so and the diskette will be ejected immediately.

Note: *If the user is not allowed to insert disks and he introduces a System disk at computer start-up, he will have access to the Macintosh but not to the hard disks which do not allow floppy insertion.*

PASSWORD VALIDITY

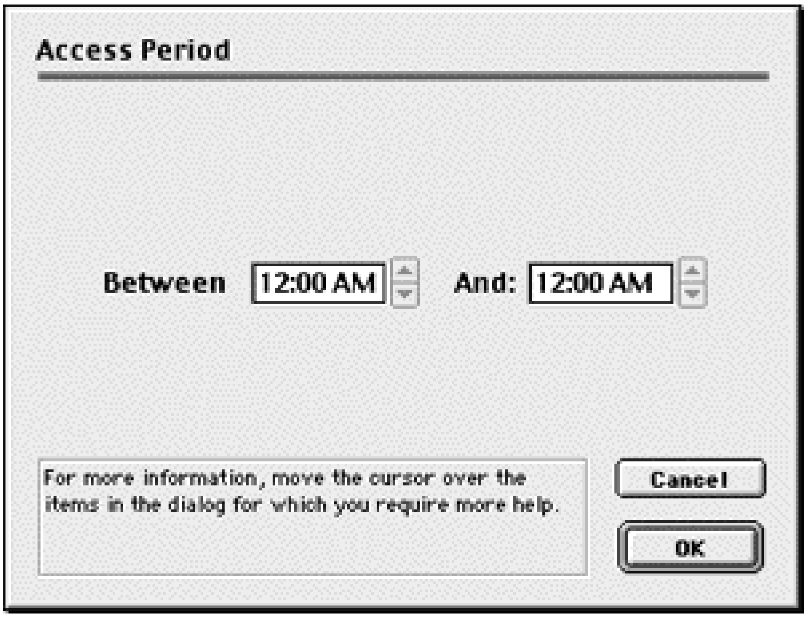
The following features restrict the use of the User password in time.

Note: *As soon as one of these three options is active, the internal Macintosh clock can no longer be modified by the users accessing the hard disk with the User password.*

- **Days:** You can enable the User password on certain days only, for example from Monday to Friday. The highlighted boxes indicate the days on which the user is allowed to access the disk.

- **Time**: You can authorize the user to access the disk during a certain period of the day only, for example during work hours. The user will be notified in advance that the disk will shut down at a specific time. Drag the pointer from the starting hour to the finishing hour.

To define a more precise time zone, double-click the time table. The following dialog box appears:



Access Period

Between 12:00 AM And: 12:00 AM

For more information, move the cursor over the items in the dialog for which you require more help.

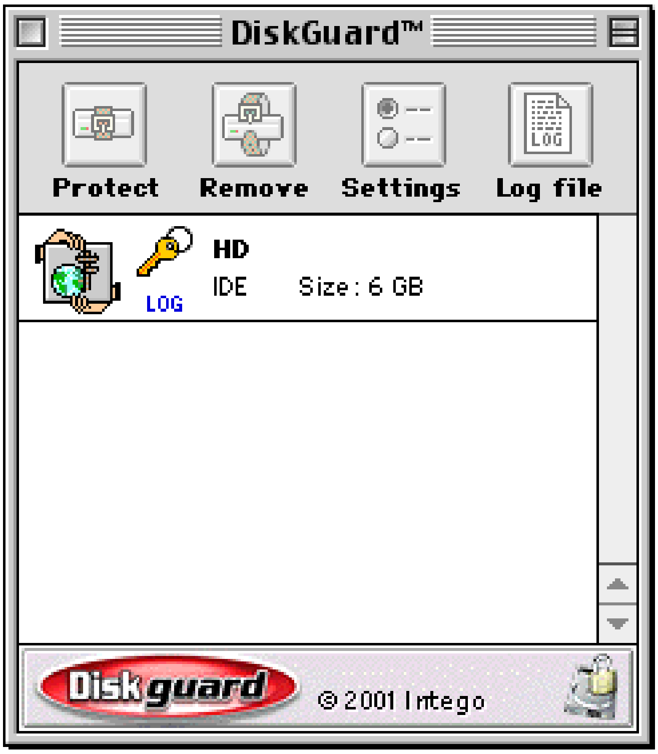
To modify the time zone, click on the hours or minutes and enter a new value or use the up and down arrows.

OPTIONS

DiskGuard includes some additional options for PowerBook owners as well as for users of remote access software.

To configure these options:

1. Select a protected hard disk in the DiskGuard screen and click the Settings button or double-click the hard disk.



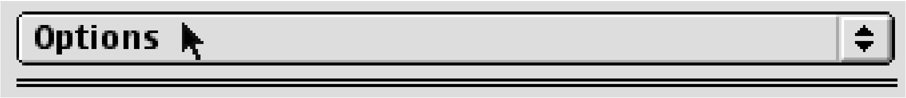
HD
IDE Size : 6 GB

You will be prompted to enter the Master password.

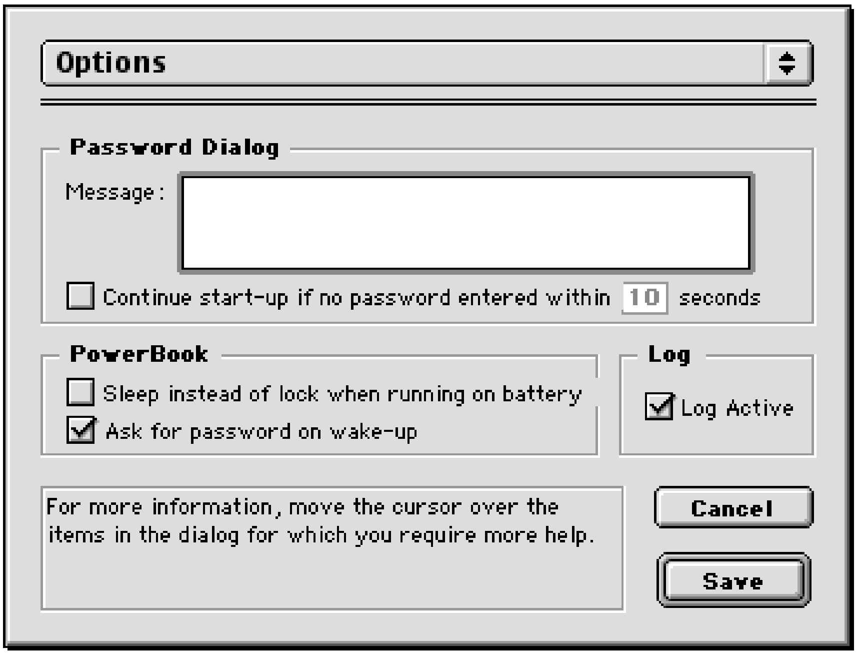
2. Enter the Master password and click the OK button.

3. In the pop-up menu, select Options.

You can also use the arrow keys to navigate through the pop-up menu.



The following dialog appears:



Options

Password Dialog

Message:

□ Continue start-up if no password entered within 10 seconds

PowerBook

□ Sleep instead of lock when running on battery

☑ Ask for password on wake-up

Log

☑ Log Active

For more information, move the cursor over the items in the dialog for which you require more help.

PASSWORD DIALOG

• **Message**: The information you enter in this box will appear each time DiskGuard requires the password for the volume you are protecting.

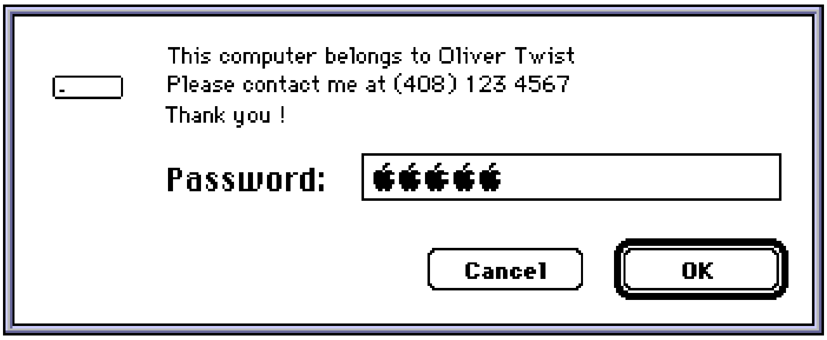
There are several uses for this message. It can:

- Inform the User that the volume is protected and that the correct password must be entered to access the volume.

- Identify an individual volume if several protected volumes are connected to the same Macintosh.

- Include your name and address if DiskGuard is installed on a PowerBook or an external volume. You can then be contacted if your hardware is lost or stolen.

- Include a reference to the password in case you forget it. Never write down the password itself.



This computer belongs to Oliver Twist
Please contact me at (408) 123 4567
Thank you !

Password: ●●●●●

Note: *A default message “Please enter the password for <volume name>” appears if you leave this text box empty*

- **Continue start-up if no password entered within *X* second**s: Use this option to allow for remote power-up access of a Macintosh with a protected start-up volume through Apple Remote Access, Timbuktu, etc. If no password is entered for the start-up volume within the designated number of seconds, DiskGuard will allow the complete boot-up process to take place. As soon as all extensions are loaded, the screen lock kicks in.

As the extensions of the remote access utility you use are loaded, you can then connect and enter the password to start working on the remote Macintosh.

POWERBOOK

- **Sleep instead of lock when running on batter**y: Normally, your PowerBook will not go into sleep mode when the screen lock is active. If you frequently run on battery power, you may prefer to check this option.

Doing so will cause your PowerBook to use the sleep mode in place of the screen lock mode, thereby saving valuable battery power.

Note: *If you check this option, we recommend you also check the option "Ask for password on wake-up".*

- Ask for password on wake-up: Normally, DiskGuard asks for a password every time a protected PowerBook wakes up from sleep mode. This feature is especially useful if you frequently leave your computer unattended while at work. Some PowerBook owners, however, may find this to be an unnecessary interruption. To allow a protected PowerBook to wakeup without requiring a password, simply deselect this option.

LOG

- **Log Activ**e: When the log is active, DiskGuard frequently writes information onto the hard disk. If you are working on a PowerBook and you have set the hard disk to spin down after a certain time, you will be slowed down whenever DiskGuard needs to write to its log because the disk will then need to spin up again. If you want to prevent this from happening, simply deselect this option and DiskGuard's log will be deactivated.

MODIFYING SETTINGS

All protection settings (passwords, restrictions, ...) can be modified at any time:

1. Select a protected hard disk in the DiskGuard screen.

Important: *If you select several disks, the modifications will be valid for all selected hard disks.*

If the settings are not identical on all selected hard disks, the password text boxes and some settings checkboxes will be grayed. A grayed box means three different options are possible:

- The grayed position means DiskGuard will not alter the feature's settings on all different disks when you click Save.

- By activating or deactivating the checkbox, DiskGuard will alter the settings of this particular feature on all disks when you click Save.

In the same way, when typing a new password, it will automatically apply to all selected hard disks.

2. Click the Settings button or double-click the disk.

You will be prompted to enter the Master password.

3. Enter the Master password and click OK.

The Screen Lock configuration window appears (See page 16)

4. You can navigate through the different configuration windows by using the pop-up menu or the arrow keys.

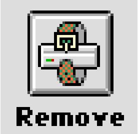
5. Change the settings and click Save to validate the modifications.

6. When modifying the settings, do not forget to inform the various users of the changes made.

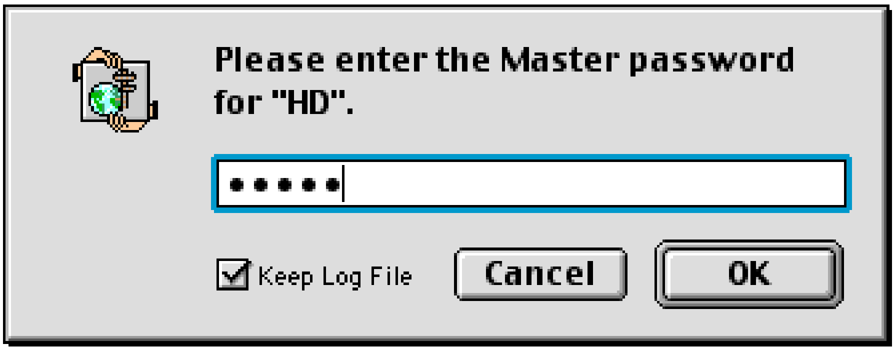
REMOVING PROTECTION

To remove the protection of a hard disk, proceed as follows:

1. In the DiskGuard screen, select a protected disk and click the Remove button.



The following screen appears:



Please enter the Master password for "HD".

•••••

☑ Keep Log File

2. Enter the Master Password.

3. You may wish to uncheck the Keep Log File box.

By default, DiskGuard keeps the log file of the hard disk when removing its protection. If you protect the hard disk afterwards, DiskGuard will continue to use the former log file. If you do not wish to keep this log file, uncheck the box.

4. Click OK.

Protection is removed

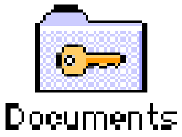
CHAPTER THREE- FOLDER PROTECTION

FOLDER PROTECTION

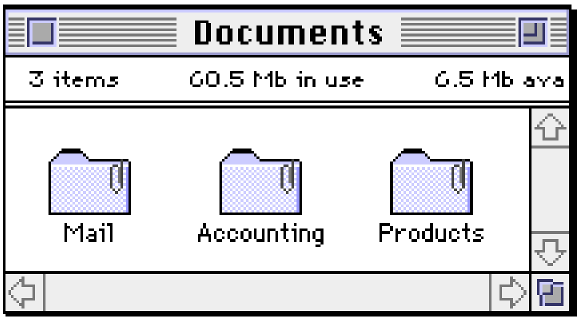
DiskGuard allows you to protect individual folders against unauthorized access. When someone accesses a disk with the User password, any folders you have protected will now be completely invisible to them.

PROTECTING A FOLDER

Before protecting a folder, make sure that the disk which contains that folder is protected by DiskGuard. From the Finder, you may then select any folder on that disk and choose Protect Folder from the File menu. You will notice that the folder's icon has been modified to indicate that it is now protected.

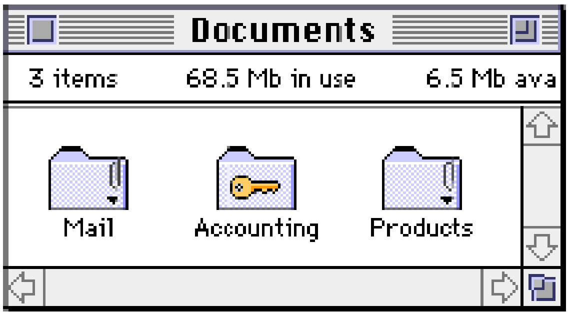


A key on a folder's icon indicates that the folder is protected and will be invisible to other users. A paper clip on the corner of a folder's icon indicates only that it is inside a protected folder.



Important: *If you move any of the enclosed folders to an unprotected disk, folder or to the desktop, they will no longer be protected. In the illustration above, for example, the three enclosed folders (Mail, Accounting, Products) will be invisible to other users as long as they remain inside the protected Documents folder. As soon as they are moved out of the Documents folder, however, they will be fully accessible to all users. To avoid this, protect any important enclosed folders individually using the Protect Folder command.*

In the illustration below, the folder Accounting will remain protected regardless of where it is located on the protected drive.



REMOVING THE PROTECTION

To remove a folder’s protection, select the folder and choose Remove Protection from the File menu.

PROTECTING THE SYSTEM FOLDER

All folders on a protected hard drive, including the System Folder, can be protected via the Protect Folder command in the File menu. Protecting the System Folder prevents any modification of its contents. You can also protect the System Folder by activating the Protect System Folder option in the User Restrictions screen of DiskGuard (See “Privileges”, page 21).

***Note:** Unlike other protected folders, the System Folder’s icon remains visible to users even when protected.*

CHAPTER FOUR - THE LOG FILE

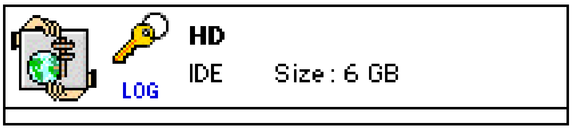
THE LOG FILE

The following chapter describes DiskGuard's log file: How to use it, how to filter the log file's data and how to make and create filters according to your own requirements.

WHAT IS THE LOG FILE?

DiskGuard's log file lists all valid and invalid access attempts to the protected hard disks and when they have occurred. It also keeps you updated on any information relative to the actual protection process (modification, removal, ...) and when the disks have been used. If, for instance, you want to know if somebody tried to access your disk or change its configuration during your absence, you can consult the log file. It also informs you on how long you, or any other authorized user, used the computer, etc.

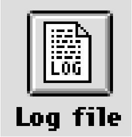
As soon as a disk is protected with a Master password, DiskGuard automatically generates a log file. A notification appears on the right of the hard disk icon in the DiskGuard window.



CONSULTING THE LOG FILE

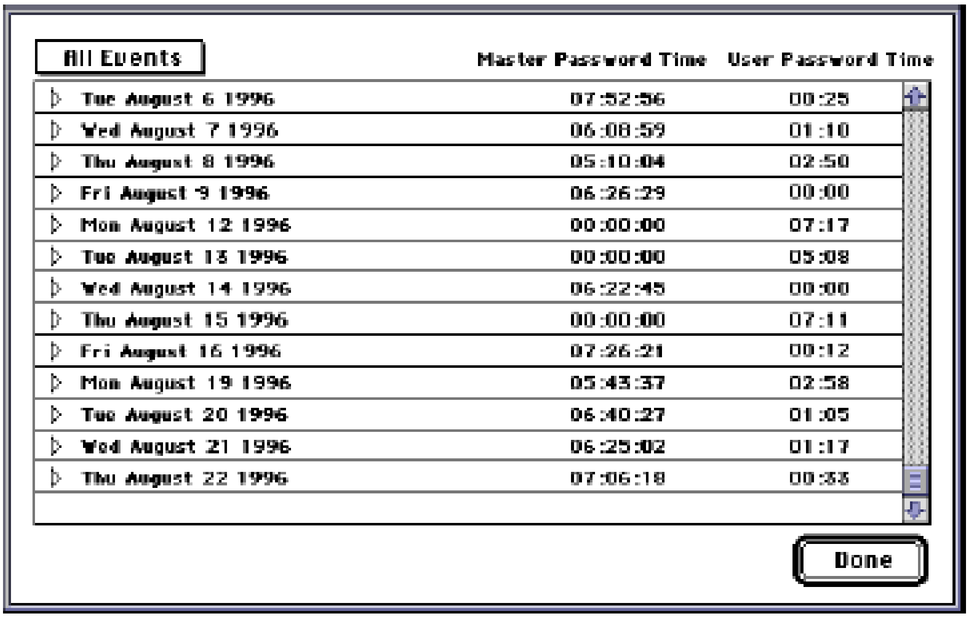
To view the log file of a protected hard disk:

1. Select a protected disk in the DiskGuard screen and click the Log file button.



2. Enter the Master or User password.

The following screen appears:

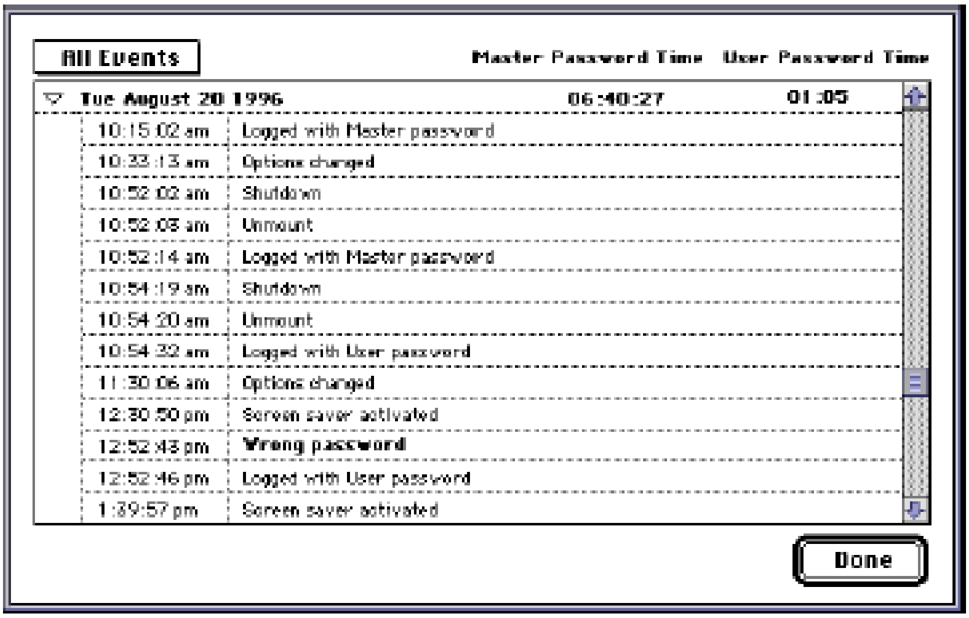


	Master Password Time	User Password Time
▷ Tue August 6 1996	07:52:56	00:25
▷ Wed August 7 1996	06:08:59	01:10
▷ Thu August 8 1996	05:10:04	02:50
▷ Fri August 9 1996	06:26:29	00:00
▷ Mon August 12 1996	00:00:00	07:17
▷ Tue August 13 1996	00:00:00	05:08
▷ Wed August 14 1996	06:22:45	00:00
▷ Thu August 15 1996	00:00:00	07:11
▷ Fri August 16 1996	07:26:21	00:12
▷ Mon August 19 1996	05:43:37	02:58
▷ Tue August 20 1996	06:40:27	01:05
▷ Wed August 21 1996	06:25:02	01:17
▷ Thu August 22 1996	07:06:18	00:33

The days during which the hard disk has been used are chronologically listed. You will also see the total number of hours and minutes the disk has been used with either the Master password or User password are displayed on the right-hand side.

3. If you want to know the events that took place on your hard disk on a particular day, click the triangle located on the left of that day.

The following screen appears:



	Master Password Time	User Password Time
▽ Tue August 20 1996	06:40:27	01:05
10:15:02 am	Logged with Master password	
10:33:13 am	Options changed	
10:52:02 am	Shutdown	
10:52:08 am	Unmount	
10:52:14 am	Logged with Master password	
10:54:19 am	Shutdown	
10:54:20 am	Unmount	
10:54:32 am	Logged with User password	
11:30:06 am	Options changed	
12:30:50 pm	Screen saver activated	
12:52:43 pm	**Wrong password**	
12:52:46 pm	Logged with User password	
1:39:57 pm	Screen saver activated	

To view the events of all days, press the Option key and click any of the triangles.

LIST OF EVENTS

DiskGuard's log file informs you of the following events:

- **Protection:**

- Protection installed

- Protection removed

- Protection updated: A new version of DiskGuard was installed and the protection was updated

- Master password changed: The administrator modified the Master password

- User password changed: A user modified the User password

- User refused to enter a new password: A user refused to modify his User password after it had expired

- Options changed: The administrator modified the screen lock configuration, the user password or the user restrictions

- **Access:**

- Logged with Master password: The Master password was introduced at the Macintosh's start-up or during an identity verification after a screen lock

- Logged with User password: The User password was introduced at the Macintosh's start-up or during an identity verification after a screen lock

- Wrong password: DiskGuard denied access to the computer after somebody made three unsuccessful attempts at entering the correct password

- Attempt to access the start-up disk: Somebody tried to access the hard disk and shut the computer down or the Macintosh shut down automatically after having displayed the password window for 5 minutes

- After hours access refused: A user tried to access the hard disk during a non-authorized hour or day

• Macintosh use:

- Shutdown

- Screen saver activated: The screen saver was activated after a period of inactivity or on user’s command

- Administrator changed the clock

- User changed the clock

- User tried to change the clock: A user tried to modify the clock although restrictions were set for the user password validity

- User tried to insert a floppy disk: A user tried to insert a diskette although he did not have the privilege to do so

- Unmount: Somebody disconnected the hard disk at start-up or after a screen lock, or the disk was ejected (put in the Trash)

- Crash

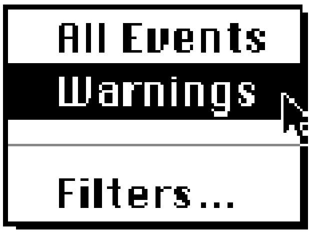
- Attempt to erase the disk: Somebody tried to initialize the protected hard disk

- Disk driver updated

USING FILTERS

The log file lists all above mentioned activities by default. If you prefer not to view all of this information, you can use filters. The Warnings filter lists events such as password entries, System errors (crashes), after hours access denial, … To filter this kind of information:

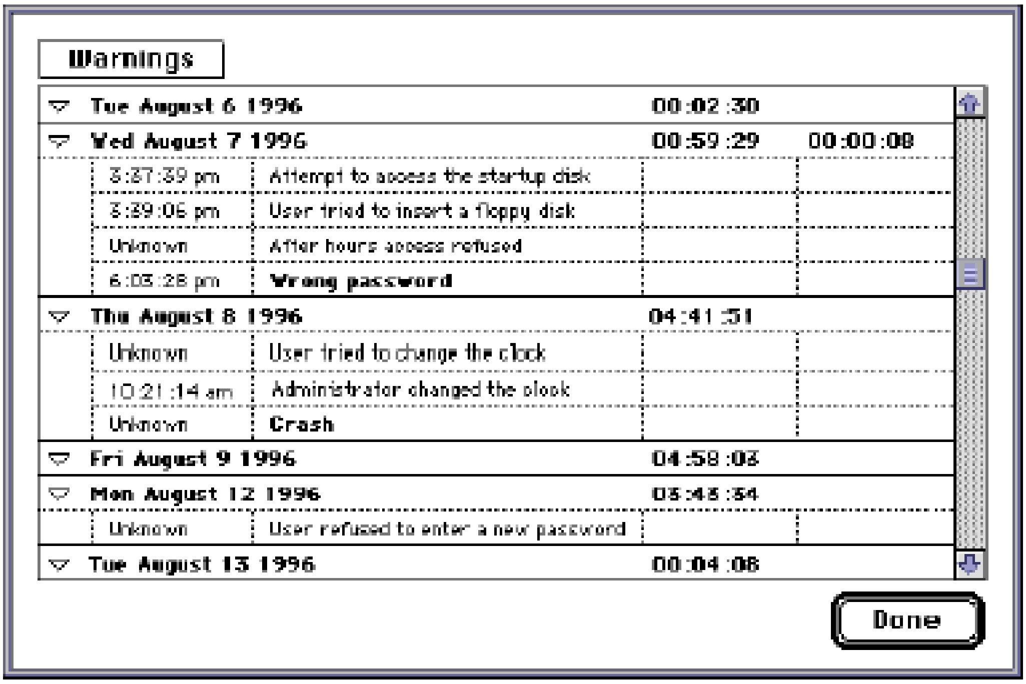
1. Open the pop-up menu and select the Warnings item.



2. Click the triangle of the day you would like to view.

To view the events of all days, press the Option key and click any of the triangles.

The events listed in the Warnings filter will immediately be displayed.



Warnings

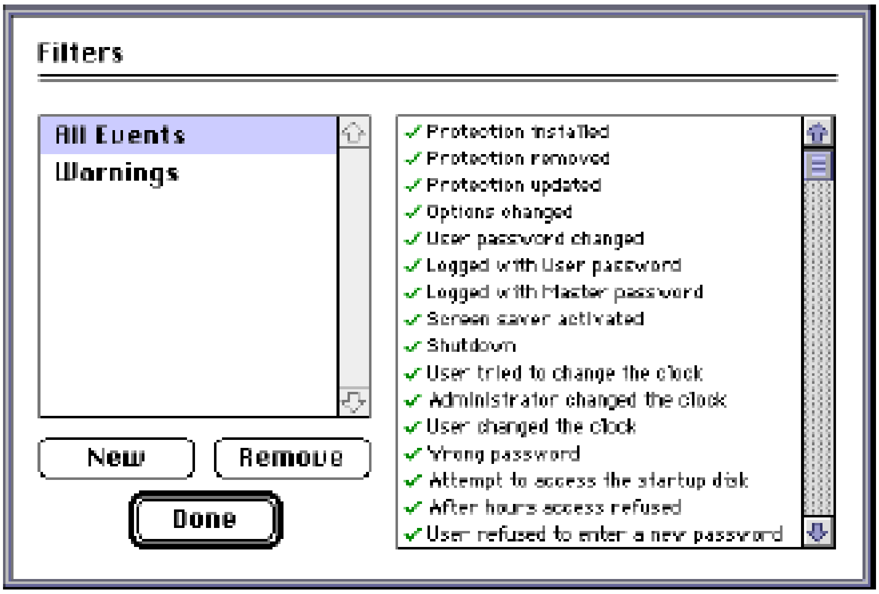
▽ Tue August 6 1996		00:02:30	
▽ Wed August 7 1996		00:59:29	00:00:08
3:37:39 pm	Attempt to access the startup disk		
3:39:06 pm	User tried to insert a floppy disk		
Unknown	After hours access refused		
6:03:28 pm	**Wrong password**		
▽ Thu August 8 1996		04:41:51	
Unknown	User tried to change the clock		
10:21:14 am	Administrator changed the clock		
Unknown	**Crash**		
▽ Fri August 9 1996		04:58:03	
▽ Mon August 12 1996		03:48:54	
Unknown	User refused to enter a new password		
▽ Tue August 13 1996		00:04:08	

Note: *You can change the events related to the Warnings filter (see below "Modifying filters").*

CREATING FILTERS

1. Open the pop-up menu and select the Filters… item.

The following screen appears:



Filters

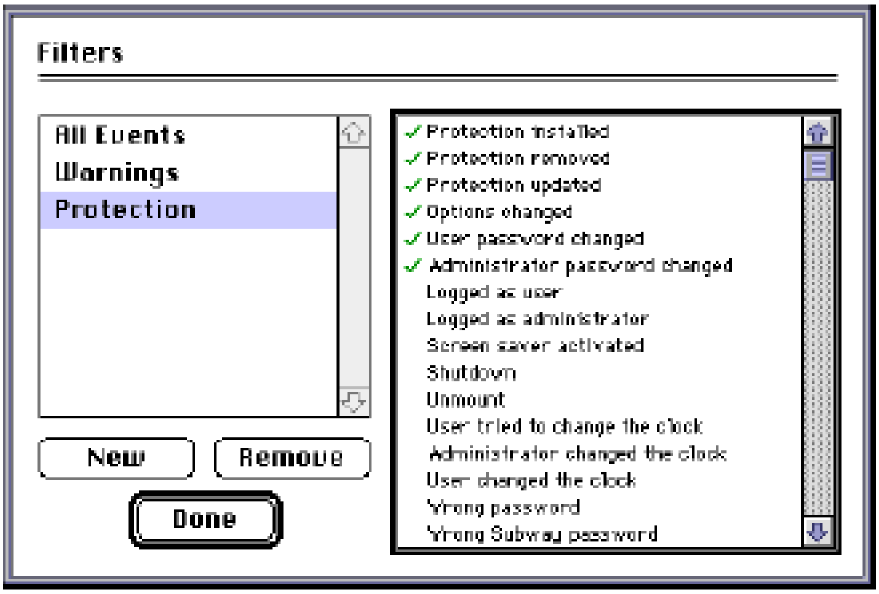
All Events
Warnings

✓ Protection installed
✓ Protection removed
✓ Protection updated
✓ Options changed
✓ User password changed
✓ Logged with User password
✓ Logged with Master password
✓ Screen saver activated
✓ Shutdown
✓ User tried to change the clock
✓ Administrator changed the clock
✓ User changed the clock
✓ Wrong password
✓ Attempt to access the startup disk
✓ After hours access refused
✓ User refused to enter a new password

2. Click the New button and type the name you would like to give to the filter.

Give a name which explains the type of information you would like to view.

3. In the right of the window, select one or more events you would like to list under the new filter. When finished, click the Done button.



Filters

All Events
Warnings
Protection

✓ Protection installed
✓ Protection removed
✓ Protection updated
✓ Options changed
✓ User password changed
✓ Administrator password changed
Logged as user
Logged as administrator
Screen saver activated
Shutdown
Unmount
User tried to change the clock
Administrator changed the clock
User changed the clock
Wrong password
Wrong Subway password

4. Select the filter you've just created in the pop-up menu.

MODIFYING AND REMOVING FILTERS

To modify the events related to a filter, select the latter and choose other events. To modify the name of a filter, select it and type in a new name.

To remove a filter, select it and click the Remove button.

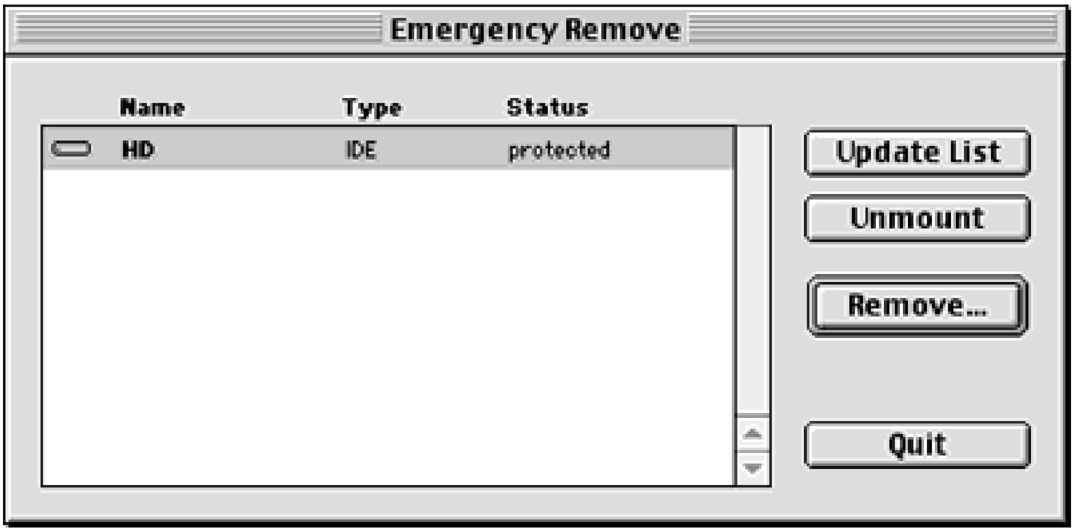
Even under the best of conditions, hard drive directories and files can become corrupted. In most cases, disk repair utilities can fix such damage quickly. Should your volume’s protection itself become damaged, however, the procedure to remove it as described above may not work properly. In such cases, you must use the Emergency Remove application found on your program floppy.

Warning: *Do not use a disk repair utility like Disk First Aid, Norton Disk Doctor, Techtools or MacTools on a volume with damaged protection. Doing so could corrupt the data on the volume.*

1. Start up your Macintosh with the CD-ROM or Disk Tools floppy which came with it, then insert the DiskGuard program floppy.

2. Double-click the Emergency Remove application.

The following dialog appears:



Emergency Remove

Name	Type	Status
HD	IDE	protected

3. Select the volume from which you want to remove the protection and click on Remove.

Note: *If the requested volume does not appear in the list, make sure it is switched on and click on Update.*

4. Enter the password for the selected volume and click on OK.

The volume’s protection is now removed.

Note: *If the problem continues,contact our technical support at support@intego.com.*

INDEX