FileGuard 4

User Manual

http://www.intego.com

FileGuard for Macintosh

Intego.

www.intego.com

TABLE OF CONTENTS

INTRODUCTION

Thank you for choosing FileGuard! We hope this software will satisfy all your Macintosh security requirements.

Before going any further, please complete and send in your Registration Card. Attach the serial number label to your User Card and put it in a safe place. You will need your serial number during the FileGuard installation and whenever you contact our customer support.

Overview

FileGuard is a powerful and easy-to-use Macintosh security program. It provides automatic and transparent protection of documents, as well as protection for all volumes, folders and applications on your Macintosh.

FileGuard is installed and configured by an Administrator. The Administrator can appoint Super Users to assist him with the day-to-day management of the system. Together the Administrator and Super Users are responsible for implementing and maintaining all security measures.

These include:

- **Access control.** Users must identify themselves to FileGuard before they are able to use your Macintosh.

- **Volume protection**. All rewritable volumes, such as hard disks, partitions,removables and floppies, can be protected using a password.

- **Folder protection.** Folders can be protected and shared by setting access privileges.

- **Application protection.** Applications can be protected against unauthorized use or copying.

- **Document encryption.** Documents can be encrypted to safeguard their contents. Once encrypted, a document can only be opened by entering the correct password.

- **Activity logging.** FileGuard maintains a log of User activity, as well as a comprehensive system usage chart.

Customer Support

Do not hesitate to contact us if you have any questions about FileGuard. You will find the address of the distributor for your country in the Customer Support file on the FileGuard program floppy. For quick answers to frequently asked questions, you may also want to refer to the Questions & Answers document on the FileGuard program floppy. When you call for support, please make sure you have returned your Registration Card and have the following items handy:

- This manual

- Your FileGuard license number. The license number is the six digit number which corresponds to the last group of six digits in the serial number

- Your current FileGuard version number.

  You can find the FileGuard version number by choosing About FileGuard… from the FileGuard Menu. The version and serial number of the FileGuard software are also on your User Card (the other half of the registration card you were asked to keep for your own records).

- The type of Macintosh you are using.

- Your system version number. You can find this information under the Apple menu by choosing About This Macintosh… while in the Finder.

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

About this Manual

This manual guides you through the process of installing, configuring and using FileGuard. We strongly suggest that you install and configure FileGuard in a single session. It is both easier and more secure to complete these tasks in one session than to break off and restart at a later date.

Many of the techniques you employ in FileGuard, such as using the mouse or working with windows, are standard ways of working with a Macintosh. If you are unfamiliar with these techniques or the vocabulary used to describe certain features you should refer to your Macintosh Owner's Guide for further information.

This manual is organized as both a tutorial and reference guide:

Chapter One is concerned with installation. It explains how to install, upgrade and remove FileGuard.
Chapter Two describes how to configure FileGuard. It explains how to create Users, set the Administrator, set general options, protect specific items on your Macintosh and check the log from within the FileGuard configuration application.
Chapter Three covers the day-to-day use of FileGuard. It explains how to log in, log off, lock your screen, change your user password and protect items from within the Finder.

A comprehensive guide on the day-to-d ay use of FileGuard is available on the FileGuard program floppy. It has been especially written for those Users who work on a Macintosh with FileGuard installed but who are not the FileGuard Administrator. Please feel free to distribute this file to all people concerned.
Note: For further information regarding common FileGuard queries, please refer to the Questions & Answers file on the FileGuard program floppy.

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 in Chapter Two 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.*

Note for FileGuard Users on a Network

If you want to protect several networked Macintosh computers, we recommend you use **FileGuard® Remote.** In addition to all of FileGuard's standard features, this application allows you to remotely install, remove, modify and update FileGuard's protection and instantly lock volumes over the network.

FileGuard Remote is fully compatible with FileGuard. If you previously protected some of your computers with FileGuard, you will also be able to access and configure them with FileGuard Remote over the network.

FileGuard Remote is available in office packs and site licenses.

For further information on FileGuard Remote, please contact the FileGuard distributor for your country. You will find the distributor addresses in the Customer Support file on the FileGuard program floppy.

CHAPTER ONE - INSTALLATION

This chapter describes:

- **System Requirements** for installing FileGuard. Read this section if you wish to upgrade FileGuard or install for the first time.

- **Before Installing or Upgrading FileGuard**. Read this section before you upgrade FileGuard or install for the first time.

- **Installing FileGuard.** Read this section if you wish to install FileGuard for the first time.

- **Upgrading FileGuard.** Read this section if you wish to upgrade FileGuard from a previous version to Version 3.

Important: Installing FileGuard does not in itself make your Macintosh secure. FileGuard must be configured and your **startup volume protected to provide security protection**. We strongly recommend that you install and configure FileGuard in one session as your Macintosh is not secure until this process is complete.

System Requirements

FileGuard requires a Macintosh running System 7.0 or later, 4 megabytes of RAM and at least one hard disk. See the Read Me file on the FileGuard program floppy for up-to-date details on system requirements and compatibility.

Before Installing or Upgrading FileGuard.

Before installing or upgrading FileGuard, it is important for you to take the following precautions:

1. Make a backup copy of your data.

2. Check your volume. A volume can contain minor defects that may cause problems when you protect it.

We recommend you check the state of your volume with the utility called Disk First Aid Or SOS Disk. This utility is included on the CD-ROM or on the System disks that came with your Macintosh.

3. Remove any automatic volume compression utilities such as Stacker® or TimesTwo® as they may interfere with volume protection. File level compressors such as StuffIt™ or DiskDoubler™ present no such problems.

4. Remove all other protection utilities as these will interfere with FileGuard.

Note: *Do not install an outdated version of FileGuard as it may conflict with your hardware and software. If you are in doubt, contact our Technical Support department. Check the Read Me file on the FileGuard program floppy and our Web site for compatibility information.*

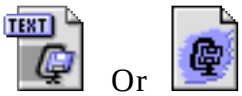
Installing FileGuard

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

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.



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 :

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

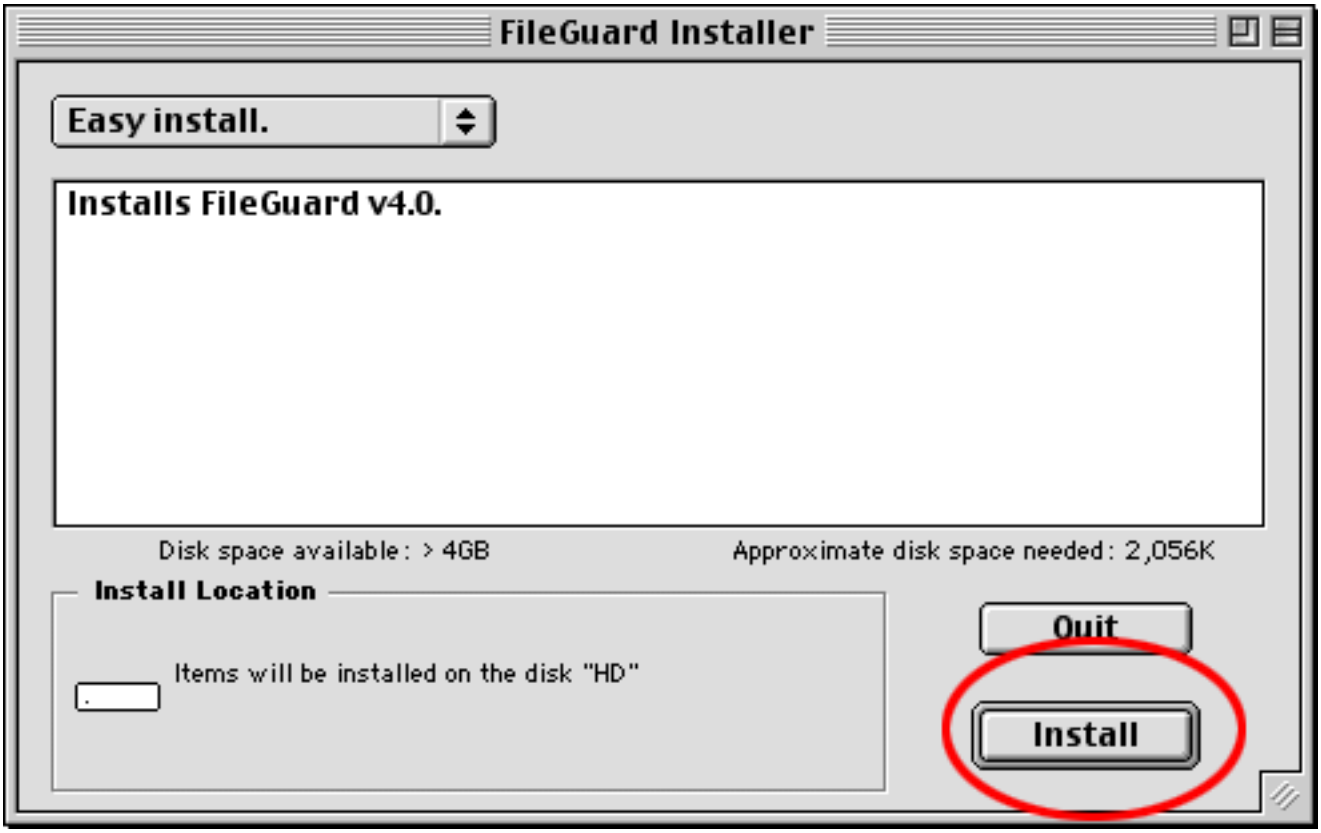
Double-click on the FileGuard installer icon **(1)**. When you see this splash screen **(2)**, click continue.

(1) 

(2) 

The FileGuard 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 FileGuard 4.0.



Click install to start the installation process.

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

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

Once you have restarted and your desktop appears, you will see a little icon in the menu bar. If you choose to configure the program, you will be asked to enter your serial number in order to use the program.

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 FileGuard

Note: *If you are using a version prior to 3.0, we recommend you decrypt all encrypted files with your actual version before upgrading.*
FileGuard 3.0 cannot decrypt files which were encrypted using FileGuard versions prior to 3.0.

Read this section if you are upgrading FileGuard:

1. Insert the CD you received with FileGuard and drag the folder named "FileGuard® Folder" from the CD to your hard disk. The folder contains the FileGuard application and documents.
If you are upgrading from version 3.0 and above you must remove all previous versions of the FileGuard application from your hard disk. Only the latest version of the FileGuard application must remain on your disk.

2. Restart the Macintosh while holding down the Shift key to disable all extensions.

3. Double-click the folder's icon, then double-click the Read Me icon to view important late-breaking information about FileGuard. Please read this file.

4. Double-click the "FileGuard®" icon. A dialog box appears warning that FileGuard is not installed on your Macintosh. You are asked if you want to upgrade FileGuard.

5. Click on **Yes**. The installation proceeds. If you are upgrading from a version of FileGuard prior to 3.0 the registration window appears. Enter your name, organization and the 17-digit serial number you received with the program, then click on **OK.** Serial numbers for previous versions will not work with FileGuard 3.0 and above.If you are upgrading from version 3.0 and above there is no need to enter registration or User details as this information is retained.

6. Click on **OK.** A dialog box appears asking you to restart your Macintosh in order to complete the installation process.

7. Click on **OK,** then choose Restart from the Special menu.

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

Note: *Your application, volume, document and folder protection settings are retained by the new version of FileGuard. Your Users list and all associated privileges are also transferred intact. You may want to reconfigure your Users and options, however, to take advantage of new features.*

Removing FileGuard

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

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

You should remove the protection before uninstalling FileGuard .

1) To Uninstall all FileGuard extensions, open your extensions folder and select the extensions.

2) Drag the two extensions (Fileguard extension and Subway) into the trash.

3) Restart your Macintosh.

4) Empty the trash once your computer has restarted.

CHAPTER TWO- CONFIGURING

Configuring FileGuard

This chapter describes how to configure FileGuard and is the most important part of this manual. It explains how to create Users, set the Administrator, set general options, protect specific items on your Macintosh and check the log from within the FileGuard configuration application.
To configure FileGuard you need to:

1. Create a User

2. Specify this User as the Administrator and configure the Administrator.

3. Create and configure other Users.

4. Set general options that define how your Macintosh will function and what actions Users can perform.

5. Protect your startup volume, followed by other volumes, folders, applications and documents that require protection.

The structure of this chapter follows this process. When you have completed this process your Macintosh will be secure.

The following section explains concepts and features you should understand before configuring FileGuard.

Concepts and Features

Privileges

Privileges are assigned to Users and items. They are used by FileGuard to determine what actions a User can and cannot perform. When a User logs in, FileGuard checks the privileges associated with that User and instantly knows what he is authorized to do.

User Passwords

Users are identified by their name and user password, both of which are required to log in. As soon as a User logs in, FileGuard knows what privileges that User has been given. A user password must be composed of at least four characters. User password fields are case sensitive.

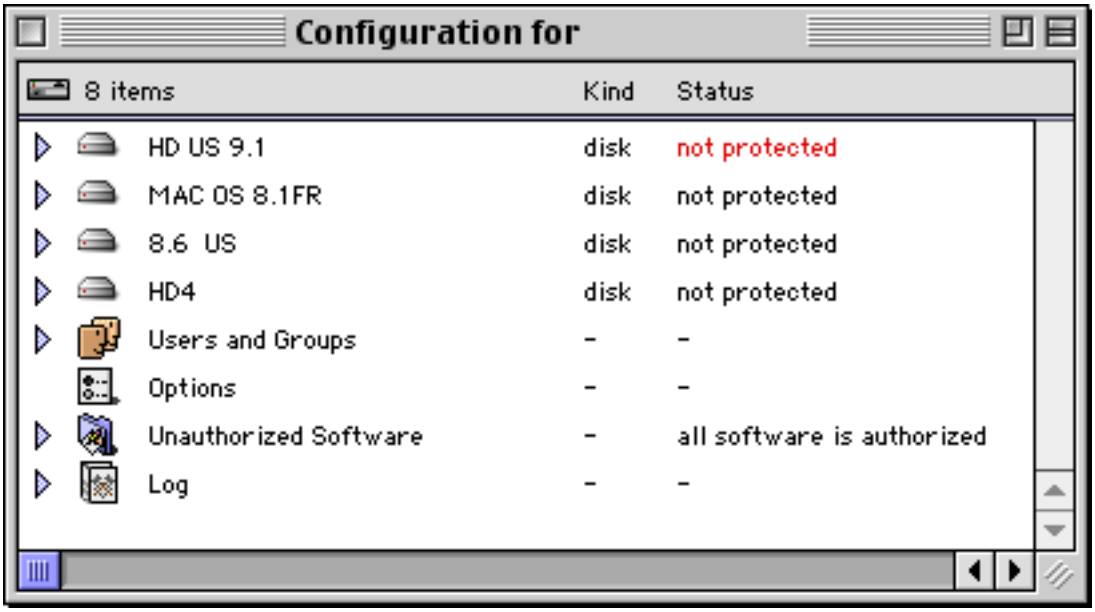
For information on lost user passwords refer to the Questions & Answers file on the FileGuard program floppy.

Document, Application and Volume Passwords

FileGuard allows you to protect individual items with unique passwords. Users must know these passwords in order to use items that are protected in this way. For example, an encrypted document requires a password before it can be opened. Likewise, a volume can be set to request a password before mounting. Passwords must be composed of at least four characters and are case sensitive. Passwords can be applied to documents, applications and volumes only. Folders are protected by assigning user privileges. You cannot assign an individual password to a folder.
For information on lost passwords refer to the Questions & Answers file on the FileGuard program floppy.

The Configuration Window

The Configuration window is the starting point for all FileGuard configuration operations:



Note: *The text in the title bar of the Configuration window comes from the Macintosh Name section of the Sharing Setup control panel. To view this control panel, choose Control Panels in the Apple menu, then choose Sharing Setup.*

User Types

The following user types can be defined within FileGuard:

User

An everyday user of the Macintosh. Each User has a name and user password that must be entered when he logs in. FileGuard then knows what privileges that User has been given and what he is authorized to do.

Administrator

FileGuard allows you to specify one User as the security “Administrator”. The Administrator is the ultimate authority within FileGuard. He defines who can do what, when and how. The Administrator is the only User with complete access to the Configuration window. For this reason the Administrator’s user password must be strictly confidential. This manual is written for the Administrator. *We assume that you, the reader of this manual, plan to become the Administrator.*

Super User

The Administrator can appoint Super Users to look after the day-to-day maintenance of FileGuard. A Super User might be a departmental computer supervisor or university lab assistant responsible for looking after a number of machines. The Super User is typically responsible for minor changes to User configurations. Super Users can only create or make changes to Users. They cannot create, change or delete the Administrator, other Super Users or themselves.

Guest

The Guest is similar to a standard User with one important exception. Anybody can log in as Guest because no user password is required. For this reason, the Guest is typically given very low level access privileges. The Administrator can choose to enable or disable the Guest feature. Disabling the Guest ensures that only authorized Users have access to the Macintosh. The Guest is the only user immediately after FileGuard is installed for the first time.

The Guest can be useful in certain situations:

- A college network administrator wants his students to be able to use any of the machines in his programming lab. If he sets appropriate privileges for the Guest he does not need to create a User for each student. His students can simply log in as the Guest and use any machine at any time.

- The manager of a computer showroom wants his customers to test drive the machines, while ensuring the machines remain protected. If he sets appropriate privileges for the Guest he does not need to give user passwords to customers.

If the Guest is enabled, anyone can log in as the Guest and use your Macintosh. To minimize any security risk you should set the Guest's privileges accordingly. If the Guest is disabled, only those individuals with a user password can use your machine. Refer to "Setting General Options" on page 35 for further information.

User Icons

The following icons are used to represent the different user types:

User/Guest

Administrator. Note the black border.

Super User. Note the gray border.

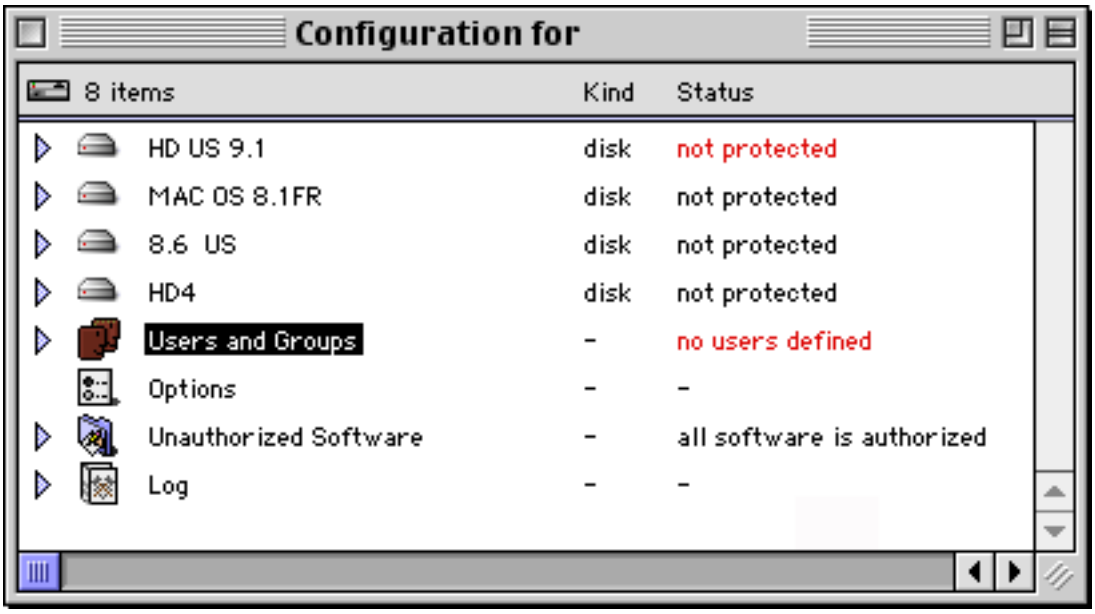
In addition, the icon of the current User appears to be awake while the icons of all other Users appear to be asleep:

Current User

Other Users

Launching FileGuard

You must launch FileGuard in order to configure it. Once you have successfully installed FileGuard and restarted your Macintosh, double-click the FileGuard icon or select Configure from the FileGuard menu. The Configuration window is displayed:



Note: *The first time you launch FileGuard, no password is requested because the Administrator is set to the Guest. Once you have set yourself as the Administrator you must enter your user password whenever you launch FileGuard. Super Users can also configure FileGuard after entering their user name and password.*

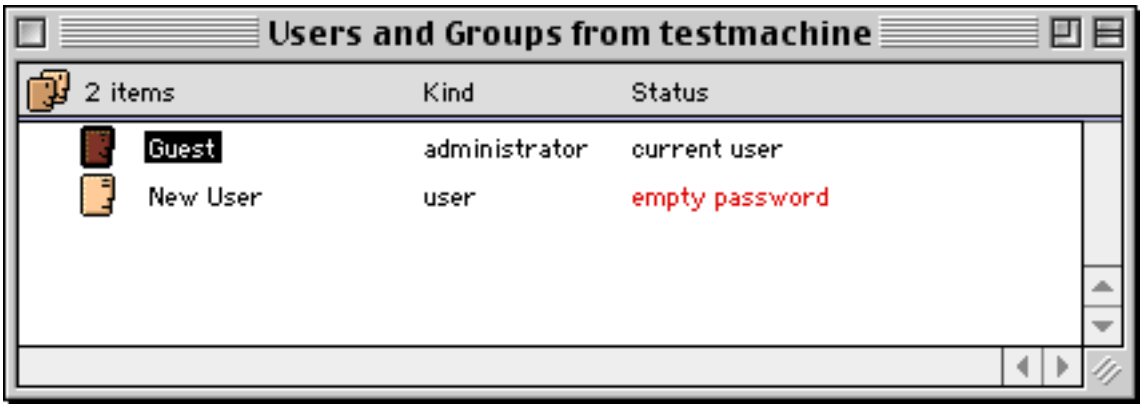
Creating the First User

The first step in configuring FileGuard is to create a User who you then specify as the Administrator.

To create this User:

1. Double-click the Users and Groups icon in the Configuration window. The Users and Groups window is displayed:

2. Choose New User from the Users menu. A new User icon appears in the Users and Groups window:



3. Name the new User. Use your own name if you wish to be the Administrator.

You must now define the User you have just created as the Administrator.

Defining the Administrator

Immediately after FileGuard is installed the role of Administrator is set to the Guest. This is a risky situation. In order to prevent unauthorized individuals from logging in as the Guest, configuring themselves as the Administrator and taking control of your Macintosh, it is essential you specify the new Administrator as soon as possible. To define a User as the Administrator:

1. Select the User you wish to become the Administrator in the Users and Groups window. We assume that you wish to become the Administrator.

2. Choose Make Administrator from the Users menu. You are asked if you want the selected User to become the new Administrator.

3. Click on **Yes.** The selected User is assigned the role of Administrator.

Configuring the Administrator

So far you have created a User and specified that User as the Administrator. You must now configure the Administrator to determine exactly what he can and cannot do.
The choices you make here determine how FileGuard operates for the Administrator:

1. Double-click the Administrator icon in the Users and Groups window.
The following dialog appears:

2. Configure the Administrator by entering a user password and by setting the administrator options. The configuration options are explained in the following sections.

3. Click on the close box then click on **Save.**

Defining the Password

1. Click the **Password** text box and enter a password for the Administrator.

2. Click the **Confirmation** text box, or press the Tab key, and re-enter the password.

You have now set the password for the Administrator. This password is required every time you log in. Make sure you remember your user password and that you keep it secret. You can change your password at any time in this window or when you log in. Refer to “Changing a User Password” on page 83 for further information.

Setting the Administrator Options

Ask to encrypt new documents

FileGuard allows you to encrypt the contents of a document when it is saved for the first time. Checking this box causes a dialog to be displayed when the document is first saved, asking if the document contents should be encrypted. Refer to “Protecting Items” on page 40 and “Protecting Documents when Created” on page 84 for further information.

Remind me to change password every X days

Check this box to remind yourself that you should regularly modify your Administrator password. Enter the number of days after which you want to be reminded. As the Administrator, you can only be reminded to change your password, you cannot be forced to do so.

Creating Other Users

So far you have created, set and configured the Administrator. You can now create other Users. You can give different privileges to different Users. This allows you to define who can do what, when and how. Users can represent actual people, for example, “John”, or they can refer to an occupation or activity, for example, “Student”. *A user’s name must be unique.* To create Users:

1. Double-click the Users and Groups icon in the Configuration window. The Users and Groups window is displayed.

2. Choose New User from the Users menu. A new User icon appears in the Users and Group window.

3. Name the new User.

Repeat this process to create as many Users as you require.

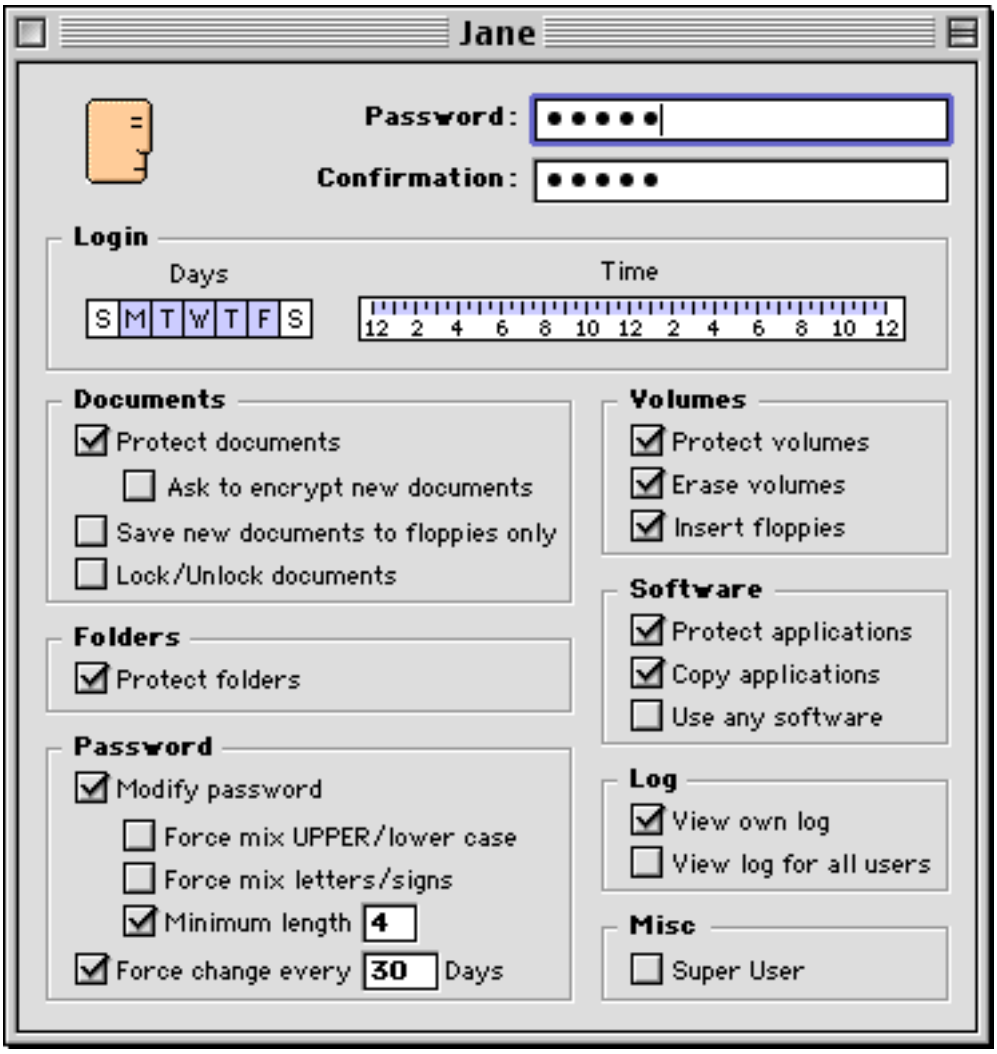
If you require many Users with a similar configuration, you can create a single User then configure and duplicate that User as many times as necessary. To duplicate a User, select the User and choose Duplicate from the File menu. When duplicated, the User’s configuration is copied.
To rename a User, click the User’s name in the Users and Groups window and type the new name.

Configuring Users

So far you have created as many Users as you require. You must now configure these Users to determine exactly what they can and cannot do.

The choices you make here determine how FileGuard operates for each User:

1. Double-click a User icon in the Users and Groups window. The Configuration dialog box for that User is displayed:



2. Configuring a User involves setting the user password, available login times and options for each User. This is explained in the following sections.

3. Click the close box then click on **Save.**

Repeat this process for all Users.

Defining the User Password

1. Click the **Password** text box and enter a user password for the User.

2. Click the **Confirmation** text box, or press the Tab key, and re-enter the password. You have now set the password for the User. A User can change his user password if you have given him the privilege to do so. Refer to “Changing a User Password” on page 83 for further information.

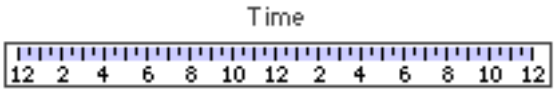
This password is required every time the User logs in. Make sure your Users understand the importance of both remembering their passwords and keeping them secret.

Available Login Times

You can restrict access to your Macintosh to specific days and times for each User:

Days: You can deny the User access to the machine on certain days of the week. For example, if you deny access on Saturday and Sunday the User cannot access the Macintosh during the weekend. The highlighted boxes indicate the days on which the User is allowed to access the machine. Click on the days in the Days bar to change their status:

Time: You can deny the User access to the Macintosh during certain periods of the day, for example outside work hours. The highlighted area indicates the hours during which the User is allowed to access the machine. Drag the pointer from the start hour to the finish hour in the Time bar:



The security screen will kick in at the specified finish hour. The User is notified three times first. These warnings occur approximately one hour, ten minutes and one minute before the screen is locked. Once the screen is locked the User’s login is refused.

Note: *As soon as you restrict a User's Available Login Times, he is no longer able to change the internal Macintosh clock using the Date and Time control panel. This prevents the User from by passing the Available Login Times restrictions. However, the User is able to check the Daylight Savings Time box.*

Documents

Protect documents

Check this box to allow the User to encrypt documents.

Important: Protected documents cannot be read without the correct password. You must be careful when giving this privilege to Users. If the User forgets a document's password or leaves the company without passing it on, the document cannot be recovered.

Ask to encrypt new documents

FileGuard allows you to encrypt the contents of a document when it is saved for the first time. Checking this box causes a dialog to be displayed when the document is first saved, asking if the document contents should be encrypted. Refer to "Protecting Items" on page 40 and "Protecting Documents when Created" on page 84 for further information.

Save new documents to floppies only

Check this box to prevent the User from saving a new document to any volume other than a floppy. Because removable cartridges are treated like hard drives, this will prevent the User from saving new files to zip, Jaz, magneto-optical or similar volumes.

Lock/unlock documents

Check this box to allow the User to lock and unlock documents. Please note that this privilege refers to the "Locked" checkbox available in the Info window for any Macintosh document. It is not related to file encryption in any way.

Volumes

Protect volumes

Check this box to allow the User to protect volumes.

Warning: If you give this privilege to the User you must protect your startup volume. If you do not protect your startup volume it is possible for Users to lock you out of your own computer.

Erase volumes

Check this box to allow the User to initialize floppies and other volumes by choosing Erase Disk… from the Special menu in the Finder.
If you disable this option, the User will not be allowed to initialize floppies and other volumes in this way.

Note: Floppies and volumes protected by FileGuard cannot be initialized using Erase Disk.

Insert floppies

Check this box to allow the User to insert floppies.

Do not enable this option if you

- want to prevent the User from copying infected applications on your Macintosh.
- do not want the User to copy your documents and applications onto floppy.

Note: *Copies of protected documents remain fully protected. Copies of protected folders contain only those items from the original folder which are visible to the User.*

Folders

Protect folders

Check this box to allow the User to protect folders.

Software

Protect applications

Check this box to allow the User to set protection for applications. Refer to “Protecting Applications” on page 56 for further information. Note that his type of protection can only be used on 68K applications, not on PowerPC native applications.

Note: *Checking this box does not give the User the ability to modify the list of Authorized Software. This list can be modified only by the Administrator and the Super Users. Refer to “Authorizing/Unauthorizing Software” on page 63.*

Important: *If you give this privilege to a User be aware that he can then set his own protection which may exclude all other Users, including yourself, from using the application.*

Copy applications

Check this box to allow the User to copy applications.

Use any software

Check this box to allow the User to use any software, regardless of whether or not it appears in the Authorized Software list. Refer to “Authorizing / Unauthorizing Software” on page 63 for further details.

Note: Even if this option is set, the User will only be able to use applications protected with a usage password if he knows that password. Refer to “Usage Password” on page 58 for further information.

User Password

Modify password

Check this box to allow the User to alter his user password from the login dialog box. Refer to “Changing a User Password” on page 83 for further information.

The following options help to prevent others from guessing user passwords:

Force mix UPPER/lower case

Check this box to force the User to include a mix of upper and lower case letters in his user password.

Force mix letters/signs

Check this box to force the User to include a mix of letters and signs in his password. Valid letters are A-Z and a-z. Valid signs are 0-9, !, @, #, $, %, ^, &, *, (,), the comma and the space character.

Minimum length X

Check this box to set the minimum number of characters the User must include in his user password. By default the minimum is four characters.

Force change every X days

Check this box to force the User to regularly modify his password, provided he has the privilege to do so. If he does not have this privilege, he must contact the Administrator or a Super User to modify his password for him. When this box is checked, the user password is only valid for the defined number of days. To enable this option, check the box on the left and enter the number of days after which the User must define a new password.

Once this option is checked:

- FileGuard prohibits a User from re-using his old passwords.
- The User is no longer able to change the internal Macintosh clock using the Date and Time control panel. This prevents the User from bypassing the Force change every X days restriction. However, the User is able to check and uncheck the **Daylight Savings Time box.**

Log

View own log

Check this box to allow the User to view his own log when he chooses Log… in the FileGuard menu.

View log for all Users

Check this box to allow the User to view the log for all Users.

Misc

Super User

Check this box to make the User a Super User. You can appoint Super Users to look after the day-to-day maintenance of FileGuard. Super Users can do virtually everything the Administrator can. They cannot, however, create, change or delete the Administrator, other Super Users or themselves. Refer to “User Types” on page 19 for further details.

Removing Users

To remove a User:

1. Select the User’s icon in the Users and Groups window and drag it to the Trash.

2. Confirm that you want to remove the User. The Administrator will automatically become the new owner of all folders previously owned by the removed User.

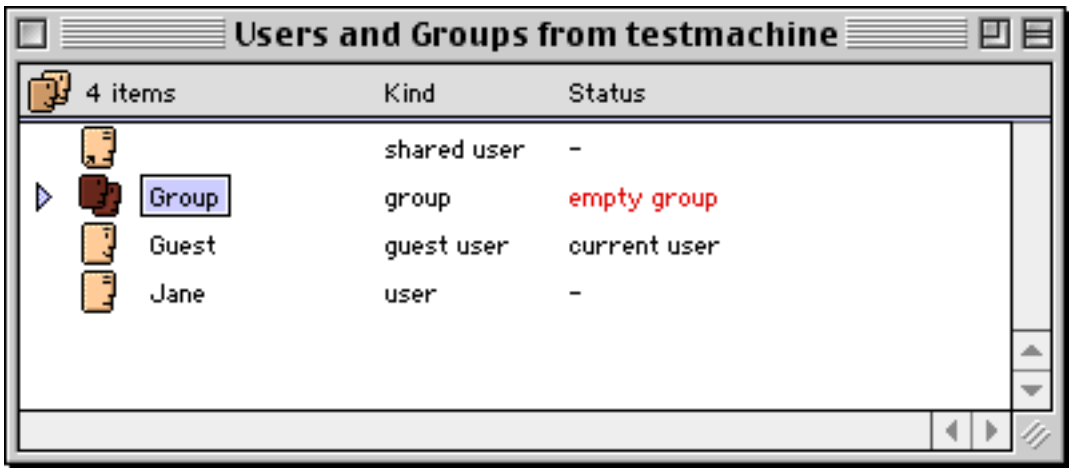
Note: If you remove the Administrator, the Guest automatically becomes the new Administrator. You cannot remove the Guest.

Creating a Group

So far you have created and configured the Administrator and as many Users as you require. You can now define groups of Users. Groups are composed of Users who are given common access privileges to specific folders. A User can be added to as many groups as required. Groups are only used in the context of folder protection; there are no groups associated with documents or applications. Consequently, there is no need to create a Group if you do not intend to use Folder protection. Refer to “Setting Folder Privileges” on page 48 for further information. To create groups:

1. Double-click the Users and Groups icon in the Configuration window. The Users and Groups window is displayed.

2. Choose New Group in the Users menu. A new group icon appears in the Users and Groups window:



3. Enter a name for the group.

4. Drag Users onto the newly created group icon to create members of the group.

Repeat this process to create as many groups as you require.

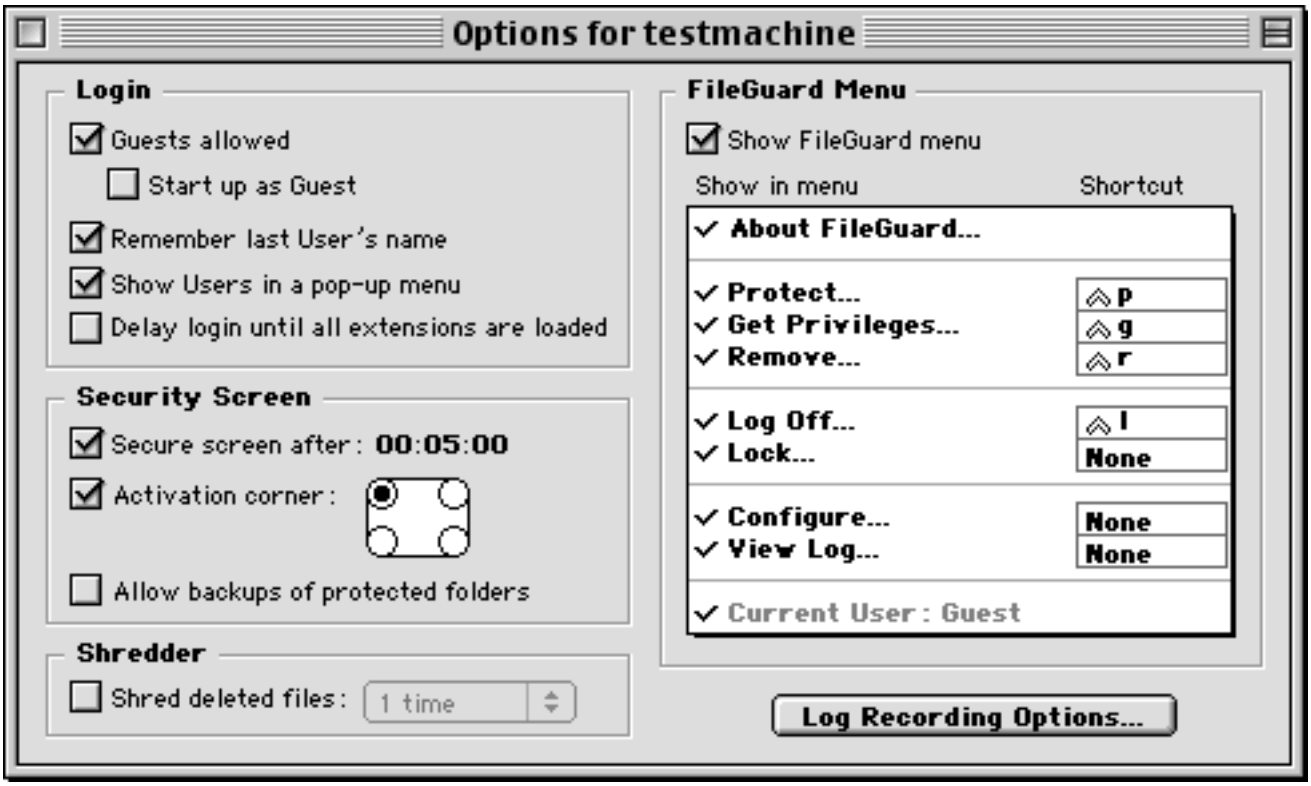
Note: *To remove a group, select the group’s icon in the Users and Groups window and drag it to the Trash.*

Setting General Options

So far you have created and configured the Administrator, Users and as many User Groups as you require. You can now set options that allow you to customize general security features and decide how the FileGuard menu appears to the Users. To set general options:

1. Double-click the Options icon:

The following dialog box is displayed:



Note: All settings shown are the defaults.

2. Set the Options as required. They are explained in the following sections.

3. Click the close box then click on **Save.**

Login

Guests allowed

Check this box to enable Guest access. If this option is enabled anyone can log in as Guest and use your Macintosh. Make sure you set the Guest's privileges accordingly. We strongly suggest you set a low level of access privileges for the Guest.

Start up as Guest

Check this box to specify that the Guest is the default User at startup. If this option is enabled the login dialog does not appear at startup. No user password is required, and your Macintosh automatically boots up with Guest privileges only. Any User who requires greater access privileges can log in afterwards with his user name and user password.

Remember last user name

Check this box to specify that FileGuard remembers the name of the last User when he logs off. This name is suggested as the default User the next time the Login dialog is displayed. This feature is useful if the same User regularly works on the same computer.

Show Users in a pop-up menu

Warning: Once this option is selected, unauthorized individuals no longer need to guess both a User's name and password to enter your system. If you use this feature, we recommend that you also force Users to create passwords which are difficult to guess. Refer to "User Password" on page 31 for further information.

Delay login until all extensions are loaded

Checking this box allows the User to start the Macintosh remotely and use remote access packages like Timbuktu or ARA to work on the machine. If enabled, this option ensures that the user password is not requested until those extensions necessary to use remote access packages are loaded.

Security Screen

Secure screen after

Check this box to specify that after a predefined period of keyboard or mouse inactivity the screen is secured. When the screen is secured, the login dialog will appear as soon as somebody tries to acces the computer. Set the period of time using the Minutes / Seconds counter.

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

Activation corner

A User can instantly secure his screen by placing the cursor in a corner. The default corner is the upper left corner of the screen. You can define another corner or deactivate this feature.

Allow backups of protected folders

Checking this box allows the backup of protected items. Normally the contents of folders to which the current User does not have access cannot be backed up. Enabling this option allows these items to be backed up provided the screen saver is active. For example, many organizations perform backups at night. To allow this, Users should be asked to leave their machines on with the screen saver active when they go home in the evening, allowing backups to take place.

Warning: Although the backup copy of an encrypted document remains encrypted, the backup copy of a protected folder is not protected. We therefore recommend you use this feature with caution. If this option is enabled, a malicious User could make a backup of your protected folders. It is important to strictly limit access to backup programs.

Shredder

Shred deleted files

When you trash a document its name is deleted from the disk directory. However, the actual data remains on the disk until it is overwritten by other data. Utilities are available to recover deleted files, therefore deleted data must be physically overwritten to ensure that it cannot be recovered. This process is referred to as shredding. Checking the Shred deleted files box allows you to shred files according to different security standards. When the Trash is being emptied, FileGuard automatically overwrites the disk space occupied by the deleted files, making it impossible to recover any data.

FileGuard offers several degrees of file shredding. The disk area can be overwritten once, three or seven times. Select the required degree in the pop-up menu.

FileGuard Menu

Show FileGuard menu

Check this box to display the FileGuard menu in the menu bar.

Show in menu

This feature allows you to specify which options appear in the FileGuard menu. Check the menu options you want to include in the FileGuard menu.

Shortcuts

Use the following procedure to define keyboard shortcuts for frequently used FileGuard commands such as for example, Protect:

1. Click the shortcut box next to a menu item.

2. Enter a key combination that includes one or more modifier keys and a function key or character. By “modifier keys” we mean the Control, Option, Shift or Command keys. “Character” refers to any letter or number.

To change a shortcut, simply click the shortcut box and enter a different key combination. To delete a shortcut, click the shortcut box and press the Delete key.

Note: *To help you memorize keyboard shortcuts, we recommend you use logical combinations. For example, type a key combination using the letter C to display the Configuration window, type a key combination using the letter P to protect items from within the Finder.*

Log Recording Options

Log Recording Options…

Click this button to display the Log Recording Options screen. Check the events you wish to be recorded in the log then click on OK. Refer to “Viewing the Log” on page 69 for further information.

Protecting Items

So far you have created and configured the Administrator, Users and any User Groups you require, and set general options that determine how FileGuard operates. You can now protect certain items on your system to prevent unauthorized access or use. By items we mean volumes, folders, applications and documents.

In the process of configuring FileGuard, you must protect your startup volume. You may want to protect important folders such as the System Folder and folders containing applications or important documents. You may also want to protect the applications themselves. Protecting documents is at your discretion.

Remember that without volume protection your Macintosh is not secure. This section explains how to set, change and remove passwords / privileges for volumes, folders, applications and documents.
Protecting an item involves selecting that item and then protecting it. FileGuard allows you to select and protect multiple items simultaneously by holding down the Shift key as you make your selection.

Protecting Volumes

A volume is protected with a password. As long as a volume is not protected, anyone can access its entire contents, even if FileGuard is installed. This can be done by starting up from a System disk or with extensions disabled so that the FileGuard extension is not loaded at startup. It is therefore essential to protect volumes.
Once a volume is protected, its password is only requested at startup if:

- The Ask volume password at startup box is checked.
- Someone starts up your Macintosh with another System disk.
- Someone starts up your Macintosh with extensions disabled.
- FileGuard is not installed on the startup volume.
- The copy of FileGuard used to protect the volume and the copy on the startup volume have different serial numbers.
- FileGuard is installed but the Guest is the only User. This is usually the situation before the Administrator has created any Users.

For the most part, the above situations do not apply to the normal day-to day use of FileGuard. Consequently, the volume password is not requested when Users log in at startup. This means that Users do not need to know the volume password to access the Macintosh.

Warning: *Do not give the volume password to anyone unless you want this person to have access to all items on the volume. If a User knows the volume password, he can start up the Macintosh without loading the FileGuard extension. Without this extension, the user configuration, general options, folder protection and authorized/unauthorized software is no longer valid. Only encrypted documents, protected volumes and individually protected applications remain secure.*

Because the startup volume's password is rarely requested, we suggest you write down a reference to the password and keep it in a safe place to prevent you from forgetting the password. Never write down the password itself. Refer to "Document, Application and Volume Passwords" on page 18 for further information.

Remember the following points concerning volume protection:

- Once a volume is protected, the protection is effective until it is removed.
- A volume remains protected even if the FileGuard extension is no longer installed.
- Volume protection works even if the Macintosh is shut down by a System error or power failure.
- All rewritable volumes, such as hard disks, partitions, removables and floppies, can be protected using FileGuard; CD-ROMs and DVD disks cannot.

Before Protecting a Volume

Before protecting a volume we recommend you take the following precautions:

1. Make a backup copy of your data.

2. Check your volume. A volume can contain minor defects that may cause problems when you protect it.

We recommend you check the state of your volume with the utility called Disk First Aid. This utility is included on the CD-ROM or on one of the System disks that came with your Macintosh.

3. Remove any automatic volume compression utilities such as Stacker® or TimesTwo® as they may interfere with volume protection. File level compressors such as StuffIt™ or DiskDoubler™ present no such problems.

4. Remove all other volume protection utilities as these will interfere with FileGuard's volume protection.

Setting Volume Protection

1. Select the volume in the Configuration window.

2. Choose Protect… from the Privileges menu. The following dialog is displayed:

Setting the Volume Password

1. Enter a password for the volume in the Volume Password text box.

2. Click the **Confirmation** text box, or press Tab, and re-enter the password.

If you have set a password, you can set password protection options:

1. Check the **Ask volume password at startup** box if you want the volume password to be requested at every startup.

This can be a useful option if you have set up two or more disk partitions. It allows you to protect one of them with a password. This ensures total privacy for the protected partition.

Check this option when protecting floppies or removables. This will ensure that the password is always requested, regardless of whether or not FileGuard is active when the disk or cartridge is inserted.

2. Click the **Message…** button to edit the text message that is displayed when the volume password is requested. 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 FileGuard 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.

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

3. Click on **OK.**

The volume is now password protected and is secure.

Protecting floppies and other removable media

FileGuard enables you to securely protect any mountable volume, including floppies and other removable media.This provides you with a safe way to send confidential information to others.
When a protected volume is inserted into a computer running FileGuard, it will demand the volume's password before the data on it becomes available.
If the recipient is not a FileGuard user, the volume will show a single application labeled "Open Me". All other contents will be securely locked and invisible. Double-clicking Open Me will inform the user that the volume is protected. It will allow him to install a small extension enabling his Macintosh to mount volumes protected by FileGuard (note that the extension cannot be installed if he started from a CD-ROM). After restarting, that user will be able to access the contents of any FileGuard protected volume, as long as the correct password for the volume is known.

Important: *If the Open Me application is visible, repair utilities like Disk First Aid™, Norton Disk Doctor™ or MacTools® must not be used to repair the protected volume. No files may be copied onto the volume and the Open Me application may not be removed from the volume as this may damage the data on the volume.*

Setting Volume Privileges

You can set privileges for a volume just as you would for a folder. Setting these privileges is optional and depends on your working environment. You can set volume privileges for the following user categories:

• The **Owner.**

• The **Group** of Users with whom the volume is shared.

• **Everyone.** All Users other than the Owner or the members of the Group.

You set, change and remove privileges for a volume in exactly the same way as in File Sharing. For more information on File Sharing, refer to your Macintosh User's Guide or Networking Reference Guide, or to your on-screen AppleGuide Tutorial.

To set volume privileges:

1. Select the volume in the Configuration window.

2. Choose Protect… from the Privileges menu. The volume protection dialog is displayed.

3. Refer to “Setting Folder Privileges” on page 48 for the remaining steps in setting volume privileges.

Important: *The* ***See Folders*** *and* ***See Files*** *privileges are not available for volumes. They are always enabled because your Macintosh requires these privileges in order to work properly.*

Changing Volume Protection

You can change volume protection at any time, for example to change the password:

1. Select the volume in the Configuration window.

2. Choose Get Privileges… from the Privileges menu.

3. Change volume password, options or folder protection. Refer to “Protecting Volumes” on page 40 for more information.

4. Click the close box then click on **Save.**

Removing Volume Protection

You can remove volume protection at any time, for example before you optimize a volume or re-install a driver. To remove volume protection:

1. Select the volume in the Configuration window.

2. Choose Remove Protection… from the Privileges menu.

3. Enter the password for the selected volume and click on **OK.**

The volume is now unprotected. Volume privileges are also removed.

Warning: Never leave a volume unprotected unless absolutely necessary. The contents of an unprotected volume are accessible if the machine is started with another startup volume or with extensions disabled. Starting a machine this way ensures that FileGuard does not load. The contents of encrypted documents, however, remain protected at all times.

Emergency Remove

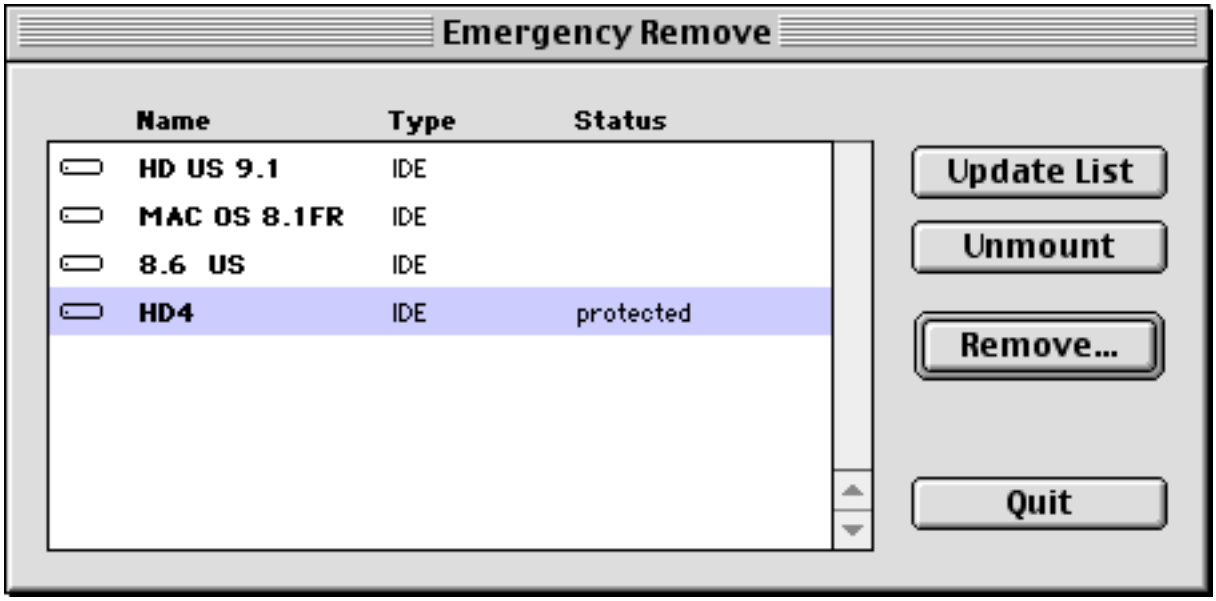
Even under the best of conditions, hard drive directories and files can become corrupted. In most cases, disk repair utilities can fix such damage quickly. Should your volume's protection itself become damaged, however, the procedure to remove it as described above may not work properly. In such cases,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

2. Double-click the Emergency Remove application.

The following dialog appears:



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. The volume now appears in the list.

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

The volume's protection is now removed.

Protecting Folders (System 7.x)

If you are using Mac OS 8.x, please skip this section and read “Protecting Folders (Mac OS 8.x)” on page 52.

You protect a folder by setting access privileges for Users and Groups. Depending on the privileges, protecting a folder prohibits unauthorized access or prevents it from being deleted or modified. You can set privileges for the following user categories:

- The **Owner.**

- The **Group** of Users with whom the volume is shared.

- **Everyone.** All Users other than the Owner or the members of the Group.

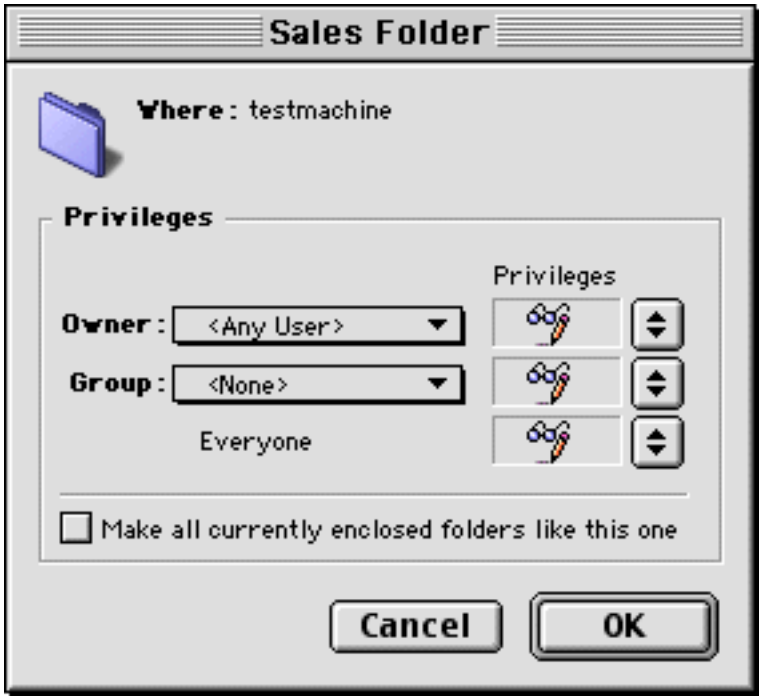
You set, change and remove privileges for a volume in exactly the same way as in File Sharing. For more information on File Sharing, refer to your Macintosh User’s Guide or Networking Reference Guide, or to your on-screen AppleGuide Tutorial.

Groups are essential for setting up folder protection. For information on creating groups, refer to “Creating a Group” on page 34.

Setting Folder Privileges

1. Locate and select the folder you wish to protect.

2. Choose Protect… from the Privileges menu. The following dialog is displayed:



Note: The name of the selected folder appears in the title bar.

3. Choose an owner for the folder using the **Owner** pop-up menu. The **Owner** pop-up menu displays all Users within Users and Groups.

Note: *Only the owner can change access privileges.*

4. Choose the **group** with whom you wish to share the folder using the **Group** pop-up menu. The Group pop-up menu displays all groups within Users and Groups.

5. Enable / disable the **See Folders** option for each user category. If enabled, this option allows Users to see all sub-folders within the folder you are protecting.

6. Enable / disable the **See Files** option for each user category. If enabled this option allows Users to see all files within the folder you are protecting.

7. Enable / disable the **Make Changes** option for each user category. If enabled this option allows Users to add and delete items or modify documents within the folder you are protecting. If disabled the Users will not be able to modify the folder's contents.

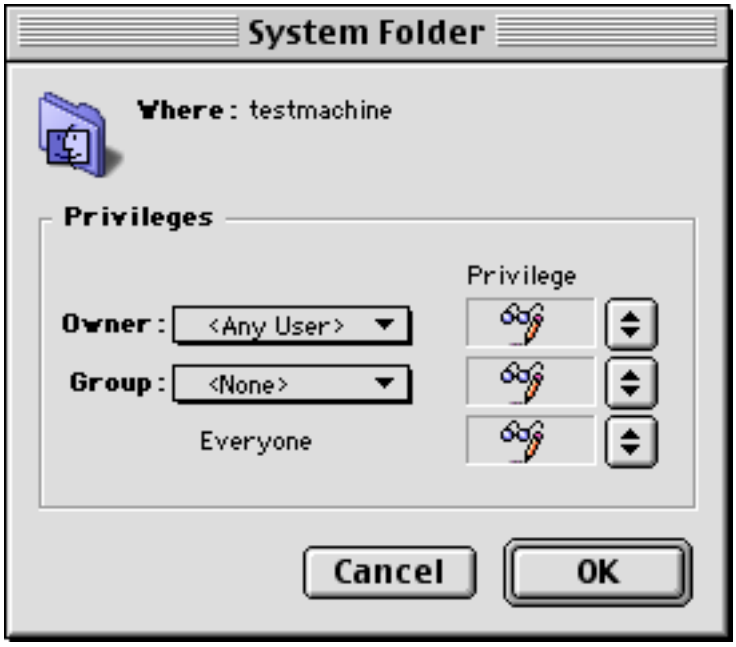
8. Enable the **Make all currently enclosed folders like this one** option to copy the privileges you have just set up to all folders held in the current folder. This provides consistency of security for all enclosed folders.

9. Click **OK** to protect the folder.

Protecting Special Folders

The System Folder

The **See Folders** and **See Files** options must be enabled because your Macintosh requires access to the items inside the System Folder in order to run properly. These options are therefore not available to prevent them from being disabled. You can however prevent Users from opening the System Folder. This way you are certain they cannot copy or gain access to files and folders located inside the System Folder and modify their contents. The **Make Changes** option is available and can therefore be disabled.



Note: *The folders inside the System Folder can be protected as normal folders. Some of these folders, such as Preferences and PrintMonitor Documents, require the Make Changes option to be enabled because certain applications and the System both need to write in them. The folders that require the Make Changes privilege depend on the software you are using. Unfortunately, we cannot list all folders which require the Make Changes privilege because new versions of software may differ from previous versions.*

Folders containing applications

The **See Folders, See Files** and **Make Changes** options are available for these folders and can therefore be disabled. However, some applications need to write within their own folder and will not run properly if Make Changes is disabled.

For folders containing this type of application, you must leave Make Changes enabled.

The Desktop Folder

The **See Folders** option must be enabled because your Macintosh requires access to the folders on the Desktop in order to run properly. The option is therefore unavailable to prevent it from being disabled. The Make Changes and **See Files** options are available and can be disabled.

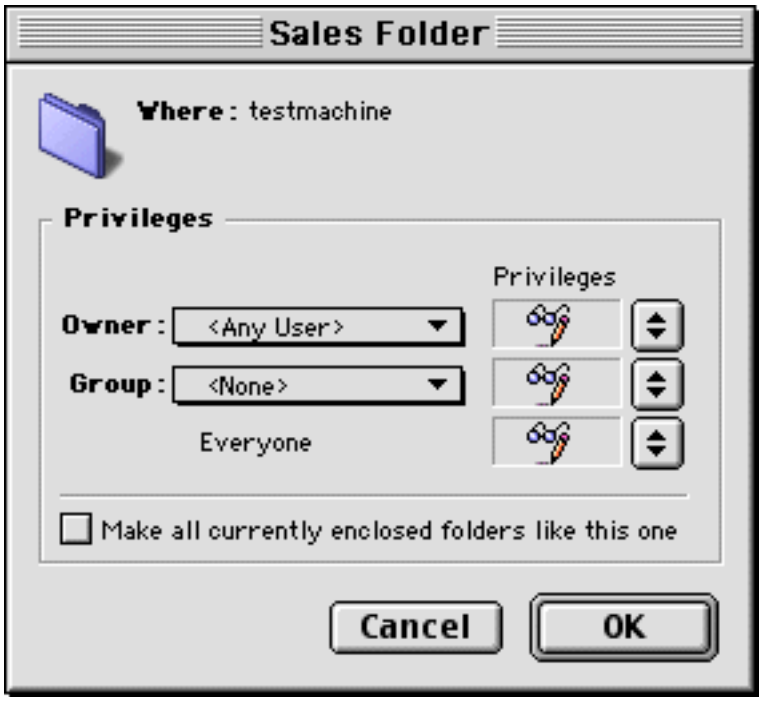
The Trash

This folder cannot be protected. If you do not want Users to trash items, put those items in folders for which the User does not have the **Make Changes** privilege.

Changing Folder Privileges

1. Locate and select the folder whose privileges you wish to change.

2. Choose Get Privileges… from the Privileges menu. The following dialog is displayed:



3. Change the See Files, See Folder or Make Changes options for the three user categories.

4. Click the close box then click on Save.

Removing Folder Privileges

1. Locate and select the folder whose privileges you wish to remove.

2. Choose Remove Protection… from the Privileges menu.

3. Choose whether to remove privileges for the selected folder or for all enclosed folders.

Protecting Folders (Mac OS 8.x)

The version of File Sharing which comes with Mac OS 8 differs from previous versions.

The new version of FileGuard has been adapted for Mac OS 8 in order to offer you the same level of protection as with the new version of File Sharing.

You protect a folder by setting access privileges for Users and Groups. Depending on the privileges, protecting a folder prohibits unauthorized access or prevents it from being deleted or modified. You can set privileges for the following user categories:

- The **Owner.**
- The **Group** of Users with whom the volume is shared.
- **Everyone.** All Users other than the Owner or the members of the Group.

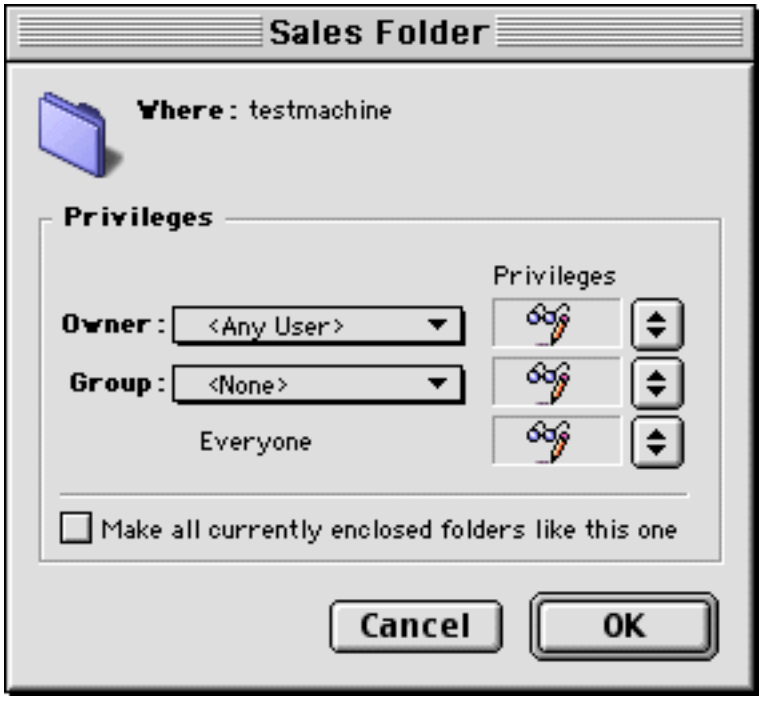
You set, change and remove privileges for a volume in a similar way as in File Sharing. For more information on File Sharing, refer to your Macintosh User's Guide or Networking Reference Guide, or to your on-screen AppleGuide Tutorial.

Groups are essential for setting up folder protection. For information on creating groups, refer to "Creating a Group" on page 34 of the FileGuard Administrator's Manual.

Setting Folder Privileges

1. Locate and select the folder you wish to protect.

2. Choose Protect… from the Privileges menu. The following dialog is displayed:



Note: *The name of the selected folder appears in the title bar.*

3. Choose an owner for the folder using the Owner pop-up menu. The Owner pop-up menu displays all Users within Users and Groups.

Note: *Only the owner can change access privileges.*

4. Choose the group with whom you wish to share the folder using the Group pop-up menu. The Group pop-up menu displays all groups within Users and Groups.

5. Choose the privileges for each user category. Clicking on the pop-up menu icon on the right of each user category pops up the menu which lets you choose between the different privileges: Read & Write, Read only, Write only (Drop Box) and None.

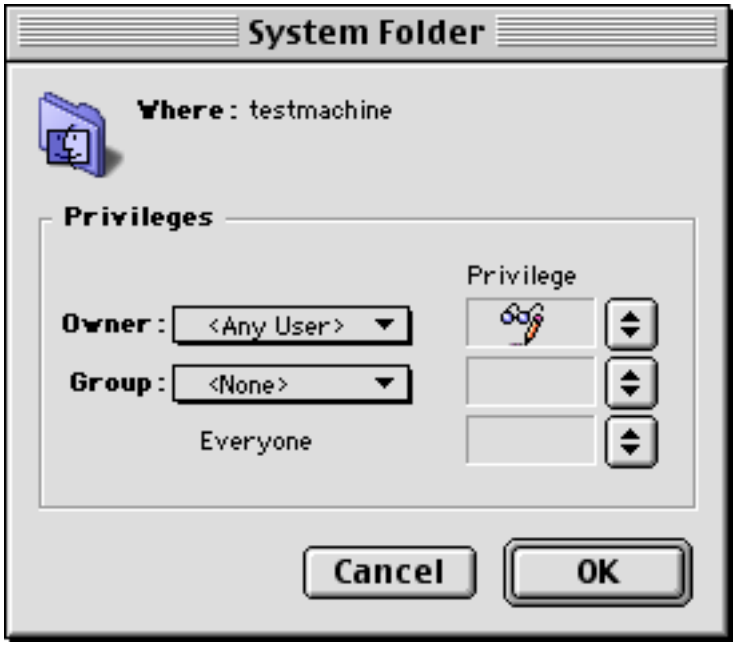
6. Enable the **Make all currently enclosed folders like this one** option to copy the privileges you have just set up to all folders held in the current folder. This provides consistency of security for all enclosed folders.

7. Click **OK** to protect the folder.

Protecting Special Folders

The System Folder

Your Macintosh requires access to the items inside the System Folder in order to run properly. You can however prevent Users from opening the System Folder. This way you are certain they cannot copy or gain access to files and folders located inside the System Folder and modify their contents. If you do not grant privileges to a user category, the Users who are part of the category will not be able to open the System Folder and will not be able to make any changes to it.



Note: *The folders inside the System Folder can be protected as normal folders. Some of these folders, such as the Preferences folder, require to remain unprotected because both certain applications and the System need to write into them. The folders that require to remain unprotected depend on the software you are using. Unfortunately, we cannot list all folders which require to remain unprotected because new versions of software may differ from previous versions.*

Folders containing applications

Applications located in folders for which the privileges are **Write Only** or None, cannot be seen by the User and can thus not be used by that User. Therefore, Users always need to have at least the **Read Only** privilege on folders which contain applications they must use.

Furthermore, some applications need to write inside their own folder. These applications will run properly only if the User has **Read & Write** privileges for the folders where the applications are located.

The Desktop Folder

Only the **Read & Write and Read Only** privileges are available for the Desktop Folder because your Macintosh requires access to the folders on the Desktop in order to run properly.

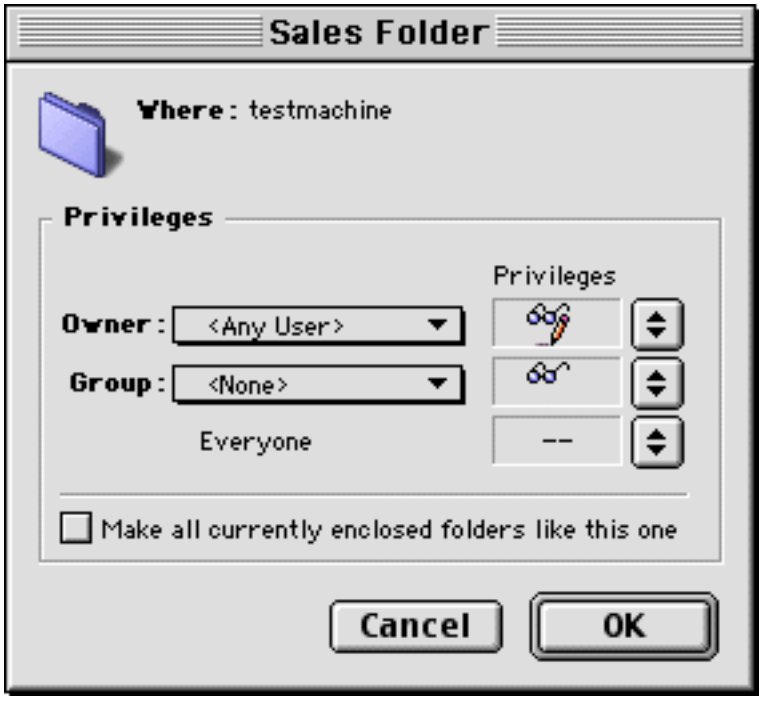
The Trash

This folder cannot be protected. If you do not want Users to trash some items, put those items in folders for which the Users only have the **Read Only** privilege.

Changing Folder Privileges

1. Locate and select the folder whose privileges you wish to change.

2. Choose Get Privileges… from the Privileges menu. The following dialog is displayed:



3. Change the privileges for the three user categories.

4. Click the close box then click on **Save.**

Removing Folder Privileges

1. Locate and select the folder whose privileges you wish to remove.

2. Choose Remove Protection… from the Privileges menu.

3. Choose whether to remove privileges for the selected folder only or also for all enclosed folders.

Protecting Applications

Important: *Due to the way they are implemented, it is not possible to apply individual protection to PowerPC native applications.*
Fat binary applications can be protected, but the protection will only be effective in 68000-compatible mode.

You protect an individual copy of an application by setting a protection password and then setting any of the following three options:

- The Usage Password. This ensures that only Users who know this password can use the protected application. The password is asked every time the application is launched, even if the application is copied to another machine.

  Alternatively, you can also restrict the use of applications using the list of Authorized Software or Folder protection. Protecting software using the list of Authorized Software protects all copies of the named application, whereas the usage password protects individual copies. Refer to “Authorizing / Unauthorizing Software” on page 63 and “Protecting Folders (System 7.x)” on page 47 for further information.

  For example, if you want to protect your MacWrite application by using the Usage Password protection, no one will be able to run this particular copy of the application without knowing the password. However, the User can still copy another MacWrite application onto your hard disk and run it. If you want to prevent MacWrite from being run on your computer, we suggest you use the Authorized Software protection.

- **Demo Application.** This feature allows you to create demo or trial versions of applications.

- **Copy Protection.** This ensures that a copy of your protected application cannot be run on any other Macintosh, even if FileGuard is installed on that machine. This feature prevents the unauthorized copying of software.

Note: *You can also restrict the copying of all applications. Refer to “Software” on page 31 within the User Options section for further information.*

These types of application protection can be used separately or in any combination. In order to set any of the three application protection options, you must first set a protection password. The User is asked for this password if he attempts to change or remove the privileges for this application. This password ensures that only Users with the protection password can alter the application privileges.

Setting Application Protection

1. Locate and select the application you wish to protect.

2. Choose Protect… from the Privileges menu.

The following dialog is displayed:

3. Enter a protection password for the application.

4. Click the Confirmation text box, or press Tab, and re-enter the protection password.

5. Set the application protection options. These are explained in the following sections.

6. Click on **OK.**

Usage Password

Check the **Require password to use the application** box if you wish to password protect the use of the application. This ensures that only Users who know the usage password can use the protected application. The usage password is requested every time the application is launched, even if the application is copied to a machine that is not running FileGuard. If you choose to check the box:

1. Click the password text box and enter a usage password.

2. Click the Confirmation text box, or press Tab, and re-enter the usage password.

Demo Application

This feature allows you to create demo or trial versions of programs. FileGuard includes two types of demo protection which can be used individually or together:

• The **Limit number of launches** checkbox. Enable this option to limit the number of times the protected application can be launched. Enter the number of permitted launch attempts in the text box.

• The **Limit time of use** checkbox. Enable this option to set a maximum amount of time during which the protected application can be used. Set the period of time using Hours / Minutes / Seconds counter.

Note: *The application can be used for longer than the set period in a single session, but it is not possible to quit and re-enter the application once the set period has been exceeded.*

You can also distribute demo protected applications for use on another Macintosh. To do this, copy the application to a floppy before you demo protect the application as described above. Whenever you give someone a floppy containing an application protected in this way, make sure you also give them the following instructions:

1. Insert the floppy into the drive and copy the application onto another volume.

2. Start the application by double-clicking its icon on the volume you copied the application to.

Copy Protection

This feature prevents unauthorized copying of software. Check the Copy Protection box to ensure that a copy of your protected application cannot be run on any other Macintosh, even if FileGuard is installed on that machine.

Note: *When demo application options are set, the application may not be copied because any copy of the protected application could again be launched the set number of times or be used during the set period.*

Therefore, the copy protection option is then set automatically and grayed out so it cannot be changed.

Changing Application Protection

1. Locate and select the application.

2. Choose Get Privileges… from the Privileges menu. A dialog is displayed requesting the application's protection password.

3. Enter the appropriate password and click on **OK.**

4. Change the options.

5. Click the close box then click on **Save.**

Removing Application Protection

To remove application protection:

1. Locate and select the application.

2. Choose Remove Protection… from the Privileges menu.

3. Enter the application's protection password.

4. Click on **OK.** The application is now unprotected.

Protecting Documents

You protect documents by encrypting their contents. This prevents unauthorized Users from reading them. FileGuard offers four encryption algorithms:

- D.E.S. (Data Encryption Standard). This algorithm was adopted as a federal standard in 1976 and authorized for use on all classified government communications. Since then D.E.S. has become an international standard.

- Triple-D.E.S. is a D.E.S. variant. It encrypts data three times in succession, using a different key each time.

- IDEA™ (International Data Encryption Algorithm). This is the most secure algorithm included in FileGuard

- FastCrypt is an algorithm especially written for FileGuard. It is less secure than the other algorithms but is very fast, making it almost transparent in use.

Encrypting a Document

1. Locate and select the document you want to protect.

2. Choose Protect… from the Privileges menu. The following dialog box is displayed:

Important: *FileGuard allows you to protect multiple documents simultaneously. To do this, hold down the Shift key as you select the documents to be protected. Only one window will appear and all documents will be protected with the same password and options.*

Refer to “Opening an Encrypted Document” on page 84 for more information on the use of encrypted documents.

Setting the Document Password

1. Enter the password for the document(s).

2. Click the Confirmation text box or press Tab, and re-enter the password.

Setting Document Encryption Options

1. Select an encryption method from the Encryption Algorithm pop-up menu.

2. Check the Self decrypting document box if you need to pass the document to Users who do not have FileGuard installed on their machines.

Normally encrypted documents cannot be read unless FileGuard is installed on the Macintosh. Enabling the Self decrypting document option means that documents can be read on any Macintosh provided the recipient knows the correct password.

An application is created which contains the encrypted document. When the recipient double-clicks this application, the password is asked. If he enters the correct password, the document is decrypted and opened in the application which created the original document.

This feature provides a secure method of transmitting sensitive documents electronically without worrying about interception.

3. Click on **OK.**

The application FileGuard Engine now starts encrypting the selected documents in the background. If you want to see the encryption progression, you can bring FileGuard Engine to the front by selecting it in the applications menu.

Changing Document Protection

You can change a documents protection at any time, for example if you want to change the encryption method or the password:

1. Locate and select the document whose protection you want to change.

2. Choose Get Privileges… from the Privileges menu. The following dialog is displayed:

3. Enter the appropriate password and click on OK. The document protection dialog appears.

4. Change the password, encryption algorithm or self decrypting status.

5. Click the close box then click on Save.

The application FileGuard Engine now starts changing the document’s protection in the background.

Decrypting a Document

You remove document protection by decrypting the document:

1. Locate and select the document you want to decrypt.

2. Choose Remove Protection… from the Privileges menu.

3. Enter the password for the document.

4. Click on **OK.**

The application FileGuard Engine now starts decrypting the selected documents in the background.

Authorizing/Unauthorizing Software

So far you have created and configured the Administrator, Users and any User Groups you require, set general options and protected items. You can now decide whether to authorize or unauthorize applications, control panels and desk accessories.

Note: *Compiled AppleScripts, like the items you find in the Automated Tasks folder under the Apple menu, are applications. Don't forget to set authorizations for these items appropriately.*

You may already have protected some applications. For example, you may have placed some applications inside protected folders or you may have protected certain applications with passwords. These methods protect specific copies of the software.

A User could still introduce a second copy of the software which would not be affected by this protection. You can prevent this from happening by authorizing / unauthorizing software on your machine. We strongly suggest that you decide whether to authorize / unauthorize software when you first install and configure FileGuard. The approach you choose will depend on your requirements.

Note: *Authorizing/Unauthorizing software does not affect the Administrator. When you log in as the Administrator you can run any software. If you want a particular User to run any software as well, you can allow him to do so by enabling the Use any software option in his User Configuration. Refer to "Software" on page 31 for further information.*

Authorizing Software

Authorizing software allows you to control which software is run on your Macintosh. Once this process is completed, you can be sure your Users cannot install games or introduce unknown, potentially contaminated, software. Authorizing software therefore increases security by reducing the chance of virus infection or system attack by low level utilities.

If you specify certain software as authorized, all other software is treated as unauthorized and will not run on your Macintosh. As a result, you may be required to regularly modify the authorized software list. We recommend that you choose to authorize certain applications and define all others as unauthorized.

Example: *If you know in advance the applications you and your Users need, you can set up a list of authorized software and leave all other software as unauthorized. A work group may use a particular word processor, spreadsheet and database. Their software requirements are therefore well defined, so you can authorize the specific applications they need. The use of all other software will be forbidden.*

Unauthorizing Software

If you specify certain software as unauthorized, be aware that all other software is authorized and will run on your Macintosh. Since it is impossible to list all existing software, this feature will only be useful in specific cases like the situation described in the example below. Therefore, we recommend you make a list of Authorized Software rather than a list of Unauthorized Software.

Example: *A college professor who runs a programming lab allows his students to experiment with many pieces of software but wishes to exclude certain applications. He can set up a list of unauthorized software. Remember that if you specify some software as unauthorized, all other software will run on your machine.*

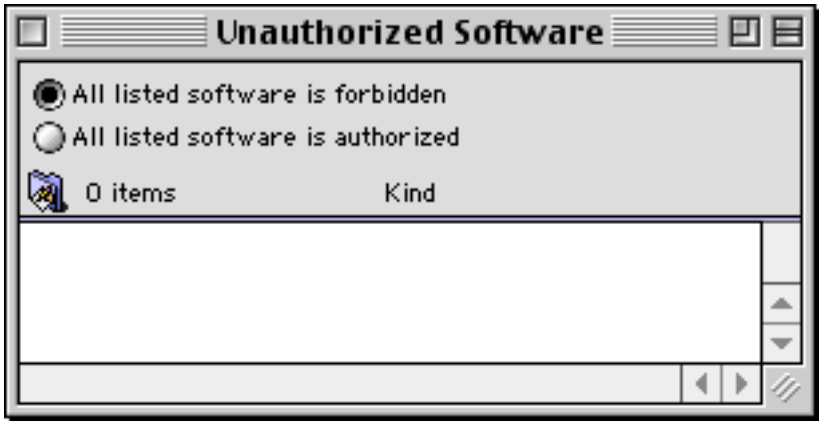
Defining Authorized Software

The following process creates a list of authorized software.

We recommend you use this approach.

1. Double-click the Unauthorized Software icon in the Configuration window.

The Unauthorized Software window is displayed. The list is empty if you have not performed this operation before:



2. Click the **All listed software is authorized** radio button to set up a list of authorized software.

3. Use one of the following methods to select the software to be authorized. The method you choose depends on how much of your software you need to protect:

- To authorize a minority of your software, locate the software you wish to authorize in the Configuration window then drag your selection onto the Authorized Software window. Alternatively, select the software and choose Authorize Selected Software from the Software menu.

- To authorize the majority of your software, choose Authorize all Applications, Control Panels or Desk Accessories from the Software menu, depending on the type of software you wish to authorize. You are asked if you wish to search all volumes or the startup disk only. Click the option you require. If your Macintosh has only one hard disk both options give the same result. FileGuard scans the selected volumes for the specified software type. When the scan is complete the authorized software is listed in the Authorized Software window.

So far you have authorized some or all of the software on your Macintosh. You can now selectively unauthorize items. This allows you to make changes to your list or correct any mistakes:

1. Click the item you wish to unauthorize in the Authorized Software window. Hold down the Shift key to select multiple items.

2. Choose Unauthorize Selected Applications from the Software menu. The items you selected disappear from the list of Authorized Software. Dragging items from the Authorized Software window into the Trash also has the same effect.

3. Click the close box.

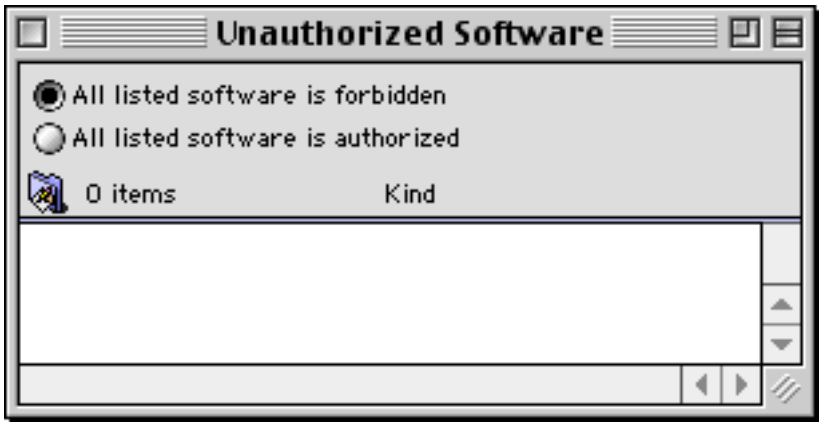
Note: *Make sure you authorize the FileGuard application as it is needed to protect items. Do not forget to include or leave out software which is used by the System, such as PrintMonitor or Chooser.*

Defining Unauthorized Software

The following process creates a list of unauthorized software. Only use this approach if you are sure it is appropriate.

Note: *To unauthorize software you must have a copy of that software installed on your volume while you set up the list of unauthorized software. Once the list is complete you can remove the unauthorized software and copy the list to other machines if necessary.*

1. Double-click the Unauthorized Software icon in the Configuration window. The list is empty if FileGuard is installed for the first time:



2. Click the All listed software is forbidden radio button to set up a list of unauthorized software.

3. Use one of the following methods to select software to be unauthorized. The method you choose should be determined by how much of your software you need to protect:

- To unauthorize a *minority* of your software, locate the software you wish to unauthorize in the Configuration window then drag your selection onto the Unauthorized Software window. Alternatively, select the software and choose Unauthorize Selected Software from the Software menu.

- To unauthorize a majority of software, choose Unauthorize all Applications, Control Panels or Desk Accessories from the Software menu, depending on the type of software you wish to unauthorize. You are asked if you wish to search all disks or the startup volume only. Click the option you require. FileGuard scans the volumes and when the scan is complete, the unauthorized software is listed in the Unauthorized Software window.

So far you have unauthorized some or all of the software on your Macintosh. You can now selectively authorize software. This allows you to make changes to your list or correct any mistakes:

1. Click the item you wish to authorize in the Unauthorized Software window.

Hold down the Shift key to select multiple items.

2. Choose Authorize Selected Applications from the Software menu.

The items you selected disappear from the Unauthorized Software. Dragging items from the Unauthorized Software window into the Trash also has the same effect.

3. Click the Close box.

The Log

FileGuard logs many activities on your Macintosh. This allows you to see which Users have performed what actions and at what time. It is useful for tracking attempts to bypass FileGuard's security.

The logged events can be divided into four groups:

1. Macintosh operation

- Macintosh switched on
- Macintosh shut down
- Crash
- Error

2. Application and control panel usage

- Application opened
- Application quit
- Control panel opened
- Attempt to use unauthorized application
- Attempt to use unauthorized control panel

3. User actions

- Wrong user password
- Wrong user name
- User password modified
- User changed the clock
- User tried to change the clock

4. Administration actions

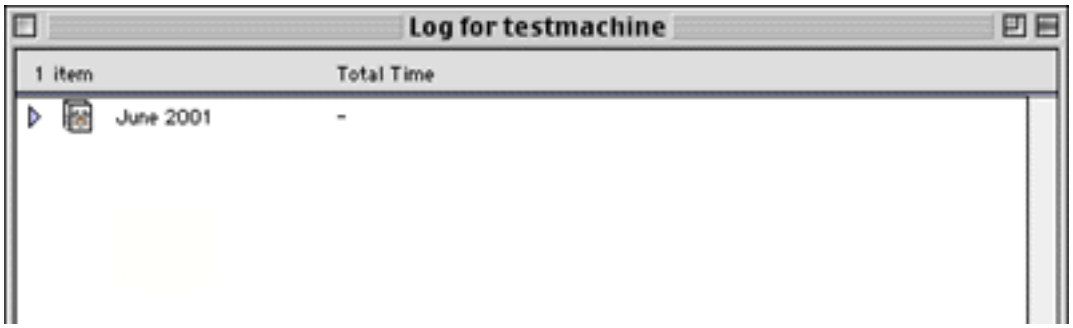
- Volume protected
- Volume protection removed
- Folder protected
- Folder protection removed
- Application protected
- Application protection removed
- File protected
- File protection removed
- Protected file opened

You determine which events will be recorded in the log by checking them in the Log Recording Options dialog. To open this dialog, click the Log Recording Options button in the Options dialog. Refer to “Log Recording Options” on page 39 for further information.

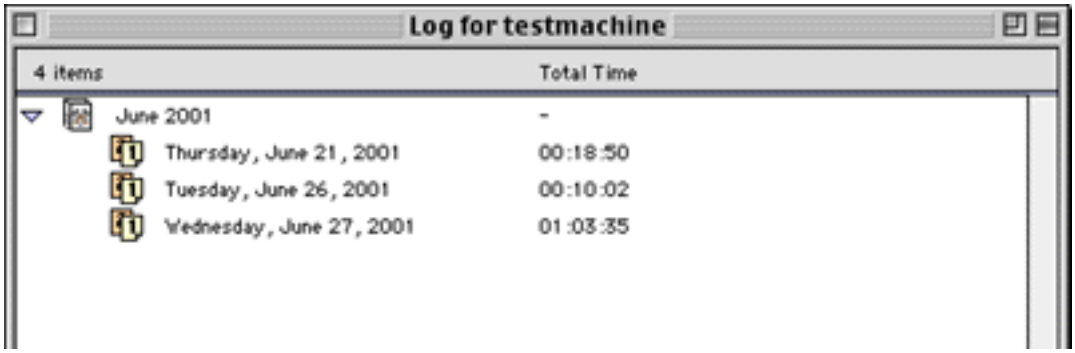
FileGuard allows you to filter the log to focus on specific events. To do this you can define filters. For example, if you wish to focus on log-in attempts, you can create a filter that only displays these events.

Viewing the Log

1. Double-click the Log icon in the Configuration window. The Log menu appears on the menu bar and the Log window is displayed. It includes an icon for each month that FileGuard has been installed:

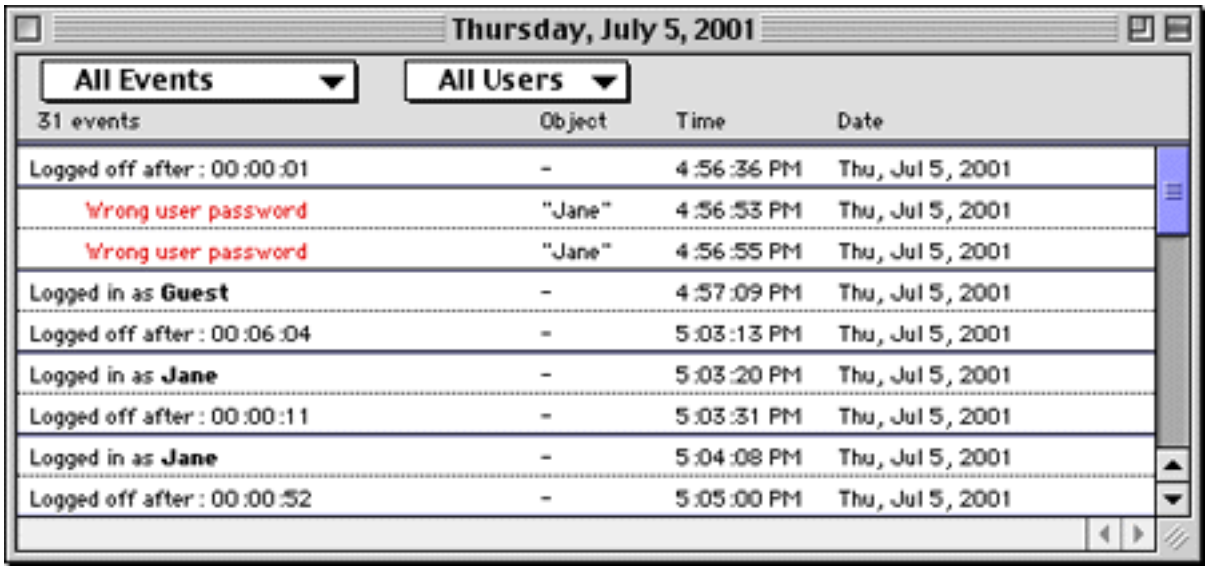


2. Double-click the icon of the month you wish to view. That month’s window is displayed:



Each icon represents the log entry for one day. The Total Time column shows how long the Macintosh has been in use during that day.

3. Double-click the day you wish to view. The log for the selected day is displayed, for example:



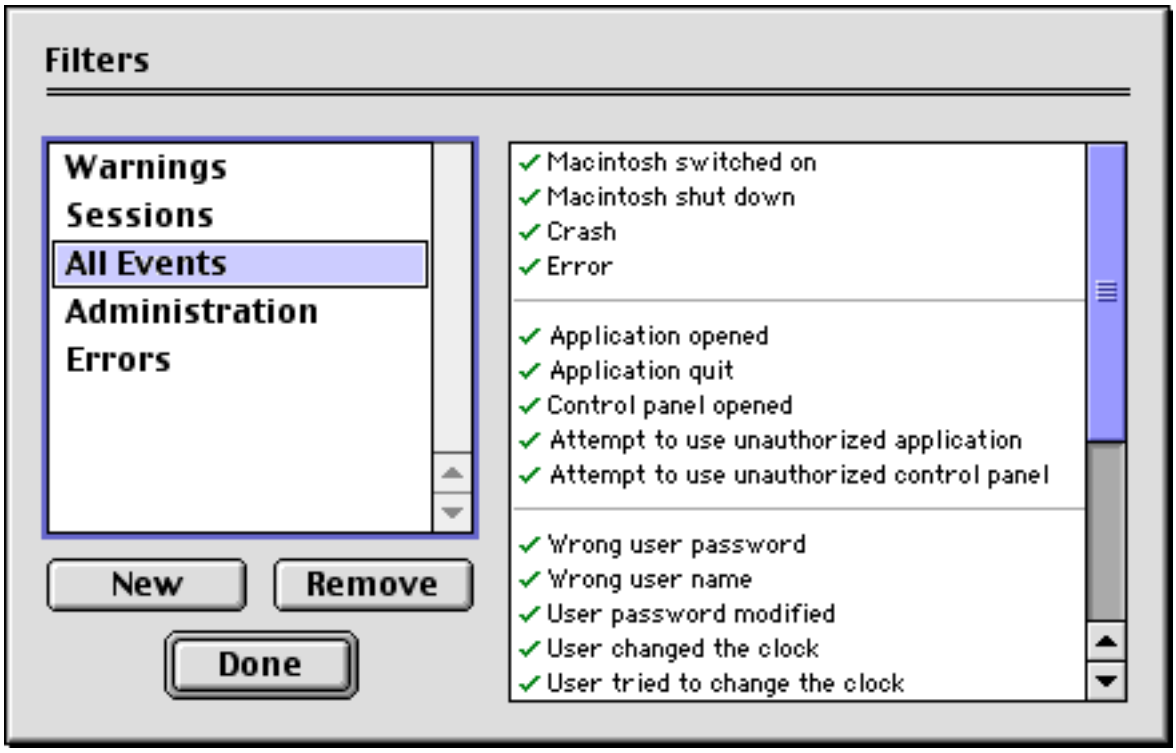
Log Filters

A filter is a means of specifying which events are shown in the FileGuard log. The pop-up menu in the Log window contains filters that allow you to specify the type of events to be displayed. The following sample filters are available:

- All Events: Choose this option to display the complete log for the selected day.
- Warnings: Choose this option to display all warnings issued on the selected day.
- Sessions: Choose this option to display the start and end of all sessions on the selected day.
- Administration: Choose this option to display the log of all the actions performed by the Administrator on the selected day.

The pop-up menu also contains the Edit Filters item. This allows you to view which events the sample filters contain, and also lets you edit the sample filters and create and edit your own filters.

For example, you can monitor a specific activity, such as login attempts, if you suspect a breach of security is taking place. To create or edit a filter, choose Edit Filters… from the Filters pop-up menu. The following dialog is displayed:



Only the checked events will be shown when the filter is used.

Note: *The Edit Filters… option is also available from the Log menu.*

Creating a New Filter

1. Click on **New.** A new filter called “Untitled” is created. Its name is highlighted, ready to be changed.

2. Enter a name for the filter.

3. Check those events on the event list you want to be included in the filter.

Renaming a Filter

1. Click the filter to be renamed.

2. Enter a new name.

Removing a Filter

1. Click the filter to be deleted.

2. Click on **Remove.**

Editing Filter Events

1. Click the filter to be edited.

2. Check the events you want to include in the filter.

Ending the Editing Session

When you have finished editing, click on **Done.**

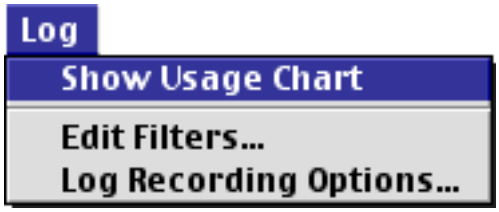
Saving and Printing the Log

1. Select the log to be saved.

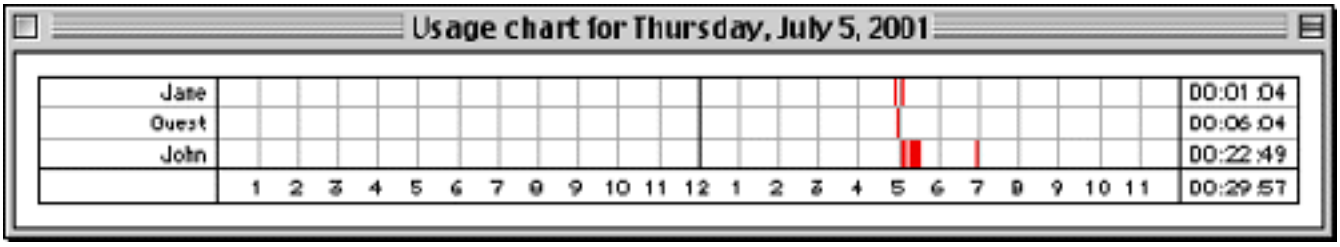
2. Choose Save As or Print from the File menu.

The Usage Chart

The usage chart is a graphical representation of user sessions on the Macintosh. It allows you to track machine usage by User or to monitor the amount of time spent on a particular project. To display the usage chart, choose Show Usage Chart… from the Log menu.



The usage chart for the selected day is displayed:



Each block represents a user session.

The Usage Chart as a Project Time Monitor

As well as showing you who has used your machine and for how long, the usage chart can also be used to monitor the amount of time spent on projects. This feature is useful in situations where work is invoiced at an hourly rate and you need an accurate record of how long a project has taken.

1. Set up each project as a User. To do this, open the Users and Groups window and create a new User named after each project, for example “The Wilson Account.”

2. Log in as “The Wilson Account” when you or others wish to work on that project.

3. Check the usage chart to see exactly how much time has been spent on the project.

Magnifying the Usage Chart

You can zoom in on an activity block to see the start and end times for that block. By default the usage chart is divided into hourly units. You can zoom six times, allowing you to display the activity block start and end times within five seconds. To zoom in:

• Move the cursor over the area you wish to inspect. The cursor shape changes to a magnifying glass enclosing a plus sign, indicating that the view is to be magnified. Click to increase the magnification.

To zoom out:

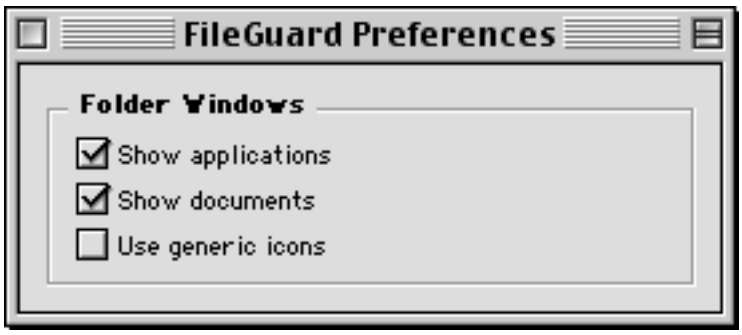
• Move the cursor over the activity block area. Hold down the option key. The cursor shape changes to a magnifying glass enclosing a minus sign, indicating that the view is to be reduced. Click to decrease the magnification.

Additional Features

This section describes FileGuard features not covered so far.

Preferences

Choose Preferences from the File menu. The FileGuard Preferences dialog is displayed:



The options are explained below:

Show applications

Check this box to include applications when displaying the contents of a volume in the Configuration window. Uncheck this box if you need to reduce the size of the Configuration window to a more manageable size.

Show documents

Check this box to include documents when displaying the contents of a volume in the Configuration window. Uncheck this box if you need to reduce the size of the Configuration window to a more manageable size.

Use generic icons

Check this box if you prefer to view generic icons instead of the standard icons. This allows a faster display of the windows' contents.

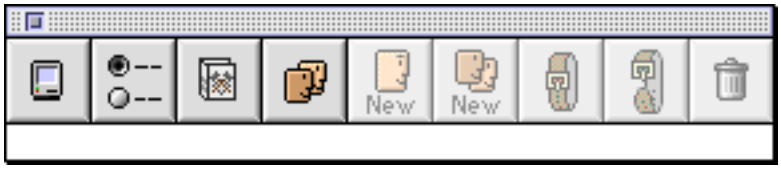
Printing

You can print any window within the FileGuard application by choosing Print from the File menu.

The Toolbar

The toolbar includes buttons representing several commonly used FileGuard menu options. Click these icons as a shortcut to a particular dialog or window. You can leave the toolbar on your screen all the time. To use the Toolbar:

1. Choose Show Toolbar from the Window menu. The Toolbar is displayed:



The actions associated with each button appear under the buttons when you pass over them. The actions are: Configure, Show Options, Show Log, Open Users and Groups, New User, New Group, Protect, Remove Protection, Delete.

2. Click a button to display the associated dialog box or window. When the action represented by a button is not available, the button is grayed-out. The protect and remove protection buttons are only available after you have selected an item.

Get Info

The Get Info item in the File menu provides information on any item relevant to the FileGuard protection. This information can be useful when setting, changing or removing privileges and protection. To use the Get Info option:

1. Locate and select an item in the Configuration window.

2. Choose Get Info in the File menu. The window containing the information on the item is displayed. The information displayed depends on the type item you selected.

Saving and Using Configurations

This section explains how to save and copy configurations between machines.

Saving Configurations

Saving your Macintosh's configuration allows you to:

- Re-use the configuration at a later date. Configurations are saved as files that can be stored until required.

- Copy the configuration between machines. This gives you a quick way to duplicate the exact configuration of one machine onto another. Configuration files can be copied over a network or distributed on floppy.

To save your machine's configuration, select an item in the Configuration window and:

- Drag it onto the desktop.

or

- Choose Save item… from the File menu. Enter a name for the configuration file, select the location and click on Save.

Both methods create a file that contains the configuration for the selected item.

You can save configurations for the following items:

- Individual Users
- Groups
- Users and Groups
- Options
- Authorized Software

You can also save the complete configuration of your Macintosh. The complete configuration includes Individual Users, Groups, Users and Groups, Options, Lists of Authorized Software together and all folder privileges. This is useful if you wish to remove FileGuard from your machine and then re-install it at a later date. This option also simplifies copying configurations between machines.

To save your complete configuration:

1. Open the Configuration window and make sure no items are selected in the window.

2. Choose Save Complete Configuration… from the File menu.

3. Enter a name for the configuration file, select an appropriate location and click on Save.

A file containing the complete configuration for your Macintosh is created in the location you specified.

Note: *When you save your computer's complete configuration, FileGuard also creates a snapshot of all the folders that were protected at that time, named "Folder Privileges". If you later reinstall FileGuard or copy your saved configuration to another computer, FileGuard uses this list to update the folder privileges so that they match your saved configuration.*

Editing Saved Configurations

If you have a saved configuration and you want to make changes to it:

1. Choose Open File from the File menu.

2. Select the file you want and click on Open. The relevant dialog opens ready for you to edit the settings.

3. Make any necessary changes.

4. Click on Save.

Note: *You cannot edit the Folder Privileges item inside a saved complete configuration file. FileGuard allows you to open this item to review the saved folder privileges only. If you will not need to restore these folder privileges, you can delete this item from the configuration file by dragging it to the Trash.*

Using Saved Configurations

You can copy saved configurations. Configuration files can be copied over a network or distributed on floppy. Use the saved file on another Macintosh by dragging the saved file into the Configuration window. For example, if you have saved an Options configuration file and wish to use those settings on another machine, simply copy the file to the other Macintosh, then copy the Options file into the Configuration window of that machine.

CHAPTER THREE - USING FILEGUARD

So far in this manual we have explained how to configure FileGuard and protect items from within the FileGuard configuration application. This chapter explains the day-to-day use of FileGuard from the FileGuard menu in the Finder. It describes:

- Logging in.
- Logging off.
- Locking the screen.
- Changing your user password.
- Protecting items from within the Finder.
- Viewing the Log.
- Configuring FileGuard.

The FileGuard menu is shown below:

Note: *The last line of the FileGuard menu always displays the name of the current User.*

Logging In

You need to log in when you switch your Macintosh on. You also need to log in whenever the screen saver is active.

If the screen saver is active move the mouse or press a key. The Login dialog is displayed requesting the User name and password:

1. Select your User name from the User pop-up menu in the login dialog or type it in.

2. Enter your User password.

3. Click on **OK.**

Your Macintosh is now ready for use.

Logging Off

Logging off ends the current session on your Macintosh. If you share your Macintosh with other Users, you must log off after each session to prevent other Users from accessing any protected items to which they should not have access.

For example, if you begin a session, work for a while and then decide to take a break without logging off, anyone can sit down at your Macintosh while you are away and access items to which they should not have access. As far as your machine is concerned it is still you at the keyboard. Logging off between sessions is therefore essential to keep the Macintosh secure. To end your current session use one of the following options:

- Choose Log Off… from the FileGuard menu.
- Use the Log Off keyboard shortcut if configured.
- Use the Log Off screen corner.

The FileGuard screen saver is now displayed. The Macintosh remains like this until the mouse is moved or the keyboard is used.

Warning: *When you open an encrypted document, it is not re-encrypted until you quit the application that created the document. If you are working on a protected document, it is important that you close the corresponding application before logging off. If you fail to do so, the document you were working on will remain decrypted for the next User, even if you closed the document itself before logging off.*

Note: *FileGuard can be configured to automatically log off after a fixed period of inactivity. Refer to* *"Security Screen" on page 36* *for further information.*

Locking the Screen

Locking the screen prevents anyone from using your Macintosh in your absence. Once you have locked the screen you are the only User who can log back in. Typically you lock the screen if you want to take a break in your session and return later.

Important: *Locking the screen may be frustrating for other legitimate Users. If they must use the machine while the screen is locked, they will have to restart, which means the current User will lose any unsaved information. Therefore screen locking should be used with care.*

To lock your Macintosh's screen:

• Choose Lock… from the FileGuard menu.

• Use the Lock… keyboard shortcut if configured.

The FileGuard screen saver now appears. The Macintosh remains like this until the mouse is moved or the keyboard is used.

Once the mouse is moved or the keyboard is used, a dialog is displayed asking for your user password:

To unlock your Macintosh, enter your user password and click on OK. The User field is grayed out because you cannot select another User.

The Macintosh is now ready for use.

Changing a User Password

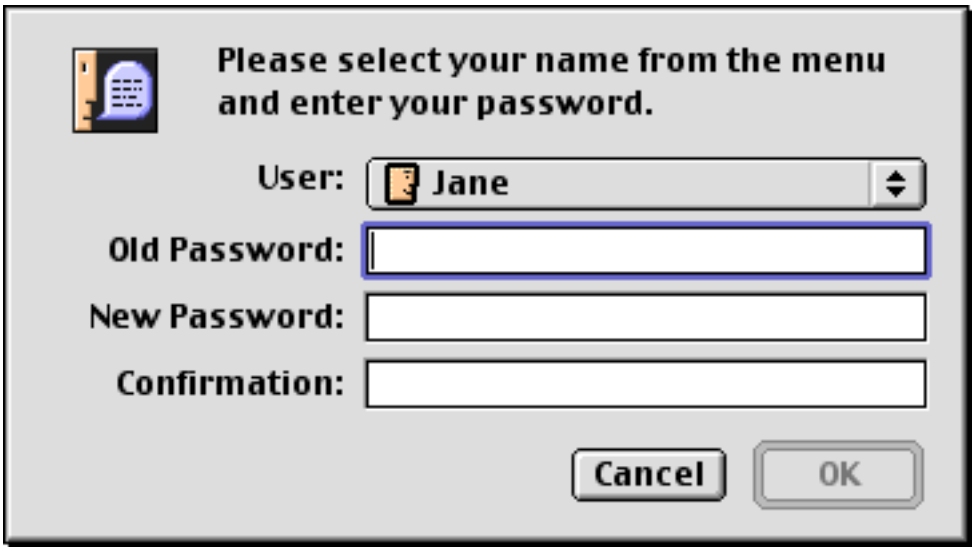
Users can change their user password using the Login dialog box if you give them the permission to do so. The Login dialog box is displayed when you start up or begin a new session. Refer to “Logging In” on page 80 for more information.

To change a user password:

1. Choose Log Off… from the FileGuard menu.

2. Move the mouse or hit any key. The Login dialog box is displayed.

3. Click the **Password** button. The Change User Password dialog box is displayed:



4. Select the user’s name from the User pop-up menu, if enabled, otherwise type the name.

5. Click the Old password field and enter the old user password.

6. Click the New password field and enter the new user password.

7. Click the Confirmation field and re-enter the new user password.

8. Click on **OK.** You are returned to the Login dialog.

9. Enter the new user password to access the Macintosh and click on **OK.**

Protecting Items

To protect an item from within the Finder, select the item and choose Protect… from the FileGuard menu.

Refer to “Protecting Volumes” on page 40, “Protecting Folders (System 7.x)” on page 47, “Protecting Applications” on page 56 and “Protecting Documents” on page 60 for further information.

Protecting Documents when Created

If the **Ask to encrypt new documents** option on the User Configuration dialog is enabled FileGuard asks if you wish to encrypt the contents of new documents when they are saved for the first time:

Click on No to save the document without encryption. Click on Yes to encrypt the document.

Opening an Encrypted Document

Opening an encrypted document is the same as opening a normal document, except that you have to enter the password to decrypt it.

Important: *The document is automatically re-encrypted only when you quit the application. Closing a document does not re-encrypt it.*

Viewing the Log

To view the log, choose View Log… from the FileGuard menu. The Log window is displayed. Refer to “Viewing the Log” on page 69 for further information.

Configure

This menu item allows the Administrator or a Super User to configure FileGuard:

• Choose Configure… from the FileGuard menu.

A dialog box appears asking for an Administrator or Super User name and user password:

• Enter the requested information and click on OK.

Refer to “Chapter Two - Configuring FileGuard” on page 17 for more information on how to configure FileGuard.

Note: *The first time you launch FileGuard no password is requested because the Administrator is set to the Guest. Once you have set the Administrator to another User you must enter the appropriate password whenever you launch FileGuard to configure it.*

INDEX

V