
User's Guide

Data Secure!

Single Workstation Version

From Boca

The logo for BOCA is rendered in a bold, blue, italicized, sans-serif typeface. The letters are thick and have a slight slant to the right, giving it a dynamic and modern appearance.

This software is protected by both United States Copyright Law and International Treaty provisions. Boca Research, Inc. grants you this license and your continued use confirms your agreement. Therefore, you must treat the software “just like a book,” with the following single exception: Boca Research, Inc. authorizes you to make archival copies of the software for the sole purpose of backing up your software and protecting your investment from loss.

By saying just like a book, Boca Research, Inc. means, for example, that the software may be used by any number of people and may be freely moved from one computer to another, so long as there is no possibility of being used at one location while it’s being used in another. This is just like a book that cannot be read by two different people in two different places at the same time; neither can this software be used by two different people in two different places at the same time.

This agreement shall be construed, interpreted, and governed by the laws of the state of Florida and shall inure to the benefit of Boca Research, Inc. its successors, administrators, heirs, and assigns.

LIMITED WARRANTY

Limited warranty on product media. To the original buyer only, Boca Research, Inc. warrants the media on which this product is recorded to be free of defects in material and workmanship under normal use for a period of 90 days from the purchase date. Any implied warranties of merchantability or fitness for a particular purpose are limited in duration to the period of 90 days for the date of purchase. Your sole and exclusive remedy in the event of a defect in material or workmanship under normal use is expressly limited to replacement of the defective item.

This warranty gives you specific legal rights, and you might also have other rights that vary from state to state.

No warranty on product software or User Guide. Even though Boca Research, Inc. has tested the software and User Guide and reviewed their contents, Boca Research, Inc. and its distributors and dealers make no warranties, either expressed or implied, with respect to the fitness for a particular purpose. the software and User Guide are distributed solely on an as is basis. The entire risk as to their quality and performance is with you. Should either the software or User Guide or both prove defective, you (and not Boca Research, Inc. and its distributors and dealers) assume the entire cost of all necessary servicing, repair, or correction. Boca Research, Inc. and its distributors and dealers will not be liable for direct, indirect, incidental, or consequential damages resulting from any defects in the software or User Guide, even if they have been advised of the possibility of such damages.

Some states do not allow limitations on how long an implied warranty lasts or the exclusion or limitation of incidental or consequential damages, so the above limitations or exclusions might not apply to you.

COPYRIGHT

The manual and the software described in it are copyrighted with all rights reserved. The manual or software may not be copied in whole or part, without written consent of Boca Research, Inc. You may not sell, rent, lease nor transfer copies of the manual or software in any other way without the prior written consent of Boca Research, Inc.

TRADEMARKS

Boca Research, Inc. and Boca MegaMedia CD are trademarks of Boca Research, Inc.

IBM is trademark of International Business Machines Corp.

Microsoft is a trademark of Microsoft Corp.

All other trademarks are acknowledged

In Case of Defective Media:

If the media should fail within 90 days of purchase, please return the original with proof of purchase for a FREE replacement. After 90 days from date of purchase, include \$9.50 for replacement. You can obtain replacement media by returning the defective copy, with your proof of purchase to Boca Research, Inc., Attention: Customer Service, 1377 Clint Moore Road, Boca Raton, Florida 33487-2722

Table of Contents

Chapter 1	Getting Started	1
Welcome		1
Why You Need the <i>Data Secure!</i> Package		1
Introducing <i>Data Secure!</i>		2
<i>Data Secure!</i>		2
<i>E-Mail Lock</i>		3
<i>Internet Defender & Virus Protection</i>		4
About This User's Guide		5
Getting Started		5
Using <i>Data Secure!</i>		5
Practical Applications		5
Troubleshooting		5
Customer Support		6
Chapter 2	Installation	7
Overview		7
System Requirements		7
Installation Procedure		8
Program Installation		8
Initial Configuration		9
Defining the System Administrator		10
Uninstalling <i>Data Secure!</i>		13
Chapter 3	Using the Login Window	15
Overview		15
The Login Window		15
Login and Logoff		16
Always On Top		16
Key Types		17
Working With Passwords		17
Changing Your Password		18
Using a Key Diskette		18
Locking the Keyboard and Mouse		19
Using the Warning Panel		19
Configuring the Warning Panel		20

Chapter 4	Introducing Data Secure! Configuration	21
Overview.....		21
User Interface.....		22
Toolbar.....		23
Menus		24
Definition Areas		25
Folder Tree		25
Data Secure! Screens.....		27
The Users Screen.....		27
The Folder Group Screen.....		28
The Access Rights Screen.....		28
The Audit Screen.....		29
The Internet Defender & Virus Protection Screen.....		30
Encryption Control Screen.....		31
Password Control Screen.....		32
Confirmation Screen.....		32
Chapter 5	Using Data Secure! Configuration	33
Overview.....		33
To open <i>Data Secure!</i> Configuration:.....		33
Overview of the User Definition Process.....		34
Creating and Modifying Users		35
Creating a New User		35
Modifying a User Definition.....		36
Changing a Users Name.....		37
Erasing a User.....		37
Working With User Definitions		38
Setting System Level Options.....		38
Assigning a Security Key Type.....		39
Assigning Folders to Authorized Users		41
Copying Definitions		41
Defining Access Rights.....		43
Selecting the Encryption Method.....		45
Selecting the Initial Password.....		46
Confirmation and Encryption.....		48
Working with Folder Groups.....		49
Working with Access Rights Groups		51
Chapter 6	<i>Data Secure!</i> Advanced Features	53
Overview.....		53
Data Secure! Guards.....		53
Introduction		53
DOS Guard		54
Configuring the <i>Data Secure!</i> Guards.....		54
Boot Lock		55
Using Boot Lock.....		55

Using the Recovery Diskette.....	56
Removable Media Protection	57
Tips and Examples	57
Replacing or Re-Creating Master Key Diskettes.....	58
Encrypted Backup and Restore	58
Overview	58
<i>Data Secure!</i> Default Options	60
Overview	60
Boot Drive	60
Master Drive.....	60
Default Encryption Protocol	60
Default Access Rights	61
Uninstalling <i>Data Secure!</i>	62

Chapter 7 Using E-Mail Lock 63

Overview.....	63
Why You Need <i>E-Mail Lock</i>	63
How <i>E-Mail Lock</i> Works	63
Limitations and Cautions	64
Encrypting Documents	64
Decrypting Documents.....	66
Decrypting Messages with Microsoft Internet Explorer™	67
Working With Recipients.....	67
Adding a Recipient.....	67
Modifying and Deleting a Recipient.....	69
The Decryption Module.....	69

Chapter 8 Using Internet Defender & Virus Protection 71

Overview.....	71
Why You Need <i>Internet Defender & Virus Protection</i>	72
How Internet Defender & Virus Protection Works	72
Internet Safe Use	74
To designate folders for Internet Safe Use:	75
Tips and Suggestions.....	75
DOS Safe Areas.....	76
Tips and Suggestions.....	76
Window Safe Areas	77
Defining Windows Safe Areas.....	77
Tips and Suggestions.....	78
Safe Setup	78
Hide While On-Line	79
Tips and Suggestions.....	80

Glossary of Terms 81

Glossary of Terms

Access Rights Parameters

Access Rights refers to the ability of a user to perform various actions on a file. Examples of access rights parameters include View, Read, Read, Delete and Rename.

Areas

Areas is another term for Folder Groups. Folder Groups are pre-defined sets of protected folders that may be assigned to authorized users.

Authorized User

An authorized user is one who has been granted access to protected areas by the System Administrator.

Definition Area

The definition area is the section in a Data Secure! Configuration window where User, Folder Group and Access Rights Group definitions appear. Double click on a definition to modify or delete a definition.

Folder Group

Folder Groups are pre-defined sets of protected folders that may be assigned to authorized users.

Key Diskette

A key diskette is a specially encoded diskette which is used to grant access to protected areas by an authorized user.

Master Drive

The drive into which the Master Key Diskette is inserted.

Master Key Diskette

A Master Key Diskette is required to allow the System Administrator to access the *DataSafe* Configuration program.

Protected folder

Protected folders may only be viewed or accessed by authorized users. A protected folder may or may not be encrypted.

Recipient

A recipient is the intended reader of an E-mail message. A recipient definition includes an encrypted password unique to the recipient.

System Administrator

The person responsible for setting security parameters and defining users and protected areas. Only the System Administrator is authorized to use the *DataSafe* Configuration program.

Chapter 1 Getting Started

Welcome

Welcome to *Data Secure!*, the revolutionary new PC security and privacy suite for Windows 95™. This User's Guide explains installation procedures for *Data Secure!* and how to use it effectively on your PC system.

Data Secure! is an integrated suite of powerful utilities designed to protect your privacy by preventing unauthorized access to your data files, messages, system areas, E-mail communication and Internet use.

This version of *Data Secure!* is designed for use on a single computer or a local workstation only. The security and privacy features will not work properly on remote network drives. *Data Secure!* protected and encrypted folders, however, are **fully protected** from access over a network.

Why You Need the *Data Secure!* Package

Your documents, messages and data are your personal property. They are nobody's business but yours. You wouldn't leave your income tax return or love letters laying around for everybody to see. You wouldn't give your competitors or the government access to your file cabinets. Your computer data is no different.

Today's rapidly changing computing environment has created a multitude of ways for outsiders to gain access to your computer without your knowledge or consent. Intruders can access your computer and read or copy confidential data. Prying eyes can read your E-mail messages. Hackers can infect your system with a virus, steal your data, or even erase your hard disk while you are happily surfing the Internet. Your children could accidentally erase that report you have been working on for a month. Your computer could be stolen.

Data Secure! guards your privacy and protects your data and your computer from unauthorized access and tampering.

Introducing *Data Secure!*

The *Data Secure!* suite consists of three integrated security and privacy programs.

- ***Data Secure!*** - Protects your PC and Data from unauthorized access and tampering.
- ***Internet Defender & Virus Protection*** - Firewall and Virus Protection.
- ***E-Mail Lock*** - “On-the-fly” E-mail and Document Encryption.

These applets provide you with a complete set of security and privacy tools accessed via a simple, user-friendly interface.

Data Secure!

Data Secure! protects your data and your system configuration files from unauthorized access and tampering. The System Administrator designates certain folders as protected and/or encrypted. The System Administrator defines which users are authorized to access individual protected folders and what types of actions may be performed on folder contents.

Authorized users log on using a password and/or a key diskette. They can only access protected folders according to the access rights granted by the System Administrator.

The System Administrator defines all security and access control parameters from a single easy to use screen.

Data Secure! features include:

- **Real Time data encryption and decryption**

Data Secure! automatically encrypts and decrypts protected data in the background, without user intervention and with no noticeable performance degradation.

Files in protected folders are invisible and inaccessible to unauthorized users, even in a DOS window or over a network.

- **Complete access control**

The System Administrator may customize access rights to folders by authorized users. Operations, such as file deletion, modification or program execution may be denied to certain users, while allowing other types of access.

- **Multiple encryption protocol support**

Data Secure! supports several encryption protocols. Data may also be protected without encryption.

- **Multiple user support**

Multiple users may be defined, each with different access privileges.

- **Encrypted Backup and Restore**

Data may be backed up and restored in encrypted form, thereby preventing unauthorized access to backup data.

- **Removable media protection**

Data Secure! can restrict access to floppy disks and other types of removable media such as CD ROM drives and ZIP[®] drives. This feature prevents the spread of viruses from infected media and unauthorized copying of confidential data.

- **Full audit trail**

Data Secure! provides a system log which records all attempts to login and logoff of the system, both successful and unsuccessful. The log also records the designation of folders as protected areas and any changes made to that designation.

- **Data Secure! Guards**

Data Secure! Guards protect your system from such dangers as:

- Booting in the MS-DOS mode
- Use of the Windows 95[™] Startup Option keys

E-Mail Lock

E-Mail Lock allows you to quickly and easily encrypt your E-mail messages and other documents “on the fly”. Your recipient can also decrypt them just as easily.

E-Mail Lock features include:

- **Ease of Use**

A simple mouse click or “hot key” command instructs *E-Mail Lock* to encrypt an E-mail message or other document. The recipient uses the hot key command to decrypt it.

- **Optional Manual Passwords**

With *E-Mail Lock*, the use of manual passwords is optional.

- **RTF Document Support**

E-Mail Lock can be used to encrypt and decrypt RTF formatted documents. The decrypted copy will retain all document formatting.

Internet Defender & Virus Protection

Internet Defender & Virus Protection protects your system from unauthorized access while you are using the Internet or other on-line services. Internet Defender & Virus Protection also protects you against damage caused by viruses, Trojan Horses, and hostile Java applets. These unwelcome guests from the information superhighway could severely damage your programs and data or even erase your hard disk. Internet Defender & Virus Protection even guards your privacy during on-line registration or on-line purchasing.

Internet Defender & Virus Protection features include:

- **Firewall Protection**

Internet Defender & Virus Protection prevents access to all but specifically designated firewall areas while on-line and while working with downloaded files afterwards.

Internet Defender & Virus Protection protects your system from unauthorized access when it is being used as an FTP server.

- **Virus Protection**

Internet Defender & Virus Protection ensures that a virus cannot infect or damage any files located outside of firewall area folders .

- **Hide While On-Line**

Areas not otherwise protected by *Data Secure!* can be hidden from view while performing on-line tasks such as: software registration, ordering or purchasing, interactive chats, on-line games, etc.

About This User's Guide

The User's Guide is an essential component of the *Data Secure!* suite. We strongly suggest that you read it to familiarize yourself with the various procedures before attempting to use the software.

It is assumed that the user has a basic familiarity with the Windows 95™ environment. Familiarity with computer security concepts is **not** required in order to use *Data Secure!*.

The manual is divided into three major sections as follows:

Getting Started

Chapters 1 through 4 deal with introductory material, installation and the user interface. These chapters are intended to help you get started using *Data Secure!* and should be read by all users prior to use.

Chapter 1 is a general introduction to the *Data Secure!* package. Chapter 2 covers the installation procedures. Chapter 3 describes the login procedures and the Login utility. Chapter 4 covers the user interface of the *Data Secure!* Configuration program.

Using Data Secure!

The following three chapters cover the three main components of the *Data Secure!* package in detail. These chapters are intended to serve both as a tutorial and a reference.

Each feature is introduced by a brief overview followed by step-by-step instructions. Screen shots and illustrations are liberally used. Examples and tips are also provided at appropriate points.

Chapters 5 and 6 cover the basic and advanced features of *Data Secure!*. Chapter 7 describes the *E-Mail Lock* feature.

Practical Applications

This chapter presents suggestions and tips on how to use *Data Secure!* in common applications. The discussion includes detailed instructions on how to configure *Data Secure!* to achieve the desired results. This chapter is intended to serve both as a tutorial and as a practical guide.

Troubleshooting

This final chapter covers troubleshooting and problem solving techniques. The troubleshooting section is organized on a functional basis and provides solutions and tips for the most common problems.

A glossary and an index complete the documentation package.

Customer Support

Satisfaction Guaranteed! Data Secure! Is backed by a full 90 day money-back guarantee. Boca's Customer Support department is at your service to help you resolve any problems with Data Secure!

Phone: 561-241-8088

Fax: 561-997-2163

Web site: <http://www.bocaresearch.com>

E-mail: support@bocaresearch.com

Compuserve: GO BOCA

BBS: 561-241-1601

Chapter 2 Installation

Overview

The installation process consists of three separate sections:

- Program installation
- Initial configuration
- Defining the System Administrator

The *Data Secure!* CD ROM includes a setup utility that will install the software and its components. It is essential that all steps in the installation and configuration process must be successfully completed before you can safely use *Data Secure!*.

Before you begin the installation process, please fill out and return the registration card. Keep the registration number for your reference. You will need it to obtain upgrades and technical support.

System Requirements

To use *Data Secure!*, the following is required:

- 486SX/33 or higher PC
- Minimum of 8 MB RAM (12 MB recommended)
- At least 5 MB free disk space
- Microsoft Windows 95™
- 3.5" diskette Drive
- 2X speed or greater CD ROM drive

*A Master Key Diskette is required to allow the System Administrator to access the **Data Secure!** Configuration program.*

Before you begin the installation program, prepare at least two freshly formatted diskettes for use as **Master Key Diskettes**. We recommend that you manually format these diskettes, as the manufacturer's format is occasionally unreliable.

You may only install **Data Secure!** on a single computer or a local workstation. Do not attempt to install **Data Secure!** on a network server.

Installation Procedure

Program Installation

Perform the following steps in order:

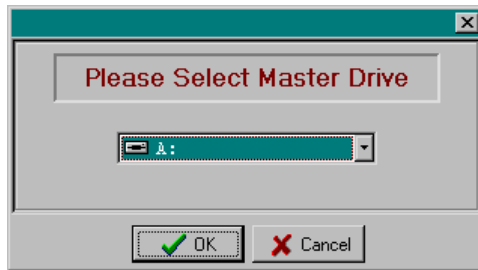
1. Close all other applications that are running.
2. Insert the CD ROM into the drive.
3. Run the Setup program using the Explorer or the **RUN** option on the Start Menu.
4. Follow the instructions on the screen.
5. At the conclusion of the process, a dialog will appear requesting that you restart your computer in order to complete the installation process.
Click on **OK** continue and your computer will restart.
6. Remove the CD ROM.

Once your computer restarts, proceed to the **Initial Configuration** section.

Initial Configuration

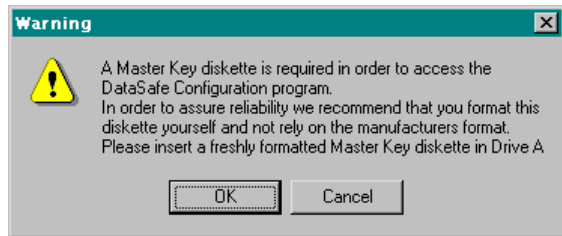
During the second part of the installation process you will create the Master Key Diskettes and set initial parameters. Perform the following steps in order.

1. Upon restarting the computer, the following dialog box appears.

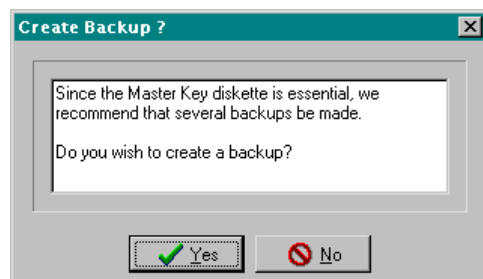


The Master Drive is the drive into which the Master Key Diskette is inserted.

2. Select the drive to be designated as the Master Drive from the pull down list. Click on **OK** to continue. The program encodes the Master Key Diskette.
3. Insert a diskette in the Master Drive when the following warning box appears.



Click on **OK** to continue. The Create Backup dialog box appears.




4. We recommend that at least one backup diskette be made. Click on **Yes** to make a backup Master Diskette.
5. Repeat steps 4 and 5 until a sufficient number of backups are created. Click on **No** to continue.
6. The *Data Secure!* welcome screen appears. You are now ready to define the System Administrator. Click on **OK** to continue.

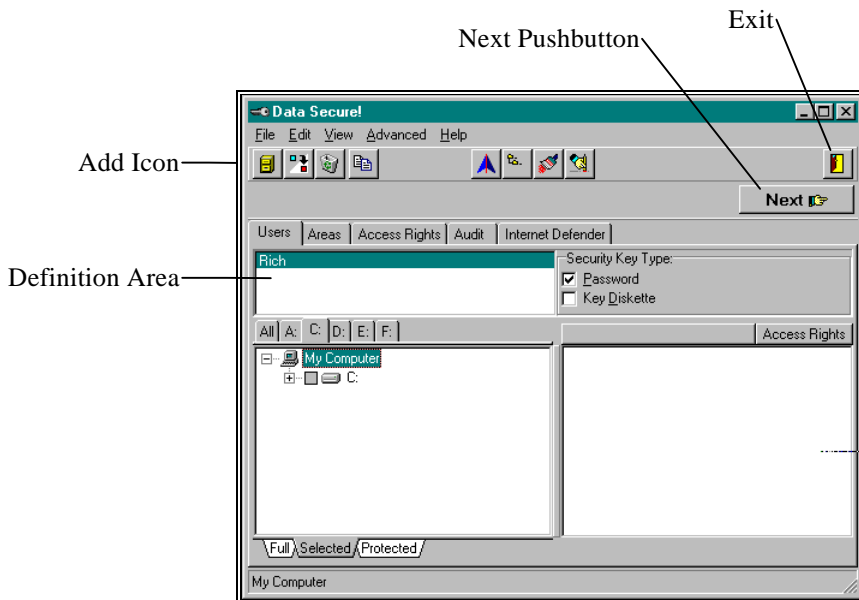
Defining the System Administrator


The System Administrator is the person responsible for setting security parameters, defining users and protected folders.

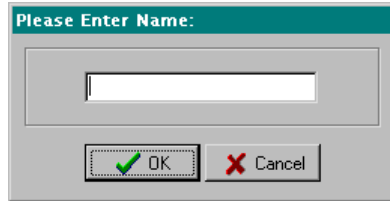
The final step of the setup process is to define your first user, which should be the **System Administrator**. At least one user must be defined in order to protect folders and use the security and privacy features of *Data Secure! Application*.

The following steps are intended to allow you to quickly define the System Administrator using *Data Secure!* Configuration without protecting any folders. Please follow the instructions exactly as written. For a detailed discussion of the definition process please refer to **Chapter 5**.

1. The *Data Secure!* Configuration main window should appear automatically. If it does not, right click on the red lock icon  located on the right-hand side of the taskbar. Select **Run Data Secure!** from the short-cut menu.
2. The *Data Secure!* welcome screen appears. You are now ready to define the System Administrator. Click on **OK** to continue.
3. The *Data Secure!* Configuration window appears:

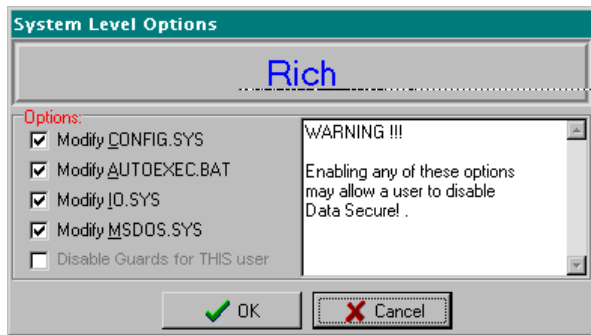


- Click on the **Add**  icon on the toolbar. The Enter Name dialog box appears.



Type "**System Administrator**" in the space provided. You may substitute a different name if you wish. Click on **OK** to continue. The new name will appear in the Definition area.

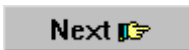
- The System Level Options dialog box appears.




Click to place a check mark in the box next to all of the options. This dialog box must appear exactly as above. Click on **OK** to continue.

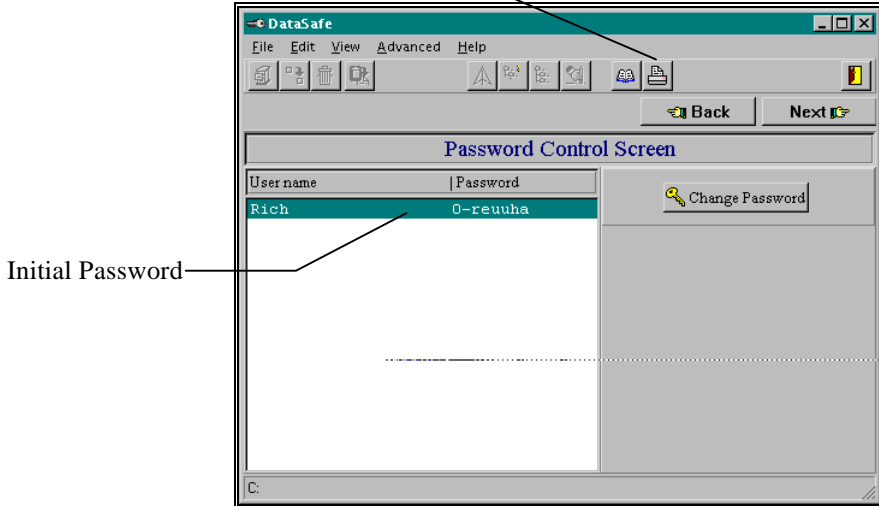
At this point it is possible to select files to be protected and to perform other definition actions. We recommend that you **do not** do so at this time.

- Click on the **Password** check box in the Security Key Type section.
- Click on the **Next** pushbutton. The Encryption Control screen appears. Click on the **Next** pushbutton again. The Password Control screen appears.



- Click on the **Print** icon  on the toolbar. A report showing the initial password assigned to the System Administrator will print.

Print Icon



Initial Password


The initial password is also displayed on the screen. The System Administrator will need this password in order to login to *Data Secure!*.



- Click on the **Next** pushbutton to continue. The Confirmation screen appears.



- Click on the **Finish** pushbutton to complete the definition process.

- Click on the **Exit**  pushbutton to exit *Data Secure!* Configuration.

This completes the installation process. *Data Secure!* is now ready to protect your computer. At this point you may continue to use *Data Secure!* Configuration to define additional users.

Uninstalling *Data Secure!*

In order to uninstall *Data Secure!* all of the installation and initial configuration steps, as described in the preceding sections, must have been successfully completed.

To uninstall *Data Secure!*:

1. Run *Data Secure!* Configuration.
2. Erase all users.
3. When all users have been deleted, click on the **Next** pushbutton until the Confirmation screen appears.
4. Click on the **Finish** pushbutton. *Data Secure!* will decrypt all encrypted folders and unprotect all protected areas.
5. Select **Uninstall Data Secure!** from the Advanced Menu or use the **Add/Remove Programs** feature on the Windows 95™ Control Panel.
6. When the Uninstall window appears, click on **OK**.
7. When the Erasing *Data Secure!* Files window appears, click on **OK**. Click on **OK** on the confirmation box.
8. Restart your computer.

Chapter 3 Using the Login Window


Overview

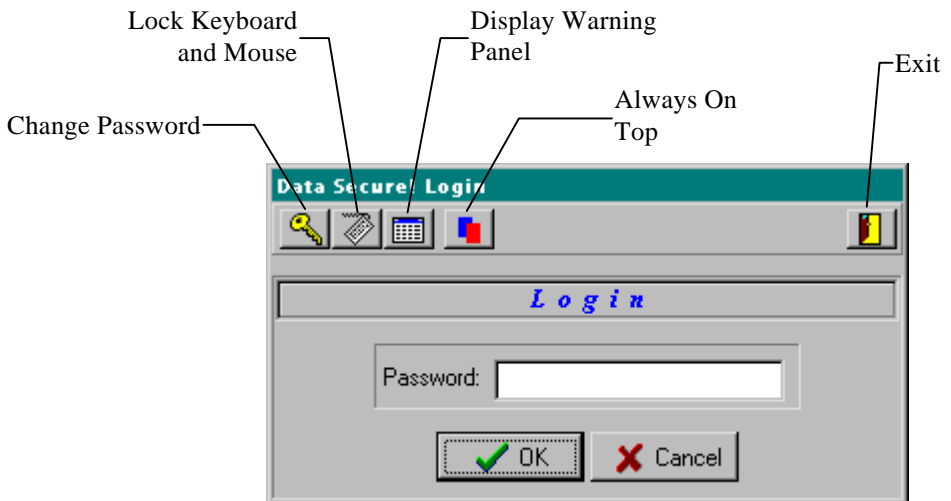
A user gains access to *Data Secure!* protected areas by “logging in” with a “key”, which may be a password and/or a key diskette. This is accomplished via the **Login** window.

The Login window also allows the user to perform additional tasks, such as changing the password, locking the keyboard and configuring the warning panel.

The Login Window

The Login window appears automatically when Windows 95™ starts up. The user may open the Login window at any time.

To open the Login Window, double click on the lock icon  located on the right-hand side of the taskbar. Login may also be opened via the Start Menu.




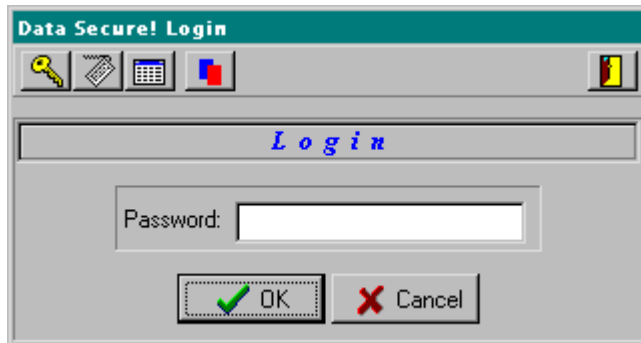
The Login Window

Login and Logoff

Users login and logoff the computer using the **Login Window**. A password and/or a key diskette is required for authentication.


To login to *Data Secure!*:

1. If a **Key Diskette** is required for access, insert it in the appropriate drive.
2. Double click on the lock icon  located on the right-hand side of the taskbar to open the Login window or select *Data Secure!* from the Start Menu. The Login panel appears in the window.



3. If a **Password** is required, type your password in the space provided. Type your password exactly as it was defined including the number and the dash.
4. If a **Password is not** required, do not type anything at all in the Login window. *Data Secure!* will not recognize the password and an error message will appear.
5. Click on **OK** to confirm and close the window. The Login window will close.


To Logoff of *Data Secure!* :

1. Double click on the lock icon  located on the right-hand side of the taskbar to open the Logoff window.
2. Click on **OK** to confirm and close the window.

Always On Top

The Login window may be configured to appear on top of all open windows.

To enable **Always On Top**, open the Login window and click on the

Always On Top  icon. This icon is a toggle and will appear depressed when active. To disable, simply click again.

Key Types

The System Administrator may require an authorized user to use a **Password**, a **Key Diskette** or both together in order to access protected folders. A password is the default Security Key.

Working With Passwords

Data Secure! passwords consist of two parts. The first part is a number followed by a dash (-). The number is assigned by *Data Secure!* and cannot be changed.

The second part is the password text itself, which may be changed by the user. Both parts of the password must be typed correctly in order to gain access.

An example of a valid password is: 0-wtssbotnoht.

Passwords may contain up to 20 characters including the number and dash. Any letter, number, or symbol available on a standard keyboard may be used in a password.

A good password can be remembered easily by the user but is difficult for an impostor to guess or to crack. Words and numbers to avoid include:

- Names of family, friends, pets or celebrities
- Personal information such as addresses, phone numbers, birthdays, Social Security numbers, etc.
- Complete words or phrases

Some suggestions for a safe password include:

- Use a mixture of letters (upper and lower case), numbers and symbols.
- Make your password at least six characters long.
- Join two unrelated words with a symbol such as: **BIrd!learN.**

Do not attempt to copy or backup a user's Key Diskette. Unlike the Master Key Diskette, it cannot be backed up. The copy will not work and the original may become damaged.

Changing Your Password

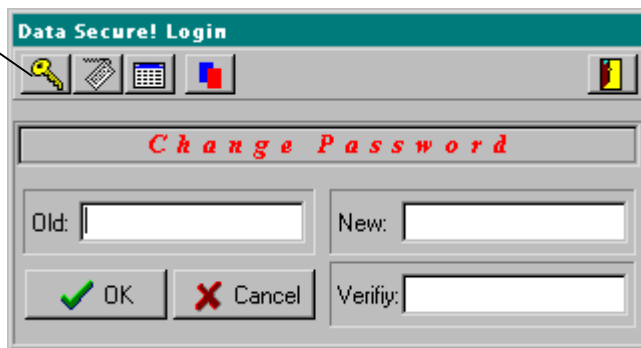
A user may change her password at any time. A user's password may only be changed by the user him/herself (or someone who knows the password!). The System Administrator cannot change a user's password once the definition process is complete.

We recommend that a user change his password on a regular basis.

To change your password:

1. Double click on the lock icon  located on the right-hand side of the taskbar to open the Login window.
2. Click on the **Change Password** icon . The window displays the Change Password panel.

Change Password



3. Enter your current password in the **Old** field.
4. Type your new password in the **New** field.
5. Type the new password again in the **Verify** field. If the **New** and **Verify** entries do not agree, an error message will appear. Repeat steps 3 and 4 as necessary.
6. Click on **OK** to confirm and close the window.

Using a Key Diskette

When the System Administrator designates a Key Diskette as the security key type for a new or existing user, it is necessary to login using the initial password and to physically create the Key Diskette.

If your key diskette is lost or damaged, contact the System Administrator to receive a new one.

Do not attempt to copy or back up a user's Key Diskette. Unlike the Master Key Diskette, it cannot be backed up. The copy will not work and the original may be damaged during the process.


Locking the Keyboard and Mouse

Data Secure! allows a user to temporarily lock the keyboard and mouse. This prevents unauthorized use of the computer while the user is away from his/her desk.

The keyboard and mouse can only be unlocked by the same authorized user who locked them in the first place.

Programs running in the background are not affected by locking the keyboard and mouse.

To lock the keyboard and mouse:

- Open the Login window and click on the Lock Keyboard  icon. Mouse movement is restricted to within the Login window. Keyboard activity is restricted to the password field.

To unlock the keyboard and mouse

- Enter your password and/or insert the key diskette in the drive as required.


Using the Warning Panel

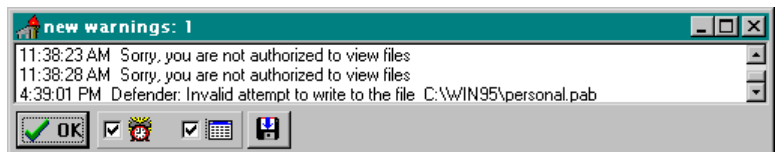
The Warning Panel is a pop-up window that displays warnings and messages generated by *Data Secure!*. These messages indicate breaches of security guidelines, such as an unauthorized attempt to access protected folders or an attempt by an Internet application to write outside of the firewall area.

The Warning Panel displays the last 20 messages generated during the current session.

By default, the Warning Panel appears automatically whenever a warning message appears.

To display the Warning Panel


- Open the Login Window and click on the Warning Panel  icon. Use the scroll bars to browse through a long list.




- **To close the Warning Panel**, click on **OK**.

Configuring the Warning Panel

The controls on the bottom of the window control the behavior of the Warning Panel.

To sound an audible tone when a warning message is received , select the check box next to the bell icon .

To enable automatic display of the Warning Panel upon receipt of a warning message, select the check box next to the window icon .

To save the current Warning Panel settings , click the disk  icon.

Chapter 4 Introducing Data Secure! Configuration


Overview

This chapter describes the user interface and functionality of the *Data Secure!* Configuration program. These descriptions do not include detailed operating procedures. The operating procedures are discussed in the following chapters as well as in the context sensitive help.

Data Secure! Configuration is your security and privacy control center. The System Administrator uses *Data Secure!* Configuration to define protected folders, to define users authorized to access them and to set parameters for various other features, including the *Internet Defender & Virus Protection* and *E-mail Lock* utilities.

The System Administrator must use the Master Key diskette to run *Data Secure!* Configuration.

To open *Data Secure!* Configuration:

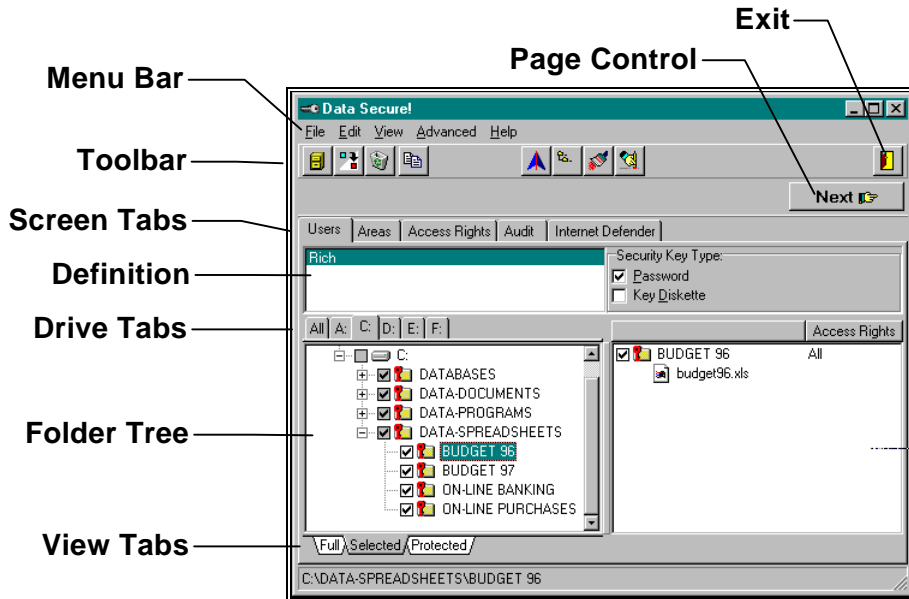
1. Insert the Master Key Diskette.
2. **Right** click on the  lock icon located on the right-hand side of the taskbar. You may also run *Data Secure!* Configuration via the Start Menu.
3. A shortcut menu appears.



4. Select **Run Data Secure!**. The Welcome screen appears. Click on **OK** to continue.

User Interface

This section describes the user interface features of *Data Secure!* Configuration. The System Administrator interacts with the program using the Configuration window shown below.



Data Secure! Configuration Main Window

All operations are performed in a series of easily accessible screens within the Configuration window. Use the **Screen Selection Tab**, located under the toolbar to access the various screens.

During the process of defining authorized users and protected folders, the System Administrator is required to work with three additional screens which are accessed using the **Page Controls** located in the upper right-hand corner of the window.

Use the menus and icons located on the toolbar to access the various features and commands.

Toolbar

The toolbar provides quick access to several functions. The functions of the various icons are discussed below.

Please note that icons appear on the toolbar only when that particular function is available. Icons which are not available may appear grayed out or may not appear at all.



Configuration Window Toolbar



Add Definition Click to add a definition of a User, Folder Group or Access Rights Group.



Rename Definition Click to rename a definition of a User, Folder Group or Access Rights Group.



Delete Definition Click to delete a definition of a User, Folder Group or Access Rights Group.



Copy Selection Click to copy a definition from one User or Folder Group to another.



Save Click to save Folder Group and Access Rights Group definitions. A definition must be saved in order for it to be available in future sessions.



Maximize/Minimize Folder Tree Click to expand the visible folder tree by hiding the Definition area on the User and Folder Group screens.



Collapse Folders View Click to collapse the folder tree to its lowest level.



Refresh Folder View Click to update the Folder Tree to account for changes made to folders since the Configuration window was opened.



Clear Selections Click to deselect all folders in the currently displayed folder tree.



Print Preview Click to view the User Password report on the screen. This icon is available on the Password Control screen.



Print Click to print the User Password report. This icon is available on the Password Control screen.



Exit Click to exit *Data Secure!* Configuration.

Menus

Data Secure! Configuration menus contain all of the available functions and commands, including those that are not available on the toolbar. The following table describes the available menus:

File	Contains Add , Save , Rename and Delete options for the various definition types (User, Area and Access Rights). Also included are the Print Preview and Print functions for the password report as well as the Exit option.
Edit	Contains the Copy Selection command and the Clear Selection command.
View	Contains options for viewing the Tree window.
Advanced	Contains the following advanced functions: <ul style="list-style-type: none">• Default Options - Modifies the <i>Data Secure!</i> system defaults.• Guards Options - Global settings that prevent access to the DOS mode.• User Access - Controls the ability of individual users to modify certain system configuration files and to start the system in the DOS mode.• E-Mail Passwords - Define global recipients for <i>E-mail Lock</i>.• Boot Lock - Enables the Boot Lock feature, which requires password entry at boot time.• Create Master Key Diskette - Re-creates the Master Key Diskettes.• Encrypted Backup/Restore Mode - Activates the encrypted backup and restore feature.• Uninstall Data Secure! - Uninstalls <i>Data Secure!</i>.
Help	Accesses the on line help system.

Definition Areas

Definition areas display definitions created by the System Administrator using *Data Secure!* Configuration. The following definitions are available:

- **Users** are individuals authorized to access protected folders.
- **Folder Groups** are pre-defined groups of protected folders which can be assigned to users.
- **Access Rights** are pre-defined groups of access rights parameters that can be associated with folders assigned to a specific user.

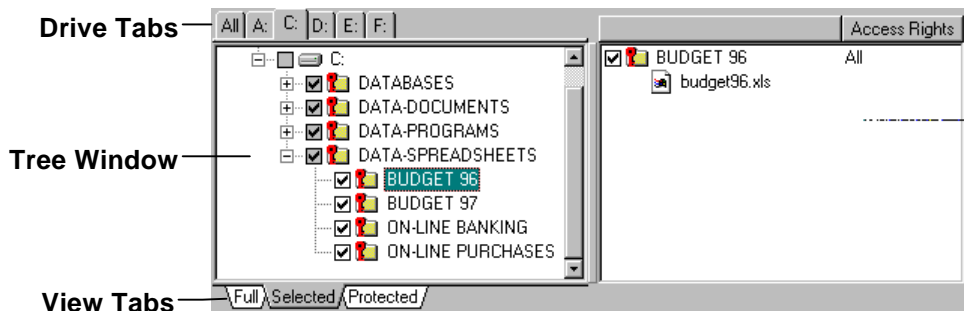
Use the Definition area on the user and access rights screen to select a definition to work with.

To add, erase or rename a definition, perform one of the following actions:

- Click on the appropriate icon on the toolbar.
- Right click in the Definition Area and select the desired option from the short-cut menu.
- Select the desired option from the **File** menu.


Folder Tree


The **Folder Tree** displays the folder hierarchy and looks and works very much like the Windows 95™ Explorer tree. Use the Folder Tree to select folders for various operations such as assigning folders to users.



The Folder Tree contains the following components:

- **Tree Window** - Use the Tree window to display and select folders and sub-folders.
- **Access Rights Window** - Use the Access Rights window to modify the access rights parameters for selected folders. To display folder contents in the Access Rights window, click on the folder or on its name in the Tree window.
- **Drive Tabs** - Click to display only folders on the indicated drive or folders on **All** drives in the Tree window.
- **View Tabs** - Click to display folders in the Tree window as follows:
 - Full** - Displays all folders.
 - Selected** - Displays selected folders only.
 - Protected** - Displays protected folders only.
 - Hidden** - Displays hidden folders only.

A red key  on a folder indicates that the folder is protected and/or encrypted.

The word "hide" on a folder  indicates that a folder is hidden using the **Hide While On-Line** feature.

This is also known as **expanding** a folder.

This is also known as **collapsing** a folder.

To display the contents of a folder in the Tree window, click on the plus sign (+) or double click on the folder.

To hide the contents of a folder in the Tree window, click on the minus sign (-) or double click on the folder.

To select a folder together with all its sub-folders, collapse the folder before selecting it as above.

To select an individual folder, click on the check box next to the folder icon. An individual folder is indicated by a minus sign or no symbol. A check mark appears in the box. To deselect a folder, click again on the check box. The check mark disappears.

Data Secure! Screens

This section discusses the various screens and briefly describes their function. Detailed procedures are contained in subsequent chapters.

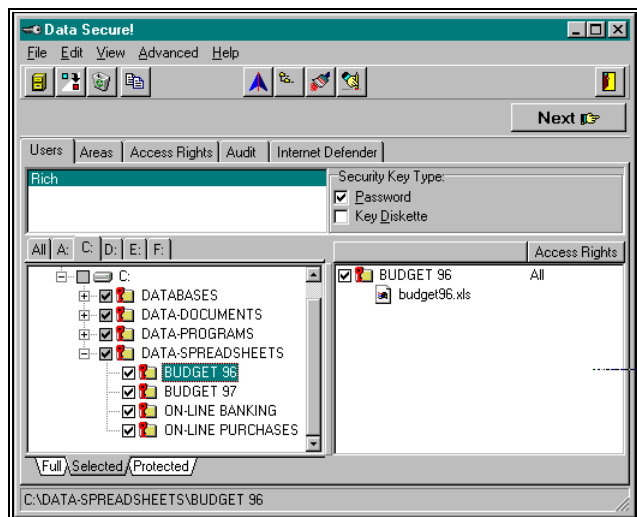
Menus and the toolbar are available from all screens.

The following screens are available via the Screen Selection tabs, below the toolbar. Click on a tab to view the screen.



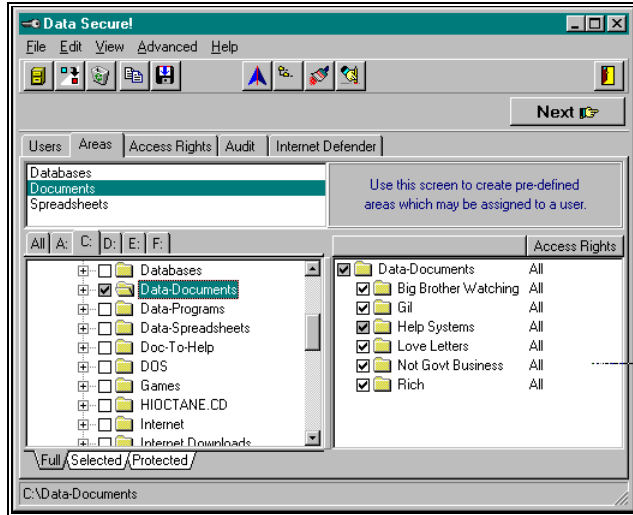
The Users Screen

Use the **Users** screen to create and modify authorized users and their access rights to protected folders.



The Folder Group Screen

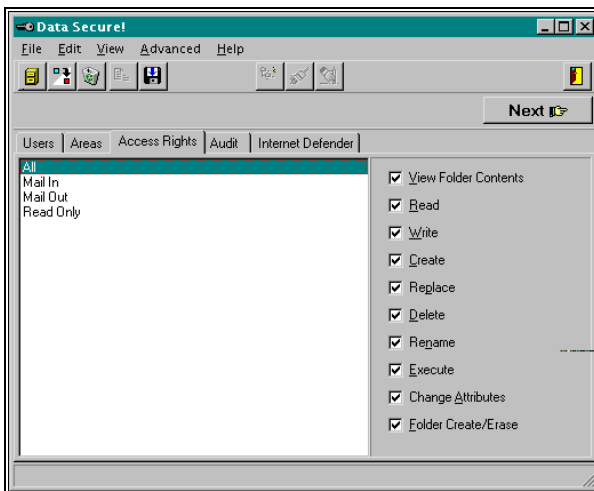
Use the Folder Group screen to create and modify pre-defined **Folder Groups** which can be assigned to authorized users.



Use the Definition Area to add or select a group name. Use the Tree window to select or modify the folders belonging to the selected group.

The Access Rights Screen

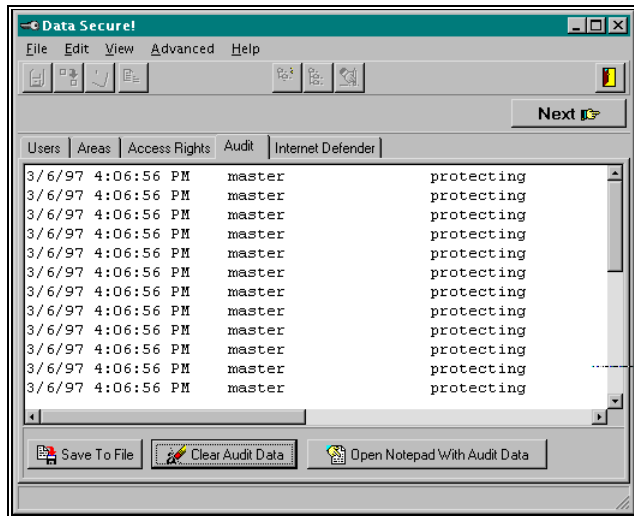
Use the Access Rights screen to create or modify pre-defined groups of access rights parameters which may be assigned to folders in **Authorized User** and **Folder Group** definitions .



Use the **Definition Area** to add or select a group name. Click the check boxes to the right to select an access category.

The Audit Screen

The **Audit** screen displays an audit list showing all logon and logoff attempts, including unsuccessful attempts. This audit list also contains changes to folder protection status.



Use the vertical and horizontal scroll bars to scroll through the list and to display additional data.

The pushbuttons below the window allow the user to save the audit data to a file, clear (erase) the audit data, or to annotate the audit data using a text editor.

The Internet Defender & Virus Protection Screen

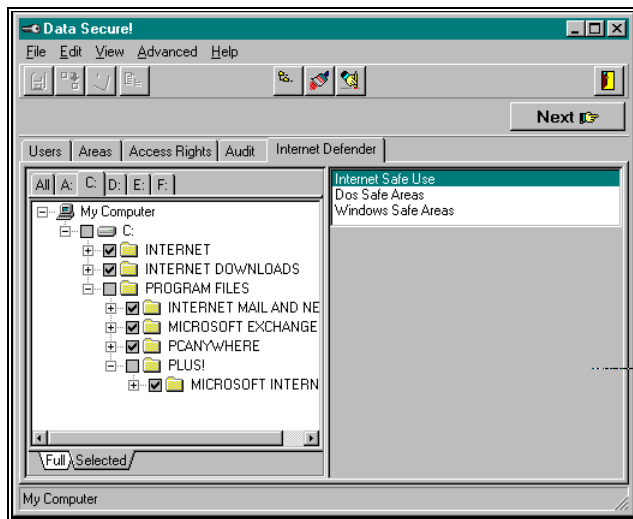
Tools such as Internet Defender & Virus Protection are commonly referred to as a **Firewalls**

We refer to those areas to which certain activities are confined as **Firewall Areas**

Internet Defender & Virus Protection is a collection of privacy and virus protection tools that protect your system by confining Internet and other on-line activities to special restricted areas called **Firewall Areas**.

Any attempt by a program originating from within a firewall area to create, write to or otherwise alter a file outside of that firewall area will be stopped and an error message will be displayed in the Warning Panel.

Use the **Internet Defender & Virus Protection** screen to define Firewall Areas and to designate folders as hidden from view while on-line.



Internet Defender & Virus Protection contains several different firewalls:

- Internet Safe Use areas contain folders from which Internet and/or other on-line resource applications may be run.
- The DOS Safe Area contains folders from which DOS based programs may be safely run.
- The Windows Safe Area contains folders from which a Windows installation program may be run and into which an application may be installed.
- Hide While Online hides designated folders, which are not otherwise protected by **Data Secure!**, from view while connected to a remote computer (i.e. during on-line registration or purchasing).



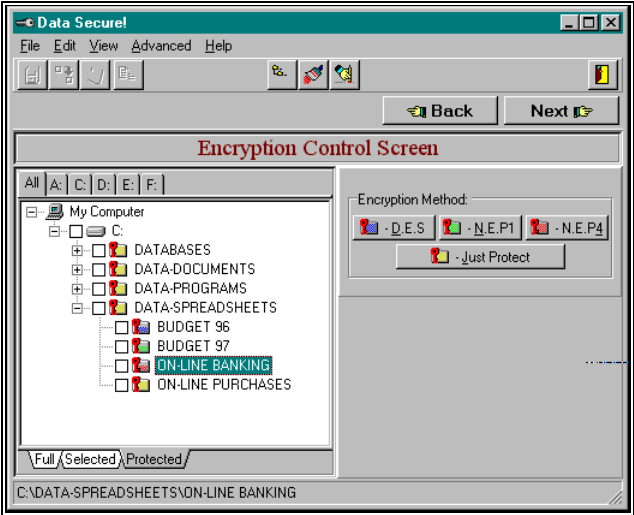
The following screens are used to change the encryption method, to change a users initial password and to confirm the definition and physically perform the encryption and protection. You access these screens by using the **Next** and **Back** pushbuttons located in the upper right-hand corner of the window.

You **MUST** page through all three screens in order to record any additions or changes to a user definition or folder protection.

To access these screens, click on **Next** to scroll forward to the next screen or **Back** to scroll backward to the previous screen.

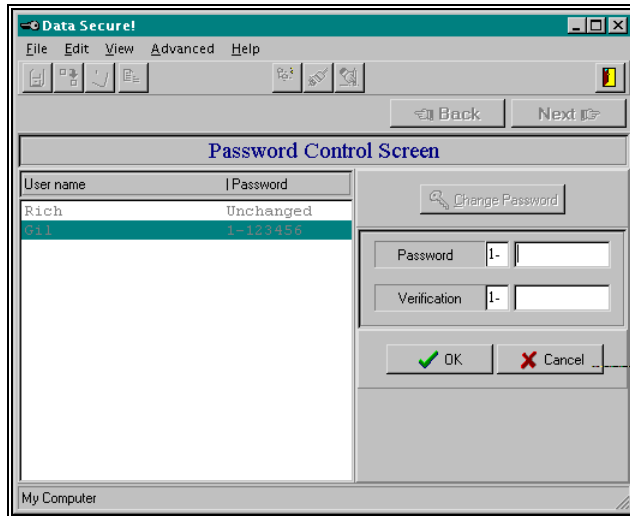
Encryption Control Screen

Use the Encryption Control screen to select the encryption protocol for protected folders. Use the folder tree to select the protected folders. Different encryption methods may be designated for different folders.



Password Control Screen

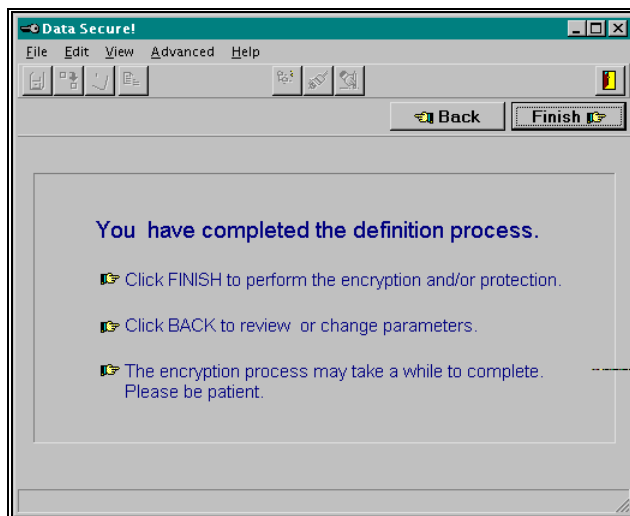
Use the Password Control screen to print out the initial password for a new authorized user. This screen may also be used to change the initial password for a new user should this be necessary.



Confirmation Screen



This screen appears at the end of the process of defining or modifying an authorized user. You **MUST** click on **Finish** in order to record the changes and to perform the protection and encryption.



This screen also displays appropriate warning messages.

Chapter 5 Using Data Secure! Configuration

Overview

An authorized user is one who has been granted access to protected folders by the System Administrator.

Protected folders may only be viewed or accessed by authorized users. A protected folder may or may not be encrypted.

This chapter provides detailed operating procedures and step-by-step instructions for using **Data Secure!** Configuration to define protected folders and authorized users. We suggest that you read **Chapter 4 Introducing Data Secure! Configuration** to familiarize yourself with the user interface.

The System Administrator uses **Data Secure!** Configuration to:

- Define authorized users
- Assign protected folders to authorized users
- Define access rights parameters for authorized users.


The System Administrator also uses **Data Secure!** Configuration to set parameters for the **E-mail Lock** and **Internet Defender & Virus Protection** utilities. **These features are discussed in subsequent chapters.**

A folder must be "assigned" to at least one authorized user in order to be protected and/or encrypted.

Note:

*Users must log in again after the System Administrator has used **Data Secure! Configuration**.*

To open **Data Secure! Configuration**:

1. Insert the Master Key Diskette.
2. **Right** click on the  lock icon located on the right-hand side of the taskbar. You may also run **Data Secure! Configuration** via the Start Menu.
3. Select **Run Data Secure! Configuration** from the shortcut menu. The Welcome screen appears. Click on **OK** to continue.

Overview of the User Definition Process

The user definition process consists of the following basic steps:

1. Start **Data Secure!** Configuration.
2. Add a new user or select an existing user to be modified.
3. Set system level options as necessary.
4. Select the security key type.
5. Assign folders to the user.
6. Define access rights parameters for folders assigned to the user.
7. Click on the **Next** pushbutton to go to the **Encryption Control Screen**. Select an encryption method to be used, if any, for individual protected folders.
8. Click on the **Next** pushbutton to go to the **Password Control Screen**. Review the initial password and change if desired. Print the Password Report and give it to the user.
9. Click on the **Next** pushbutton to go to the **Confirmation Screen**. Click on the **Finish** pushbutton to confirm the definition and perform data encryption.

Notes:

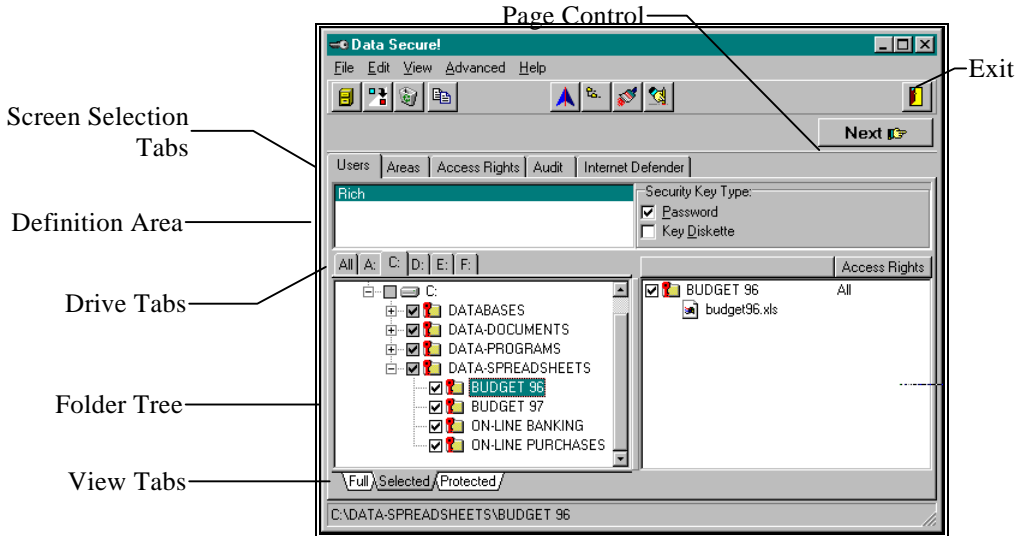
*You **MUST ALWAYS** page to the confirmation screen using the **Next** pushbutton, and then click on **Finish** (Steps 7-9) in order to complete the definition and physically perform the protection and encryption. These steps are always required even if no changes are made using these intermediate screens.*

You may define more than one user at a time by repeating steps 1 through 6 as often as necessary and completing steps 7 through 9 after the last user has been defined.

Data Secure! Configuration is highly flexible and provides several tools to simplify this process. For example, you may assign pre-defined groups of folders and access rights parameters to authorized users. You may also copy a definition from one user to another.

The System Administrator uses the Users screen to define authorized users.


To display the Users screen, click on the Users Screen tab.

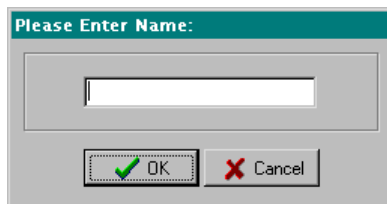


Creating and Modifying Users

Creating a New User

To create a new user:

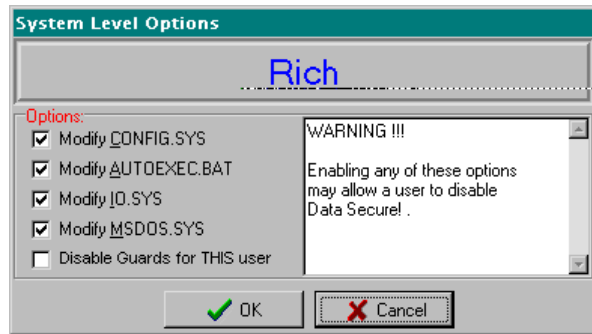
1. Open *Data Secure!* Configuration and select the **User** tab. The User screen appears.
2. Open the Enter Name dialog as follows:
 - Click on the **Add**  icon on the toolbar, or
 - Right click anywhere in the definition area and select **Add** from the shortcut menu, or
 - Select **Add User** from the **File** menu.
3. Type the new user name in the dialog box and click on **OK**.



Note:

The word "**Master**" is a reserved word and cannot be used for User or Folder Group names.

4. The name appears highlighted in the Users definition area and the **System Level Options** dialog box appears.



The System Administrator can control a user's ability to modify or delete certain system configuration files and can disable the *Data Secure!* Guards for an individual user. These options are discussed in detail in the *Data Secure! Guards* section.

5. Click in the check box to enable an option for this user. Click on **OK** to continue.
6. This completes the process of adding a new user. Proceed with the user definition process as described in the **Working With User Definitions** section.


Modifying a User Definition

To modify an existing authorized user definition :

1. Click on a name in the definition area of the **User** screen. That user name will appear highlighted.
2. Proceed with the definition process as described in **Working With User Definitions** section.
3. When finished, click on the **Next** pushbutton until the Confirmation screen appears. Click on **Finish** to confirm and record the selections.


Changing a Users Name

To change an authorized users name:

1. Click on a name in the definition area of the **User** screen. That user name will appear highlighted.
2. Do one of the following:
 - Click on the **Rename** icon  on the toolbar, or
 - Right click in the definition area and select **Add** from the shortcut menu, or
 - Select **Rename User** from the **File** menu.
3. Type a new name in the dialog box. Click on **OK** to continue.
4. When finished, click on the **Next** pushbutton until the Confirmation screen appears. Click on **Finish** to confirm and record the selections.

Erasing a User

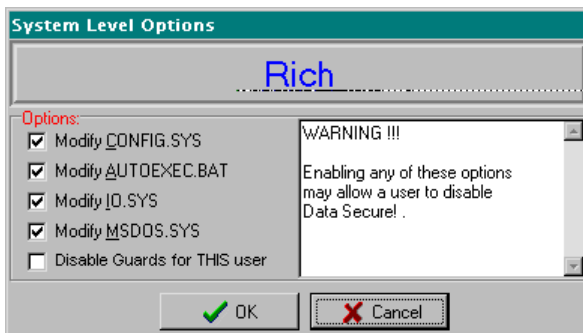
To erase an authorized user name:

1. Click on a user name in the definition area of the **User** screen. That user name will appear highlighted.
2. Do one of the following:
 - Click on the **Erase** icon  on the toolbar, or
 - Right click in the definition area and select **Erase** from the shortcut menu, or
 - Select **Erase User** from the **File** menu.
3. Click on the **Next** pushbutton until the Confirmation screen appears. Click on **Finish** to confirm and record the selections. Any folders assigned exclusively to this user will be decrypted and unprotected.

Working With User Definitions

Setting System Level Options

The System Administrator uses this dialog box to control a user's ability to modify certain system configuration files and to disable the *Data Secure!* Guards feature for an individual user.



Place a check mark in one of the first four boxes to permit modification of the indicated system configuration file.

Place a check mark in the final box to disable the *Data Secure!* Guards feature for the indicated user. If this option is grayed out the *Data Secure!* Guards are disabled for all users.

All of these boxes **MUST** be enabled for the System Administrator since this individual needs to control system operation and to deal with crashes and other emergencies. We strongly recommend, however, not to allow system configuration file modification and to enable the *Data Secure!* Guards for ordinary users.

The System Administrator **MUST** login before attempting to install or uninstall software and drivers. The System Level Options dialog box is displayed automatically when a new user is created.

If an unauthorized user attempts to modify any of the listed configuration files, a message will be displayed in the Warning Panel and the operation will be stopped.

To change the system level options:

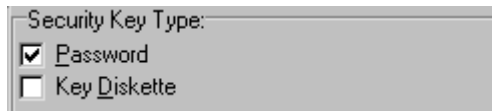
1. Click on the **User** tab to access the Users screen.
2. Click to select the desired user from the definition area.
3. Select **User Access** from the **Advanced** menu. **The System Level Options** dialog box appears.
4. Click the box next to the desired option. A check indicates that the option is enabled. Click on **OK** to close the dialog box.

Assigning a Security Key Type

The System Administrator may require an authorized user to login using a password, a key diskette or both .

Data Secure! Configuration does not create the user's Key Diskette. This will be done the first time the user logs in. Follow the procedures listed below for initial login using a password and/or a Key Diskette.

Do not attempt to copy or back up a user's Key Diskette. Unlike the Master Key Diskette, it cannot be backed up. The copy will not work and the original may become damaged.



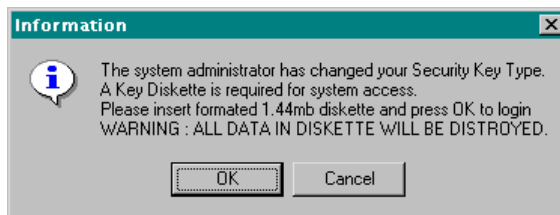
To assign a Security Key type to a user,

- Click on either or both of the check boxes to the right of the User screen definition area to select a security key type. **Password** is the default Security Key type.

To login for the first time using a Key Diskette :

The following procedure must be performed whenever the System Administrator assigns a user's security key type as **Key Diskette**, or **Key Diskette** and **Password** together.

1. Open the Login window.
2. Type the users password (or initial password assigned by the system) in Login window. Click on **OK** to continue.
3. An information dialog box appears. Insert a freshly formatted diskette into the designated drive and click on **OK** to continue.



4. If a password is not required together with a Key Diskette, an information message appears. Click on **OK** to continue. The former password is no longer valid in this case.
5. Login is complete. Remove the diskette. The Key Diskette must be used for subsequent login attempts.

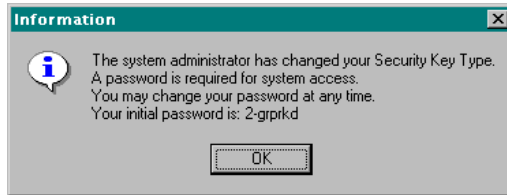
Note:

If only a key diskette is required, do not type anything in the Login screen. An incorrect password message will appear.

To Login the first time using a password:

The following procedure must be performed whenever the System Administrator assigns a user's security key type as **Password** or **Password** and **Key Diskette** together.

1. Open the Login window.
2. If a Key Diskette was previously required, place it in the drive. If you forget, a reminder will appear.
3. A dialog box appears indicating the new password. Write down the password. This password may be changed by the user at any time. Click on **OK** to continue.



4. If a key diskette is no longer required, an information message appears. Click on **OK** to continue.



5. Do not type the password at this time. Login is complete. Remove the diskette. The user must login using the password in subsequent attempts.

Assigning Folders to Authorized Users

The System Administrator grants an authorized user permission to access the contents of a folder by “assigning” it to that user. When a folder is assigned to at least one authorized user it becomes **protected** and it may also be **encrypted**.

Once a folder is protected it cannot be accessed by a user unless it is explicitly assigned to him or her.

Note:

Protected folders are fully protected from network access.

*Remote network users cannot access protected folders, even if **Data Secure!** is active on another workstation.*

Data Secure! Version 1.0 is designed for use on a single computer only. Folders located on remote network drives cannot be protected or assigned to users. Protected folders are inaccessible over a network.

A folder must be associated with at least one authorized user in order for it to be protected and/or encrypted. If a protected folder is unassigned from its only user or if the only user to which a folder is assigned is erased by the System Administrator, that folder will no longer be protected and may be accessed by all users.

To assign a folder to an authorized user:

1. Click on the box beside the folder in the Tree window. A check mark in the box indicates that a folder is selected. Remember that if you select a folder that has collapsed sub-folders (indicated by a plus sign (+) to the left), all of the sub-folders contained therein also become selected.
2. Use the **Selected** View Tab to display folders accessible to the user.
3. Use the **Protected** tab to display all protected folders, whether or not assigned to the user.
4. Use the **Drive Tabs** to display folders on a specific drive or on all drives.

Copying Definitions


Data Secure! supports the use of predefined sets of individual folders, known as **Folder Groups**. The System Administrator may assign some or all members of a Folder Group to a user simply by copying its definition. The procedures for creating and managing Folder Groups are discussed in the **Working With Folder Groups** section on page 49.

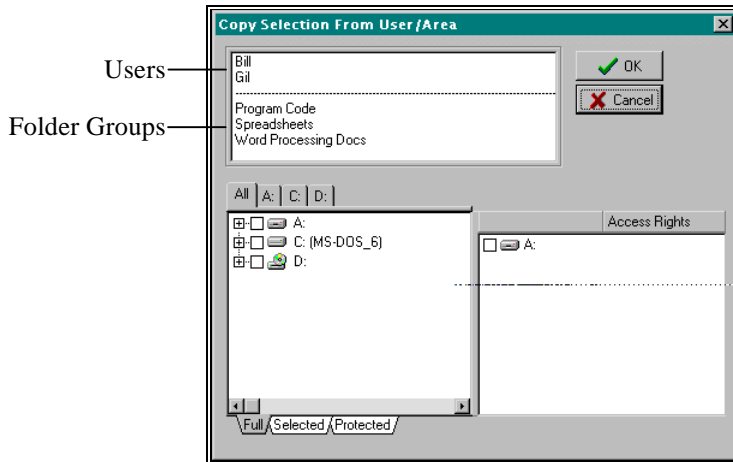
Likewise, complete or partial user definitions may be copied from one user to another, including folder assignments and all other parameters.

Any number of Folder Groups or user definitions may be copied to a user. A user definition created by copying Folder Groups and/or other user definitions can be freely modified.

To copy a Folder Group or User definition:

1. Click on the **User** tab to display the User screen.

2. Select the **User** or **Folder Group** you would like to copy using the Definition Area.
3. You may modify the folder selections at this point before continuing.
4. Click on the **Copy** icon  on the toolbar. The Copy Selection window appears.



5. Select the Folder Group or User definition from the definition window at the top of the Copy Selection window.
6. Add or remove folders using the Folder Tree.
7. Click on **OK** to copy the definition.
8. You may repeat this procedure as necessary to copy additional users or folder groups. The effect is cumulative, as each definition is added to the user currently being defined.

Defining Access Rights

By assigning **Access Rights Parameters**, the System Administrator can control access to folders and their contents by authorized users. The following access rights parameters are available:

View Folder Contents - The user may view the contents of a protected folder.

Read - The user may open and read a file contained in a protected folder.

Write - The user may save a file to a protected folder.

Create - The user may add new files to a protected folder. The **Write** option must also be selected in order for **Create** to function correctly.

Replace - An application may replace all of the contents of an existing file in a protected folder.

Delete - The user may delete a file in a protected folder.

Rename - The user may rename a file in a protected folder.

Execute - The user may run a program located in a protected folder. Please note that the **Read** parameter must also be selected in order to run a program.

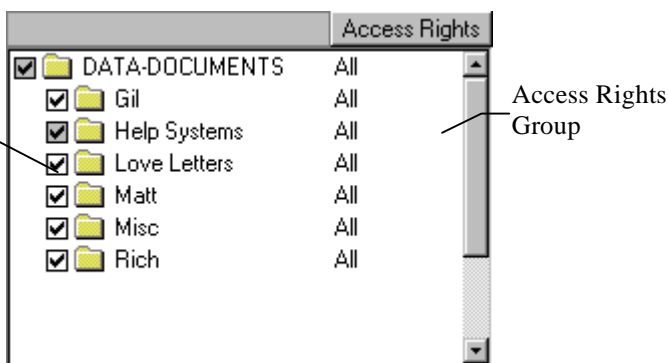
Change Attributes - The user may change the operating system file attributes for files or folders in a protected folder.

Folder Create/Delete - The user may create or delete sub-folders in a protected folder.

*The default access rights parameters may be changed by selecting **Default Options** from the **Advanced** menu.*

The System Administrator uses the **Access Rights** window on the **Users** screen to define access rights for files located in folders assigned to an authorized user.

Selected folders are indicated by a check



Important

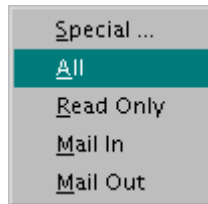
If you click on a unchecked folder or on a data file, the menu will not appear.

The current definition is displayed on the right-hand side of the screen. By default users are given full access rights to folders.

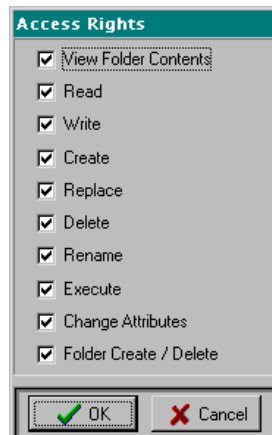
By default, an authorized user is granted all access rights parameters. The System Administrator may change this default.

To modify Access Rights to a protected folder:

1. Click on the **User** tab to display the Users screen.
2. Right click on any selected (checked) folder in the Access Rights window. A shortcut menu of choices appears on the screen.



3. Select one of the pre-defined Access Rights groups or select **Special** to define custom access rights. The above example shows the pre-defined Access Rights groups. The System Administrator may create others, which would then appear on this menu. The default groups are as follows:
 - **All** - The user has unlimited rights to all protected files.
 - **Read Only** - The user may open and read a file contained in a protected folder, but cannot modify or save it in a protected folder.
 - **Mail In** - The user may only read and delete files in a protected folder. This is useful for incoming E-mail message folders.
 - **Mail Out** - The user may only create new files. This is useful for folders containing outgoing E-mail messages.
4. If **Special** is selected, a menu of access rights parameters appears.



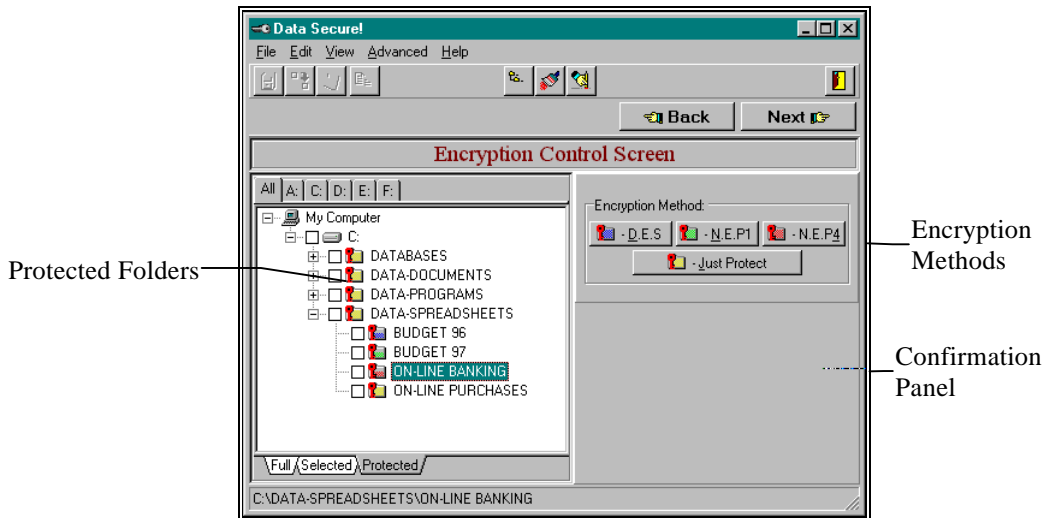
Click on the box to select or de-select an access rights parameter. A check indicates that a parameter is selected.

Selecting the Encryption Method

Data Secure! supports three different encryption methods as well as protection without encryption. Use the Encryption Control screen to select the appropriate encryption method for the selected folders.

We suggest that you only encrypt folders containing the most sensitive or private information. Protection without encryption offers excellent privacy for ordinary data.


We also recommend that you do not protect or encrypt folders containing Windows utility software. Such programs are not confidential and encryption may, in very rare circumstances, affect their operation.



By default, folders are protected without encryption. The default encryption protocol may be changed by the System Administrator.

The Tree window identifies protected folders by colored locks next to the folder icon. The color of the lock indicates the encryption method according to the key on the right-hand side of the screen.

To access the Encryption Control Screen:

1. Click on the **User** tab to display the Users screen.
2. Click on the **Next**  pushbutton located in the upper right-hand corner of the Users screen.

To change encryption method:

1. Click to select one or more folders. You can only select a folders containing a key symbol. A check mark indicates selected folders.
2. Select an encryption method from among the following options:
 - **DES** is the U.S. Government Data Encryption Standard.
 - **NEP1** and **NEP4** are Nisita proprietary encryption methods. The **NEP4** method is faster but less effective.
3. **Just Protect** indicates protection without encryption. This is the default option.
4. The **Encrypt Data Only** box is checked by default, indicating that executable program files are not encrypted. If you wish to encrypt all files including executable files, click on the box to remove the check mark.
5. Click on **OK** to continue.

This procedure may be repeated as often as necessary to change other folders.

The default encryption method may be changed by selecting **Default Options** from the **Advanced** menu.

To advance to the next screen, click on the **Next** pushbutton. The Password Control screen appears.

Selecting the Initial Password

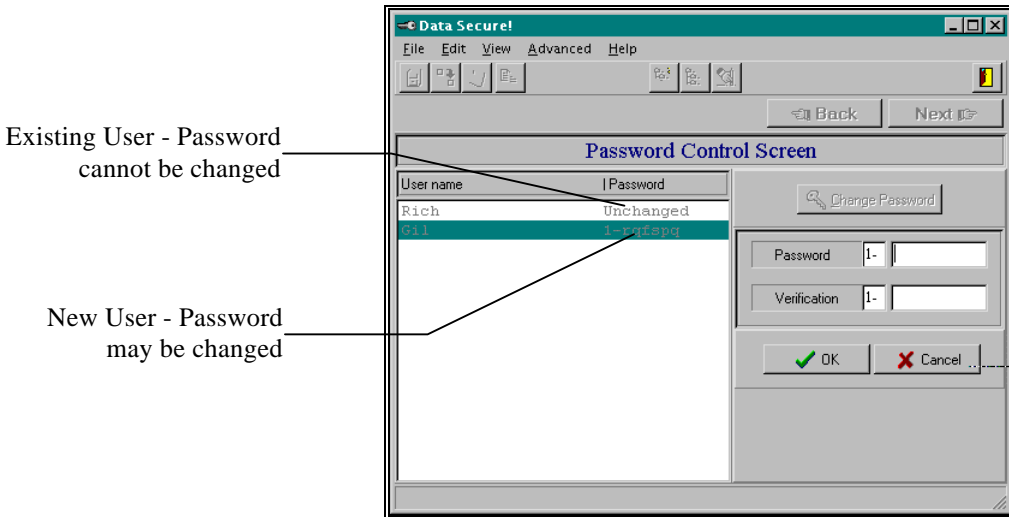
When a new authorized user is defined, *Data Secure!* automatically assigns a password. Usually, it is not necessary to change the initial password since the user can change it at will. The System Administrator should print a report showing the initial password and give it to the authorized user. The System Administrator cannot change the password after user is created.

The System Administrator uses the Password Control screen, shown below, to print the password report and/or change the initial password.



The System Administrator should always print the password report and give it to the user, as this is the only record of his initial password.

To access the Password Control Screen:

- Click on the **Next**  pushbutton located in the upper right-hand corner of the **Users** screen.

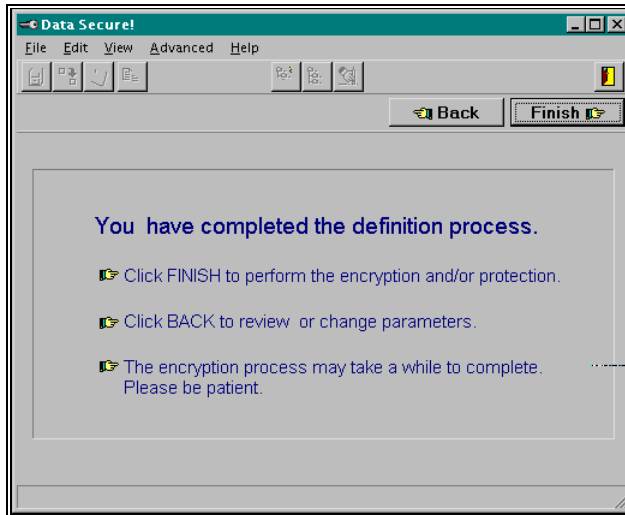


To change an authorized user's initial password:


1. Double click on the new user's name in the definition window, or click once on the user name and then click on the **Change Password** pushbutton.
2. Enter the new password in the **Password** box. Only the text portion of the password may be changed. The number and the dash are fixed.
3. Press the **TAB** key to advance to the **Verification** box and retype the password.
4. Click on **OK** to confirm. If an error message appears repeat steps 3 and 4.
5. Click on the **Print**  icon to print the password report. Give this report to the user. You may also view the password report on the screen by clicking on the **View**  Icon.
6. When you are finished with the Password Control screen, click on the **Next** pushbutton to advance to the Confirmation screen.

Confirmation and Encryption

The Confirmation screen is the last step in the definition process. This screen also displays appropriate warning messages.



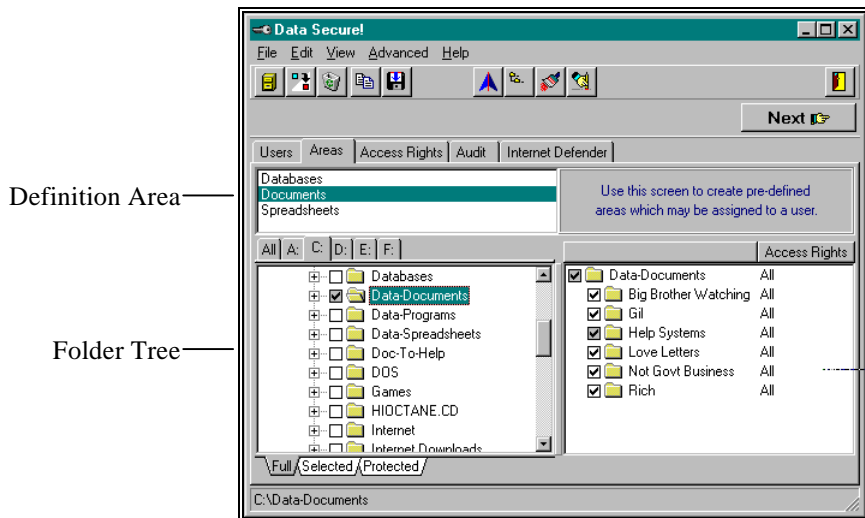
To confirm the definition and perform the protection and encryption:

Click on the **Finish**  pushbutton. A window will open showing the progress of the protection/encryption process. If you selected many folders for encryption, this may take quite some time.

Remember, you MUST perform this step in order to record any additions or changes and to physically perform the encryption and protection.


Working with Folder Groups


The System Administrator uses the **Areas** screen to create or modify pre-defined groups of folders which may be assigned to individual users.




You cannot assign folders on a remote network drive to a folder group.

To create a new Folder Group:



1. Click on the **Areas** window selection tab.
2. Create a name in the definition area as follows:
 - Click on the **Add** icon  on the toolbar, or
 - Right click in the definition area and select **Add** from the shortcut menu, or
 - Select **Add Area** from the **File** menu.
3. Type the name in the dialog box. Click on **OK** to continue.
4. Select the folders to be included in the group using the Tree window.

You may use the **Copy Selection** feature to copy definitions from other folder groups or authorized users. This feature is discussed in the **Assigning Folders to Authorized Users** section on page 41.
5. Define access rights for the folders using the Access Rights window **as discussed on page 42**.
6. Click on the **Save**  icon on the toolbar to save the new group. If this is not done, the new group will not be available the next time you use **Data Secure!** Configuration.



To modify an existing Folder Group:

1. Move to the **Areas** window using the **Window Selection** tabs.
2. Click on the desired name in the definition area.
3. Change the folder selections or access rights as required.
4. Click on the **Save**  icon on the toolbar to save the new group. If this is not done, the new group will not be available the next time you use *Data Secure!* Configuration.

To rename a Folder Group:

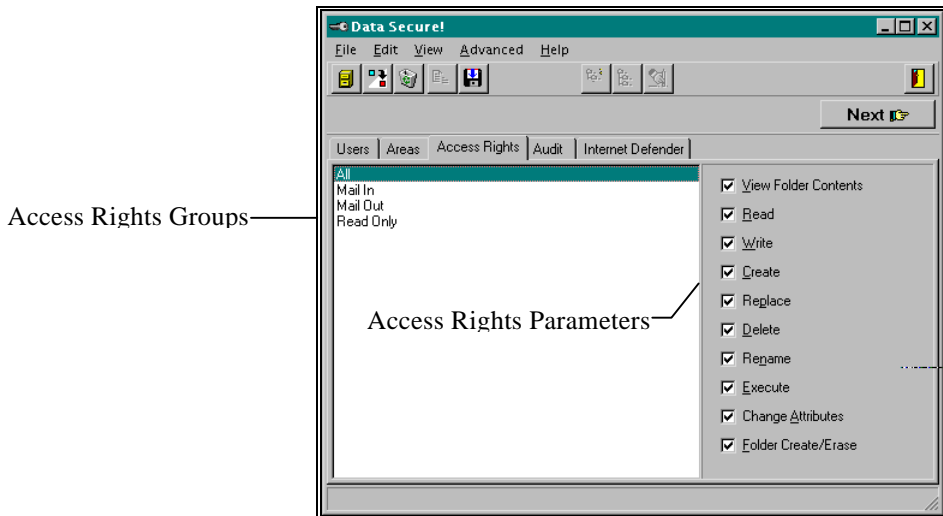
1. Move to the **Areas** window using the Window Selection tabs.
2. Click on the desired name in the definition area, and
 - Click on the **Rename**  icon on the toolbar, or
 - Right click in the definition area and select **Rename** from the shortcut menu, or
 - Select **Rename Area** from the **File** menu.
3. Type the name in the dialog box. Click on **OK** to continue.
4. Click on the **Save**  icon on the toolbar to save the new group. If this is not done, the new group will not be available the next time you use *Data Secure!* Configuration.

To erase a Folder Group:

1. Move to the **Areas** window using the Window Selection tabs.
2. Click on the desired name in the definition area, and
 - Click on the **Erase**  icon on the toolbar, or
 - Right click in the definition area and select **Erase** from the shortcut menu, or
 - Select **Erase Area** from the **File** menu.
3. Click on **OK** in the confirmation box to continue.
4. Click on the **Save**  icon on the toolbar to save the new group. If this is not done, the new group will not be available the next time you use *Data Secure!* Configuration.



Working with Access Rights Groups

The System Administrator uses the **Access Rights** screen to create and modify pre-defined groups access rights parameters. Access Rights groups appear in the menu that pops up while defining folder access rights in the **Access Rights** window of the **User** and **Areas** screens.




The various access rights parameters are discussed in the section dealing with access rights parameters on page 44.



To create a new Access Rights Group:

1. Click on the **Access Rights** tab to display the Access Rights screen.
2. Create a name in the definition area as follows:
 - Click on the **Add** icon  on the toolbar, or
 - Right click in the definition area and select **Add** from the shortcut menu, or
 - Select **Add Access Rights** from the **File** menu.
3. Type the name in the dialog box. Click on **OK** to continue.
4. Select the access rights categories from the list on the right. A check mark indicates that a category is selected.
5. Click on the **Save**  icon on the toolbar to save the new group. If this is not done, the new group will not be available the next time you use *Data Secure!* Configuration.



To modify an existing Access Rights Group:

1. Move to the **Access Rights** window using the Window Selection tabs.
2. Click on the desired name in the definition area.
3. Change the access rights parameters as required.
4. Click on the **Save**  icon on the toolbar to save the new group. If this is not done, the new group will not be available the next time you use *Data Secure!* Configuration.

To rename an Access Rights Group:

1. Move to the **Access Rights** window using the Window Selection tabs.
2. Click on the desired name in the definition area, and
 - Click on the **Rename**  icon on the toolbar, or
 - Right click in the definition area and select **Rename** from the shortcut menu, or
 - Select **Rename Access Rights** from the **File** menu.
3. Type the name in the dialog box. Click on **OK** to continue.
4. Click on the **Save**  icon on the toolbar to save the new group. If this is not done, the new group will not be available the next time you use *Data Secure!* Configuration.

To erase an Access Rights Group:

1. Move to the **Access Rights** window using the Window Selection tabs.
2. Click on the desired name in the definition area, and
 - Click on the **Erase**  icon on the toolbar, or
 - Right click in the definition area and select **Erase** from the shortcut menu, or
 - Select **Erase Access Rights** from the **File** menu.
3. Click on **OK** in the confirmation box to continue.
4. Click on the **Save**  icon on the toolbar to save the new group. If this is not done, the new group will not be available the next time you use *Data Secure!* Configuration.

Chapter 6 *Data Secure!* Advanced Features

Overview

This **chapter** discusses several additional features of *Data Secure!*:

- *Data Secure!* Guards
- Boot Lock
- Replacing Or Re-Creating Master Key Diskettes
- Encrypted Backup And Restore
- *Data Secure!* Default Options
- Uninstalling *Data Secure!*

Data Secure! Guards

Introduction

Data Secure! Guards protect you system from damage resulting from hostile virus activity, hackers and the actions of inexperienced users.

The System Administrator may choose to activate the *Data Secure!* Guards on a global basis. *Data Secure!* Guards protection may be disabled by the System Administrator for specific users.

DOS Guard

DOS Guard prevents unauthorized users from starting the computer in the MS-DOS mode or from using the Windows 95™ startup option keys. Booting in the MS-DOS mode may allow a user to erase or damage files, even in *Data Secure!* protected folders.

The System Administrator may choose to prevent a user from restarting in the MS-DOS mode and/or using the Windows 95™ startup option keys.

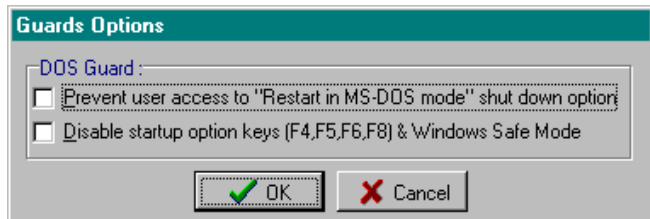
Configuring the *Data Secure!* Guards

The System Administrator activates the individual *Data Secure!* Guards on a global basis. By default, active Guards affect all users. The System Administrator may subsequently disable Guards protection for individual users.

We recommend that Guards protection be disabled only for the System Administrator and users authorized to maintain the system. The Guards should remain enabled for all ordinary users.

To globally activate individual *Data Secure!* Guards:

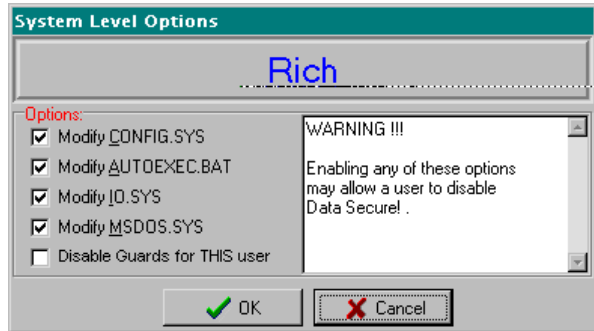
1. Run *Data Secure!* Configuration and click on the **Users** tab to display the Users screen.
2. Select **Guards Options** from the **Advanced** menu. The Guards Options dialog box appears.



3. Click on the check boxes to activate or deactivate one or both of the Guards. A check mark indicates that a Guard is active.
4. Click on **OK** to confirm and close the dialog.

To enable or disable Guards protection for an individual user:

1. Run *Data Secure!* configuration and display the User screen.
2. Select a user in the Definition area.
3. Select **User Access** from the **Advanced** menu. The System Level Options dialog box appears.



4. Check the **Disable Guards** option. A check mark indicates that all active Guards are disabled for this individual user.
5. Click on **OK** to confirm and close the dialog.

Boot Lock

Boot Lock requires authorized users to enter their password during the computer start up (boot) process. This prevents unauthorized individuals from attempting to start the computer or from interfering with the start up process.

Boot Lock also includes a Recovery Diskette feature that allows a user to restore the primary hard disk partition table in the event of damage resulting from hardware failure or virus infection.

Using Boot Lock

Boot Lock is an optional feature that may be enabled or disabled by the System Administrator. Boot Lock affects all authorized users.

When a user turns the computer on or restarts the computer, a message appears requiring him or her to enter a password. If the password is valid the start up process continues. At the conclusion of the process, the Login screen appears. It is not necessary to enter the password a second time. Simply click **OK** to login.

If an incorrect password is entered while booting the computer, the user is given two additional opportunities to enter the correct password. If the user fails to enter the correct password after these three attempts, the computer will lock up and must be restarted in order to try again.

In order for Boot Lock to function, the System Administrator must assign the **Password** Security Key type to all users. A key diskette may be required in addition to the password.

If a user attempts to bypass Boot Lock by starting the computer from diskette, the primary hard disk (usually drive C:) will be inaccessible. Secondary hard disks or partitions, however, will continue to be accessible.

WARNING: The Boot Lock feature will not function properly on compressed drives. Do not enable Boot Lock if your primary hard disk is compressed using Drive Space™ or another compression utility. You must decompress your disk and disable your compression utility before using Boot Lock.

To enable Boot Lock:

1. Run *Data Secure!* configuration and click on the **Users** tab to display the User screen.
2. Select **Boot Lock** from the **Advanced** menu.
3. Click to put a check mark in the **Enable Boot Lock** check box.
4. Insert a diskette in the drive when prompted. Boot Lock will create Recovery Diskette. You may use a Master Key diskette.
5. Boot Lock is now active. On some computers, a DOS window appears containing the message “System Transferred”. If this happens, close the window.

To disable Boot Lock:

1. Run *Data Secure!* configuration and click on the **Users** tab to display the User screen.
2. Select **Boot Lock** from the **Advanced** menu.
3. Click to remove the check mark in the **Enable Boot Lock** check box. Boot Lock is now disabled.

Using the Recovery Diskette

A Recovery Diskette is automatically created when Boot Lock is enabled. The Recovery Diskette can be used to recover the partition table for the primary hard disk (usually drive C:). Partition tables located on secondary hard disks or partitions cannot be recovered using a Recovery Diskette.

To restore a damaged partition table:

1. Turn the computer off.
2. Re-start the computer from a bootable diskette. The Recovery Diskette is usually suitable for this purpose.

3. Insert the Recovery Diskette into the drive.
4. Run the program **bl_rcv.exe** from the Recovery Diskette. This program automatically restores the partition table.

Removable Media Protection

Data Secure! can control access to removable media such as diskettes, CD ROM and ZIP™ drives. Other types of removable media may be protected if its device driver is recognized by Windows 95™ as a removable device.

This feature is useful in preventing unauthorized copying of confidential material to diskettes and preventing virus infection from infected media.

When a removable device is assigned to a user, no other user can access it unless it is also assigned to him. Like a protected folder, a removable device must be assigned to at least one user in order to be protected.

To protect a removable device:

1. Open *Data Secure!* Configuration and click on the Users tab to display the Users screen.
2. Select a user from the definition area.
3. Select the removable device from the Folder Tree.
4. Assign the desired access rights using the Access Rights window.
5. Click on the **Next** pushbutton until the Confirmation screen appears. Click on **Finish** to record the selections.

Tips and Examples

- You cannot protect an entire hard disk, a network drive or other non-removable drive. If you attempt to do so, *Data Secure!* will beep and will not accept the selection.
- You may wish to prevent employees from copying confidential data to a diskette. To do this, try the following:
 1. Create a user and assign the diskette drives to him.
 2. Assign all access rights parameters except **Write, Create, Replace** and **Folder Create/Delete** to this user.

This user will be able to view files located on the diskette, copy files from the diskette and run programs from the diskette. The user can neither copy nor save files to the diskette.

- You may wish to prevent children from running potentially infected programs from diskettes. To do this, try the following:

1. Create a user name for the child and assign the diskette drives to him.
2. Assign only the **View Folder Contents**, **Write, Replace, Create** and **Change Attributes** access rights parameters to this user.

The child will be able to view the diskette contents or copy files to the diskette but will be prevented from running any programs on the diskette and from accessing any files located on it.

Replacing or Re-Creating Master Key Diskettes

Master Key diskettes are required in order to run the *Data Secure!* Configuration program.

The System Administrator may wish to replace or re-create the Master Key Diskettes if the original is lost or stolen.

To replace or re-create the Master Key Diskettes:

1. Select **Re-Create Master Key Diskette** from the Advanced Menu. Insert a freshly formatted diskette in the drive. You may reuse existing Master Key Diskettes if they are not damaged.
2. A confirmation dialog box appears. Click on **Yes** to continue. A second dialog box appears. Click on **OK** to continue.
3. The Create Backup dialog box appears. Click on **Yes** to make a backup Master Key diskette.
4. Repeat step 3 until a sufficient number of backups are created. Click on **No** to complete the process.

Encrypted Backup and Restore

Overview

Data Secure! automatically decrypts files in an encrypted folder whenever an authorized user attempts to access them. This, however, is not desirable when backing up or restoring encrypted data. Such data should be backed up and restored in its encrypted state in order to prevent unauthorized access to the data on the backup media.

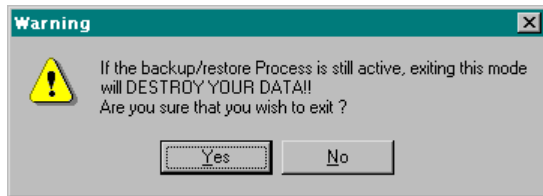
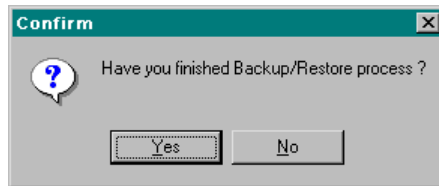
When the Encrypted Backup/Restore mode is active, **Data Secure!** will not decrypt files in encrypted folders.

To back up and restore encrypted data:

1. Select **Encrypted Backup/Restore Mode** from the Advanced Menu. A message window appears:



2. Use your software to perform the backup and/or restore. Make certain that the backup or restore process is finished before proceeding.
3. When you are finished, click on the Exit pushbutton on the message window. Two confirmation dialog boxes appear in sequence.



4. Verify that the backup/restore process is indeed completed. Click on **Yes** in each dialog to continue. *Data Secure!* will resume normal operation.

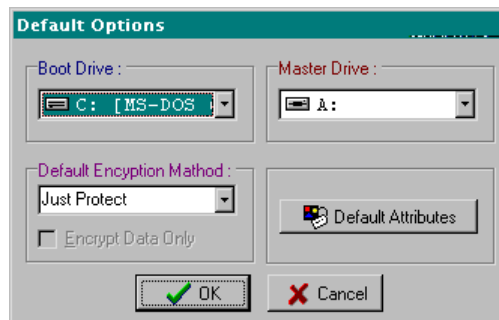
Data Secure! Default Options

Overview

Data Secure! makes use of several system defaults which can be changed by the System Administrator as desired. The System Administrator uses the **Default Options** dialog box to set or modify these parameters.

To modify the default options:

- Select **Default Options** from the **Advanced** menu. The Default Options dialog box appears.



Boot Drive

This indicates the drive that contains the system start-up (“boot”) files. This is almost always drive “C”. If your computer boots from a drive other than drive “C”, select the correct drive from the list box.

Master Drive

This indicates the diskette drive used for the System Administrator’s Master Key Diskette and User Key Diskettes. It is initially specified during the installation process.

- **To change the Master Drive**, select the desired diskette drive from the list box.

Default Encryption Protocol

This indicates the default encryption protocol that is automatically assigned to newly designated protected folders. The System Administrator may change the encryption protocol for a given folder or folders using the **Encryption Control Screen**.

The system default encryption protocol is **None**.

To change the default encryption protocol:

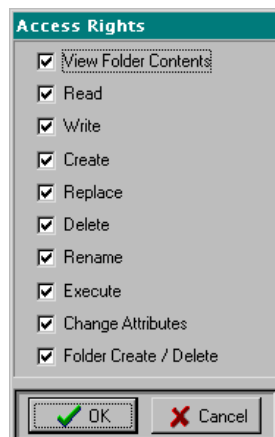
1. Select the desired default protocol from the combo box.
2. Put a check mark in the **Encrypt Data Only** check box to instruct *Data Secure!* to encrypt only data files (non-executables) by default.

Default Access Rights

Whenever the System Administrator assigns a folder to a user, *Data Secure!* automatically assigns that folder the default access rights parameters. The original default is the **All** access rights group which grants full access to a folder and its contents.

To change the default access rights parameters:

1. Click on the **Default Attributes** pushbutton. The Access Rights dialog box appears.



2. Put a check mark in the box next to the access rights parameter which you wish to assign as a default.
3. Click on **OK** to close the dialog.

Uninstalling *Data Secure!*

In order to uninstall *Data Secure!* all of the installation and initial configuration steps, as described in the Installation chapter, must have been successfully completed.

To uninstall *Data Secure!*:

1. Run *Data Secure!* Configuration.
2. Erase all users.
3. When all users have been deleted, click on the **Next** pushbutton until the Confirmation screen appears.
4. Click on the **Finish** pushbutton. *Data Secure!* will decrypt all encrypted folders and unprotect all protected areas.
5. Select **Uninstall Data Secure!** from the Advanced Menu or use the **Add/Remove Programs** feature on the Windows 95™ Control Panel.
6. When the Uninstall window appears, click on **OK**.
7. When the Erasing *Data Secure!* Files window appears, click on **OK**. Click on **OK** on the confirmation box.
8. Restart your computer.

Chapter 7 Using E-Mail Lock

Overview

E-Mail Lock allows you to quickly and easily encrypt E-mail messages and other text documents “on the fly”. The recipient can decrypt them just as quickly and easily.

This chapter describes the features of *E-Mail Lock* and provides step-by-step instructions for its use.

Why You Need *E-Mail Lock*

Simply put, E-mail is not a very private or secure form of communication. E-mail messages sent via the Internet, commercial on-line services or even over a network can easily be intercepted and read by hackers and other intruders. Other documents such as memos, reports, proposals, price lists, etc. are equally vulnerable while traveling along the information superhighway.

E-Mail Lock protects your privacy by providing powerful on-line encryption and decryption capability for E-mail messages and other documents. *E-Mail Lock* is simple to use and works effortlessly with most E-mail and word processing applications. With *E-Mail Lock* you can encrypt all or part of a document.

How *E-Mail Lock* Works

E-Mail Lock works within your E-mail and word processor software. The sender activates *E-Mail Lock* by using a special key combination or by double clicking on the *E-Mail Lock* icon. The sender then selects a name from a list of pre-defined recipients and *E-Mail Lock* automatically encrypts the message or document.

Only the designated recipient can read the document. This recipient opens the encrypted document in his E-mail program or word processor and activates *E-Mail Lock* using the same techniques. The document automatically decrypts with no further action required.

E-Mail Lock uses pre-defined “**Recipients**” as encryption keys. Recipients may be defined globally by the System Administrator or privately by an authorized user. The mere presence of the same “recipient” definition on the receiving computer enables the automatic decryption.

E-Mail Lock also supports manually defined **Passwords** which must be given to a recipient in order to decrypt the message.

Limitations and Cautions

RTF or Rich Text Format is the Microsoft standard for formatted text in Windows™ and Windows 95™.

E-Mail Lock is designed to work with virtually any Windows 95™ E-mail application. *E-Mail Lock* also works well with text editors and those word processors that support the **RTF** standard.

E-Mail Lock is designed as a tool for use with E-mail and other text documents. While *E-Mail Lock* is capable of encrypting and decrypting non-text objects such as graphics, sound files or embedded OLE objects, you may wish to avoid this. Non-text objects often result in large encrypted files that take longer to send via E-mail.

E-Mail Lock is not intended to work with non text applications such as spreadsheets, databases or drawing programs.

The E-mail client included in **Microsoft Internet Explorer™** does not allow a user to modify a received message. Therefore, you cannot use *E-Mail Lock* to decrypt messages received with this software. Refer to the **Decrypting Documents** section for a work-around.

Encrypting Documents

This section describes the procedures for encrypting documents and messages with *E-Mail Lock*.

You may encrypt an entire document or any portion thereof. *E-Mail Lock* supports multiple levels of encryption whereby an encrypted section may be included within another encrypted section. For most purposes, however, it is not needed.


A document may be encrypted by using either of two methods:

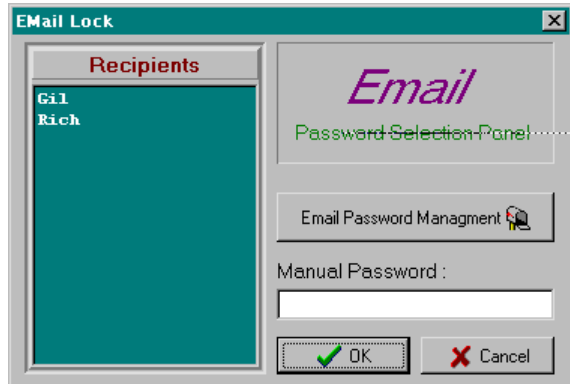
- Pre-defined recipients
- Manual Password

The pre-defined recipient is the easier of the two methods. The sender simply selects a recipient from a list. The identical recipient definition must be present on the recipient’s computer.

Alternatively, the sender may choose to enter a manual password. The identical password must be entered by the recipient in order to decrypt the document.

To encrypt an entire document:

1. Compose the document using your E-mail program or word processor. Place the cursor anywhere within the document.
2. Activate **E-Mail Lock**, using either of the following methods:
 - Double Click on the **E-Mail Lock** icon  located in the lower right-hand corner of the taskbar, or
 - Press the **Control** and the **Zero (Ctrl-0)** keys simultaneously.



3. The **E-Mail Lock** window appears. Click to choose a recipient from the list or enter a password in the **Manual Password** box to the right.
4. Click on **OK** to continue. **E-Mail Lock** encrypts the document. Some word processors may require an additional confirmation step.

The encrypted text appears as a random series of characters **as shown**:

```
=====> Encrypted Block Starts:  
ADAKNGCIBPCJBPGEAAAAGOMBKEI EPDKGNNEFDKICAHCDMDKFKMJELHFB  
DCLKDFHLFNNGKGPDKJCHMJDLHHJKOELEKOIGEDLNIBCLNCHHIFNMAAA  
OJFBCAKMLOMNL DOPBKLGCCNLI EEDJGHH  
=====> Encrypted Block Ends...|
```

To Encrypt a portion of a document:

1. Select the part to be encrypted.
2. Activate **E-Mail Lock** as described above.
3. Choose a recipient or enter a password in the **Manual Password** field.
4. Click on **OK** to encrypt the section.
5. We recommend that you press the **Enter** key once to separate the encrypted section from the adjoining text.

Decrypting Documents

The decryption process is also quite simple:

To decrypt an entire document:

1. Simply place the cursor in the encrypted text. Make certain that no part of the encrypted text is actually selected.
2. Activate **E-Mail Lock**.
3. If a **pre-defined recipient** was used, the document will decrypt automatically.

If the recipient is not defined on the receiving computer or is defined incorrectly the document will not decrypt and the **E-mail Password** dialog will appear. Enter the recipient password in the space provided and click on **OK** to continue. If the password is correct the document will decrypt.

4. If a **manual password** was used, a dialog box appears:



Enter the password exactly as provided by the sender and press **OK** to continue.

To decrypt an encrypted portion of a document

1. Select the encrypted section. Start with the text “=====> Encrypted Block Starts:” at the beginning of the block and include the text “=====> Encrypted Block Ends..:” at the end of the block.

When decrypting a section, make certain that you have selected the text exactly as described above. If you select the text incorrectly, **E-Mail Lock** will act as if you intend to encrypt another section.

2. Activate **E-Mail Lock** and continue as above.

Caution

*If decryption fails to start and/or the **E-Mail Lock** window appears, you have probably made an error while selecting the text. **DO NOT** select a recipient or enter a password. Press **Cancel** to close the window.*

Try to select the text again, making sure that you begin the selection with the text “=====> Encrypted Block Starts:”.

Decrypting Messages with Microsoft Internet Explorer™

The E-mail client included in **Microsoft Internet Explorer™** does not allow a user to modify a received message. Therefore, you cannot use **E-Mail Lock** to decrypt messages received with this software. If you are using Internet Explorer to receive E-mail the following procedure may be used as a work-around.

E-Mail Lock functions normally with **Microsoft Exchange™**.

To decrypt messages using Internet Explorer:

1. Copy the entire message or the encrypted part thereof to the clipboard. Select **Copy** from the **Edit** menu or use the **Ctrl-C** key combination to do this.
2. Paste the message into **Word Pad** or another text editor.
3. Follow the normal procedures to decrypt the message.

Working With Recipients

E-mail Lock supports two different types of recipients.

Global Recipients are defined by the System Administrator and are available to all system users without restriction.

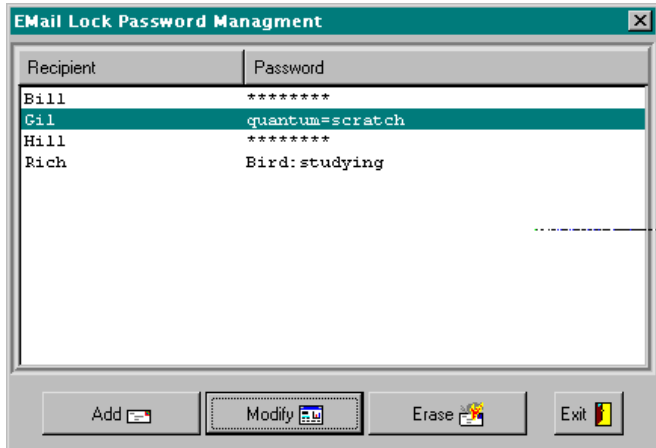
Private Recipients are defined by an authorized user and are available only to that authorized user while he is logged in. The System Administrator may not modify a private recipient nor view the password.

The recipient definition consists of a user name and a password. E-mail passwords are used as the encryption key.

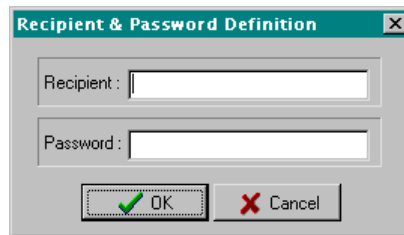
Adding a Recipient

To add a global recipient:

1. Run *Data Secure!* Configuration.
2. Select **Email Passwords** from the **Advanced Menu**. The Password Management window appears, and all recipients appear in the window. Passwords are hidden for private recipients.




3. Click on the **Add** pushbutton. The Definition dialog box opens.



4. Type the recipient's name in the space provided.
5. Type a password in the field . Click on **OK** to continue.

To add a private recipient:

1. Login using the *Data Secure! Login Window*.
2. Activate your E-mail application or word processor. Select the text to be encrypted.
3. Activate *E-Mail Lock*, using either of the following methods:
 - Double Click on the *E-Mail Lock* icon  located in the lower right-hand corner of the taskbar, or
 - Press the **Control** and the **Zero** (0) keys simultaneously.

The *E-Mail Lock* window appears.

4. Click on the **E-mail Password Management** pushbutton. The Password Management window opens.
5. Click on the **Add** pushbutton.
6. Type the recipient's name in the space provided.
7. Type a password in the space provided. Click on **OK** to continue. The recipient is added to the list.
8. Complete the encryption normally.

Modifying and Deleting a Recipient

To modify an existing recipient:

1. From the E-mail Password Management window click on the **Modify** pushbutton.
2. Type a new name or password as desired.
3. Click on **OK** to continue.

The System Administrator may only modify global recipients. A user may view and modify only her own private recipients.

To Delete a recipient:

1. From the E-mail Password Management window click on the **Erase** pushbutton.
2. Click on **OK** to confirm.

The System Administrator may delete any global recipient. A user may delete only his own private recipients.

The Decryption Module

A recipient does not need to purchase *Data Secure!* in order to decrypt messages and documents encrypted with *E-Mail Lock*. A freely transferable decryption module is may be download over the Internet.

The decryption module is actually a fully functional demo version of *Data Secure!*. Most features are enabled and work as described in this manual. The only restrictions are that a limited number of folders can be protected, only one user can be defined and the Internet Defender features are not available.

Chapter 8 Using Internet Defender & Virus Protection

Overview

Tools such as Internet Defender & Virus Protection are commonly referred to as a Firewalls.

We refer to those areas to which certain activities are confined as Firewall Areas.

Network Notes:

Internet Defender & Anti-Virus is not designed for network use. Firewall Areas cannot be defined on remote network drives.

Firewall protection is not available when Internet applications are run from a network server.

***Data Secure!** protected folders are protected against access over the network. Viruses cannot infect protected folders.*

Internet Defender & Virus Protection is a collection of privacy and anti-virus tools that protects your system by confining Internet and other activities to special restricted areas called **Firewall Areas**.

Viruses and other computer goblins cannot break out of the firewall areas, nor can they perform file operations (such as create, modify, delete, rename, etc.) on files outside of the firewall areas.

This chapter describes the *Internet Defender & Virus Protection* tools and provides step-by-step instructions for their use and configuration.

Internet Defender & Virus Protection contains three different types of firewalls:

- **Internet Safe Use** areas contain folders from which Internet and/or other on-line applications may be run. Folders into which programs and data files are downloaded should also be designated for **Internet Safe Use**.
- The **DOS Safe Area** contains folders from which DOS based programs may be safely run and where such applications may create files, write data or otherwise manipulate files. DOS Safe areas should be used to decompress and check out DOS downloaded programs.
- The **Windows Safe Area** contains folders from which a Windows installation program may be run and where an application may be installed. The Windows Safe Area is used with the *Data Secure!* Safe Setup feature. Windows Safe areas should be used to decompress and check out downloaded Windows programs and data files.

Hide While Online hides designated folders, which are not otherwise protected by *Data Secure!*, while connected to a remote computer (i.e. during on-line registration or purchasing). **Each of these tools is discussed in a separate section.**

Why You Need *Internet Defender & Virus Protection*

The explosive growth of the Internet and other on-line services has created unprecedented opportunities for hackers and other unscrupulous individuals to invade your private computer space.

Here are just a few examples of today's dangers:

- The obvious. Downloaded programs and files may contain viruses or Trojan Horse programs.
- E-mail may be intercepted and infected with a virus. Some "E-junk mail" is known to be infected.
- Internet news-groups can deliver more than just the news.
- The new Java and ActiveX technologies can do a lot more than draw pretty pictures and help you fill out on-line questionnaires. Hostile applets or controls can copy data from your computer, delete or damage data, or tamper with your database files. All this can happen while you are browsing the Web and are unaware of anything happening.
- Your computer can be spied on without your knowledge and consent during on-line registration, on-line purchasing and the like.



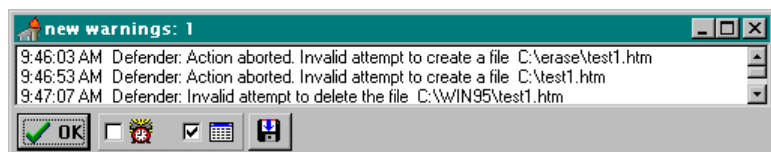
The list goes on and on. The *Internet Defender & Virus Protection* firewalls are designed to protect your computer from these dangers.

How Internet Defender & Virus Protection Works

Internet Defender & Virus Protection works together with *Data Secure!* in the background without user intervention. As mentioned in the introduction, *Internet Defender & Virus Protection* confines Internet and other communication activities to specially designated firewall areas.

Data Secure! protected folders cannot be accessed by Java applets or other snoops, **even while an authorized user is logged in**. The authorized user himself, of course, may freely access these areas using any software not designated for Internet use even while communicating with the Internet.

When a program originating from inside a firewall area attempts to create, delete, write to or modify a file or a folder located outside of that firewall area, an error message appears in the Warning Panel. *Data Secure!* halts the activity.



Internet Defender & Virus Protection does not affect any programs and actions originating from outside of firewall areas. *Data Secure!*, of course, always restricts access to protected folders according to the access rights parameters assigned to a given user.

The **Hide While On-Line** feature, together with *Data Secure!*, effectively keeps outsiders from spying on data in unprotected folders.

The System Administrator uses the *Internet Defender* screen in the *Data Secure!* Configuration utility to define the firewall areas and to designate folders as hidden from view while on-line.

Generally, folders do not belong to any firewall areas unless explicitly assigned by the System Administrator.

Programs run from inside a firewall area cannot access or manipulate files contained in **any** folders that are not explicitly assigned to a firewall area.

Internet Defender & Virus Protection does, however, consider several specific folders as belonging to firewall areas. These folders are only considered as belonging to firewall areas if the System Administrator activates *Internet Defender & Virus Protection* by defining other folders as firewall areas.

Folders automatically considered to be Firewall Areas

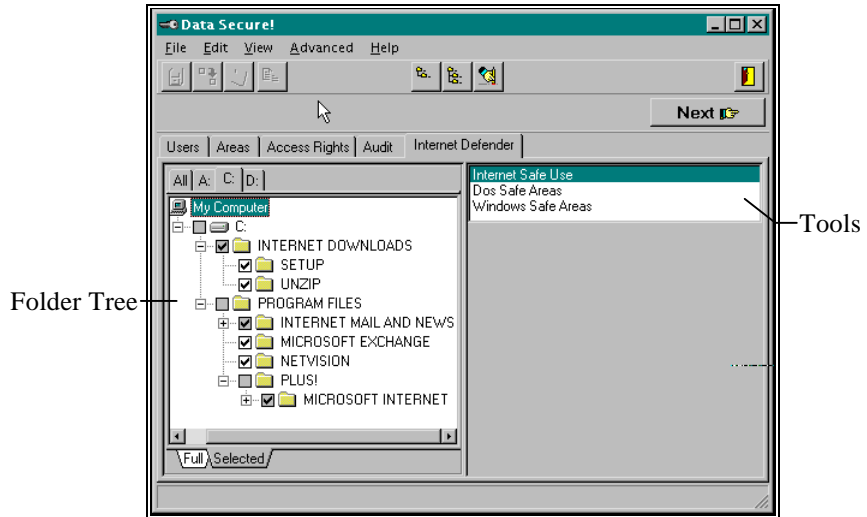
The following sub-folders of the Windows (or Win95) folder are automatically designated as Internet Safe Use areas if at least one other folder is so designated:

- Cookies
- Favorites
- History
- Forms
- Java
- Recent
- Temporary Internet Files
- Spool
- Spool/Fax
- Spool/Printers

In addition, the Recycle\Nprotect folder is considered to belong to all firewall areas if it exists on any drive. This folder is used by the Norton Utilities.

To access the Internet Defender screen:

- Run *Data Secure!* Configuration and click on the *Internet Defender* tab.



The following sections discuss the *Internet Defender & Virus Protection* tools in detail.

Internet Safe Use

You should designate all folders and sub-folders containing Internet and other communication applications as Internet Safe Areas. Some examples of such applications include:

- Internet Web browsers such as Netscape Navigator™, Microsoft Internet Explorer™ or Chameleon™
- Commercial on-line service applications such as Compuserve or America On Line
- Communication software such as Procomm Plus™ or PC Anywhere™

Refer to your application documentation to determine where application files are stored.

In addition, you should designate separate Internet Safe Use folders to receive and work with downloaded files. After downloading, files should be decompressed into Windows Safe Areas or DOS Safe Areas where they may be safely tested for viruses.

To designate folders for Internet Safe Use:

1. Run *Data Secure!* Configuration and click on the **Internet Defender** screen selection tab.
2. Select **Internet Safe Use** from the list on the right-hand side of the screen. It will appear highlighted.
3. Select the folders to be designated from the Folder Tree.
4. Click on the **Next** pushbutton until the Confirmation screen appears. Click on **Finish** to record the selections.

You cannot designate the Windows95™ folder (usually **Windows** or **Win95**), the **System** sub-folder or the **Program Files** folder for Internet Safe Use.

Tips and Suggestions

- If you are using **Microsoft Internet Defender**™ designate the following folders as Internet Safe Use areas:
 - Microsoft Internet and its sub-folders
 - Internet Explorer and its sub-folders
 - Internet Mail & News and its sub-folders

These folders usually reside in the Program Files or Plus! Folders.

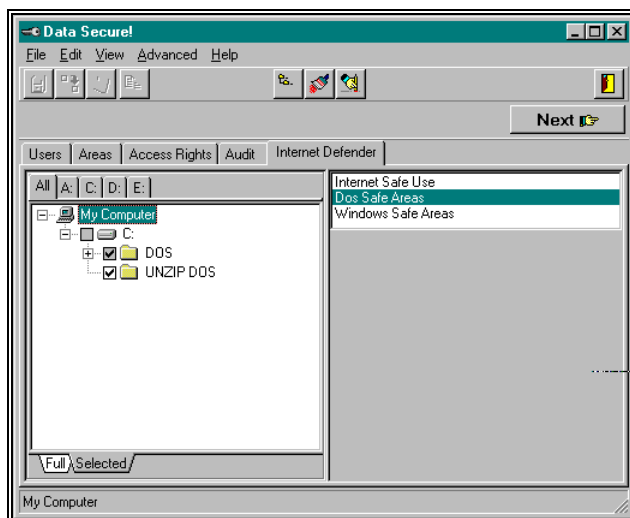
- If you are using **Netscape Navigator**™, designate the Netscape folder and all of its sub-folders as Internet Safe Use areas.
- Be careful not to designate ordinary user applications and utilities as Internet Safe Use areas. This could cause unwanted error messages because many applications write and modify files in a variety of different folders. There is no advantage to protecting ordinary user applications and utilities if they don't communicate with the Internet or on-line services.
- Remember, Internet Safe Use folders are not just for Internet clients. You should designate Internet Safe Use Folders for all on-line and communication applications.
- If you repeatedly receive warning messages in the Warning Panel regarding attempts to write to a folder that you believe to be valid, ask the System Administrator to designate these folders for Internet Safe Use. Many programs normally access or modify files in unanticipated locations.
- To guarantee firewall protection, run the **Microsoft Internet Explorer Mail** application only from within the **Explorer Web Browser**. Do not run it from a shortcut or from the Start Menu.

- To attach a file from a *Data Secure!* protected folder to an E-mail message, you must first copy it to an unprotected folder and from there attach it to the message.

DOS Safe Areas

Even today, many popular games operate in the DOS environment. Other DOS based programs also continue to enjoy widespread use. The DOS Safe Areas firewall provides protection while using DOS programs.

A program run from within a DOS Safe Area can only create, delete, write to or modify files in another DOS Safe Area.



To define DOS Safe Area folders:

1. Run *Data Secure!* Configuration. Click on the **Internet Defender** screen tab.
2. Select **DOS Safe Areas** from the list on the right-hand side of the screen. It will appear highlighted.
3. Select folders from the Folder Tree.
4. Click on the **Next** pushbutton until the Confirmation screen appears. Click on **Finish** to confirm and record the selections.

You cannot designate the root directory of a drive as a DOS Safe Area. However, the CONFIG.SYS and AUTOEXEC.BAT files may be updated by programs from within DOS Safe Areas.

Tips and Suggestions

- Do not edit a batch file residing in any firewall area from a DOS window. Use a Windows 95™ editor to do this.

- Don't designate the folder containing DOS utilities (this is often windows\command or DOS) as a DOS Safe Area. This could cause unexpected error messages.

Window Safe Areas

Windows Safe Areas are used together with the Safe Setup feature to prevent viruses or Trojan Horses downloaded from unsafe locations from spreading outside of firewall areas during installation of Windows™ software.

Safe Setup should be used only by the System Administrator.

The Safe Setup Procedure involves two steps:

1. Define the folder into which you wish to install a program as a **Windows Safe Area**.
2. Install the software using the **Safe Setup** feature to folder designated in step 1.

Defining Windows Safe Areas

Unlike the other Internet Defender & Virus Protection firewalls, you only need to define the destination folder as a Windows Safe Area. You do not need to run the setup program from within a Windows Safe Area. The Safe Setup utility does this for you.

To designate folders as Windows Safe Areas:

1. Run *Data Secure!* Configuration and click on the **Internet Defender** screen selection tab.
2. Select **Windows Safe Areas** from the list on the right-hand side of the screen. It will appear highlighted.
3. Select the folders to be designated as Windows Safe Areas from the tree list.
4. Click on the **Next** pushbutton until the Confirmation screen appears. Click on **Finish** to record the selections.

It is only necessary to designate a single folder level as a Windows Safe Area. Any sub-folders of the designated folder are automatically considered as Windows Safe Areas, including folders created during the installation process.

You cannot designate the Windows 95™ folder (**Windows** or **Win95**) as a Windows Safe Area. This is unnecessary as *Internet Defender & Virus Protection* automatically considers this folder and all of its sub-folders to be Windows Safe Areas.

You cannot designate the **Program Files** folder as a Windows Safe Area. However, you may so designate any of its sub-folders.

Tips and Suggestions

- If the folder **~mssetup.t** appears on your computer, designate it as a Windows Safe Area.
- Create a folder in your root directory called “**Safe Programs**” (or any other name you like). Designate this folder as a Windows Safe Area. Install all your new software in sub-folders of this folder. This way you never have to worry about installing to a non Windows Safe Area folder.

Safe Setup


Safe Setup works with the Windows Safe Area firewall to prevent the spread of viruses or Trojan Horses during the installation of Windows base applications. Safe Setup physically prevents the installation routine from writing to any folder that is not designated as a Windows Safe Area.

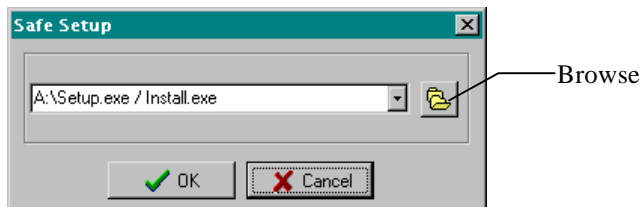
If the installation program attempts to write or alter files in a folder not designated as a Windows Safe Area, an error message will appear indicating the file name and folder to which it attempted to write.

If this occurs and is not suspected of resulting from virus activity, try the following:

1. Write down the folder name to which the installation program attempted to write.
2. Exit the installation program.
3. Using *Data Secure!* Configuration, designate that folder as a Windows Safe Area.
4. Use Safe Setup to run the installation program again. Make sure that you instruct the application’s installation program to install the application to a Windows Safe Area folder.

To start Safe Setup:

1. **Right** click on the red lock icon  located on the right-hand side of the taskbar.
2. Select **Safe Setup** from the shortcut menu. The Safe Setup dialog box appears.



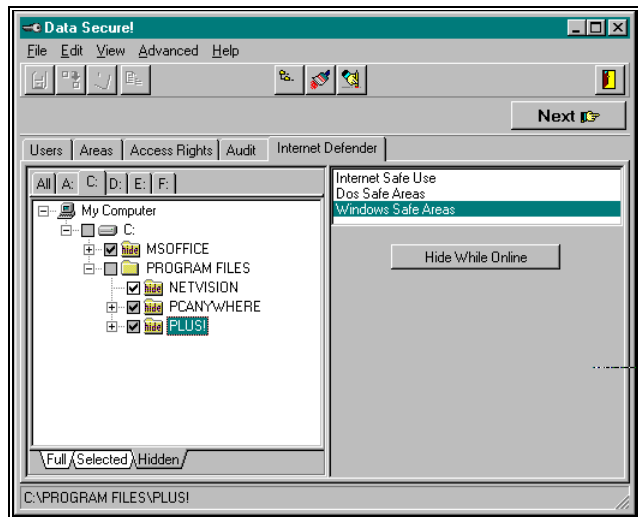
3. Run the installation program using one of the following methods:

- Select from the combo box pull-down list, or
 - Click on the **Browse** pushbutton and use the folder tree, or
 - Type the path in the text box.
4. Click on **OK** to continue. The installation program starts. Follow the instructions on the screen.
 5. Install the application to a **Windows Safe Area** folder. Most applications allow you to choose the destination folder. If you don't do this an error message may appear and the installation will fail.


Hide While On-Line

The connection to a remote computer is a two way street. It is possible that someone on the other end could access your computer while you are connected without your knowledge or consent. It is suspected that some companies scan a user's hard disk during on-line registration looking to gather data on software usage.

The **Hide While On-Line** feature is designed to hide the contents of non-protected folders from view during activities such as on-line registration or on-line ordering. *Data Secure!* protected folders are automatically hidden.



To designate folders as Hidden While On Line:

1. Run *Data Secure!* Configuration and click on the **Internet Defender** screen tab.
2. Select **Windows Safe Areas** from the list on the right-hand side of the screen. It will appear highlighted.
3. Click on the **Hide While Online** pushbutton. The word “hide” appears below the cursor.
4. Select the folders to be designated as hidden from the Tree list.
5. Click once again on the **Hide While Online** pushbutton. The selected folders will be indicated by the symbol .
6. Click on the **Next** pushbutton until the Confirmation screen appears. Click on **Finish** to confirm and record the selections.

The contents of folders selected in this manner are hidden from view during **Safe Install** and while a program launched from a Windows Safe Area is active.

Tips and Suggestions

- Hide the **Favorites** folder. Does anybody need to know what your favorite web pages are?
- Hide the folders containing saved E-Mail and your address books. Keep prying eyes out of your mail.