



Folder Guard Help Contents

Introduction

[Overview](#)
[What's new in this version](#)
[System requirements](#)
[How to install Folder Guard](#)
[This is *Try Before You Buy* software](#)
[Evaluation vs. continued use](#)
[What do you get when you order a license for Folder Guard](#)
[How to order a license for continued use of Folder Guard](#)
[Obtaining updates to Folder Guard](#)
[Our upgrade policy](#)
[Getting customer support](#)
[Uninstalling Folder Guard](#)
[How to access Folder Guard Help](#)
[Acknowledgments](#)

Quick Start Guide

[Step 1. Getting your system ready](#)
[Step 2. Installing Folder Guard](#)
[Step 3. Starting Folder Guard](#)
[Step 4. Assigning attributes to the folder](#)
[Step 5. Setting up the passwords](#)
[Step 6. Building FGD file\(s\)](#)
[Step 7. Enabling the protection at Windows startup](#)
[Step 8. Testing Folder Guard](#)
[What you may wish to do next...](#)
[If anything goes wrong...](#)

Folder Guard Basics

[Running Folder Guard](#)
[Main window](#)
[Attributes](#)
[Protecting files](#)
[Filters](#)
[Passwords](#)
[User List](#)
[Trusted Modules](#)
[Permissions](#)
[FGA files](#)
[FGD files](#)
[Active FGA file](#)
[Working folder](#)

Using Folder Guard

[Model 1: Stand-alone computer, single user account](#)
[Model 2: Stand-alone computer, multiple user accounts](#)

[Model 3: Multiple users on a network](#)
[To protect or not to protect?](#)
[Monitoring the logon](#)
[Using the Filters](#)
[Locking files and folders with passwords](#)
[Giving your computer *bullet-proof* protection](#)
[Using backup and disk utilities](#)

Reference

[Commands](#)
[Shortcuts](#)
[Dialog boxes](#)
[Filter properties](#)
[Files](#)

Appendices

[How Folder Guard initializes system folders](#)
[How FGuard.VxD searches for the FGD file\(s\)](#)
[How FGuard.VxD searches for the licensing information](#)
[How Folder Guard applies the Filters](#)
[How Folder Guard validates user name at logon](#)
[How to create a new user account](#)
[How to delete a user account](#)
[How to backup the Registry](#)
[How to enable the logon prompt on a stand-alone computer](#)
[How to enable user profiles on a stand-alone computer](#)
[How to disable the Default user account](#)
[How to disable Ctrl+Esc during logon](#)
[How to disable Ctrl+C during Windows boot-up](#)
[How to restrict the *Restart in MS-DOS mode* command](#)
[A crash course in System Policies](#)
[MSDOS.SYS: Useful commands](#)

FAQ (Frequently Asked Questions)

[How do I enter the Registration Code?](#)
[Will Folder Guard slow down my computer?](#)
[Will Folder Guard encrypt my files?](#)
[My password is not accepted...](#)
[How do I logon as the *default* user ?](#)
[How do I determine the status of the protection?](#)
[Which modules should or should not be made "trusted"?](#)
[How do I rename a folder in the Folder Guard window?](#)
[How do I hide drive icons?](#)
[How do I prevent formatting of the drives?](#)
[How do I protect folders on the Desktop?](#)
[How do I protect Start Menu?](#)
[How do I protect Control Panel?](#)
[How do I protect the Windows folder?](#)
[How do I protect user profiles?](#)
[How do I protect folders on removable drives?](#)
[Can I hide the *My Computer* folder?](#)
[How can I get printed documentation for Folder Guard?](#)

Troubleshooting hints



Introduction

[Overview](#)

[What's new in this version](#)

[System requirements](#)

[How to install Folder Guard](#)

[This is *Try Before You Buy* software](#)

[Evaluation vs. continued use](#)

[What do you get when you order a license for Folder Guard](#)

[How to order a license for continued use of Folder Guard](#)

[Obtaining updates to Folder Guard](#)

[Our upgrade policy](#)

[Getting customer support](#)

[Uninstalling Folder Guard](#)

[How to access Folder Guard Help](#)

[Acknowledgments](#)



Introduction: Folder Guard Overview

Thank you for choosing Folder Guard for Windows 95/98 !

Folder Guard is a software-only security solution for personal or publicly accessible computers running the Windows 95/98 operating system. Its features include:

- ✓ Complete control over access to files and folders of your choice. You can hide or make read-only any file or folder, so that it will be invisible to all applications including Explorer, MS Office, MS-DOS programs, common dialogs, etc.
- ✓ Optional logon monitoring, which helps protect your Windows files from intruders. A log file can be set up to help you keep track of the use of your computer.
- ✓ Password access to protected files and folders that can be set up, or changed, at any time.
- ✓ Flexible control of user access to many Windows resources, such as the Start Menu, Control Panel, Active Desktop, etc.
- ✓ User-specific access rights to files, folders, and to other Windows resources that you can configure separately for each user of your computer.
- ✓ Preventing some or all users from reformatting local drives of your choice.
- ✓ Protection from both the local and remote access. That is, if your computer is on a network, the access to the protected files and folders is restricted to other network users, even if the files are located on a shared drive.
- ✓ Easy and intuitive user interface that helps you set up the attributes of files and folders you want to protect, and helps you control other settings, as well.
- ✓ Protection that's transparent to both users and applications. While protecting specified folders and other resources, Folder Guard uses only about 40K of RAM.
- ✓ Help screens for each feature of Folder Guard. You can access Help from individual dialog boxes or from the main menu.
- ✓ Designed to operate with or without the use of System Policies, on a stand-alone computer or on a network.

Why do you need Folder Guard to control access to your computer? Doesn't Windows itself allow you to set up restrictions or hide a folder? Well, it does, but in very limited ways. Read on....

Hiding files and folders

When you hide a file or a folder using only Windows, that file will indeed be invisible in an Explorer window. However, anyone using your computer can easily make the file visible again by choosing View - Options in the menu bar of Explorer and selecting the *Show all files* option.

With Folder Guard, when you hide a file or a folder, it actually becomes invisible to all applications. To make the file visible again, you must either enter a valid password or logon as a user who has access to that particular file or folder.

Making files and folders read-only

Suppose you want to make a folder read-only - and all you have is Windows 95/98. You select that folder in an Explorer window, then press Alt+Enter to see the properties of the folder, and check the *Read-only* checkbox on the property page. Okay, what is the result? Windows does not prevent you from creating new files or deleting existing files in this folder. You are still able to modify any or all of the files within the folder. You can create new subfolders or delete existing ones. In other words, you have the same full access to the folder, as before. The only change is that if you rename a read-only folder, Windows prompts you to confirm the command; and if you choose Yes, the folder is renamed.

With Folder Guard, you can truly make a file or a folder *read-only*. The files in such a folder will be available for reading and executing, but all other operations - such as creating new files or subfolders, renaming or deleting the existing ones, modifying the contents of the files - will not be performed.

Preventing users from installing unauthorized programs

You do not want anyone using your computer to install new software without your permission. What are your options if you have Windows 95/98 as it is? None, save for physically removing or preventing access to the floppy and CD-ROM drives. What if you want the users to be able to save their work on floppies or use CD-ROM databases? Well, you can use System Policy Editor to set up the list of allowed applications that would not include Setup.exe or Install.exe, and the users would be (almost) prevented from running these installation programs. But what prevents anyone from renaming Setup.exe to, say, Setup1.exe, and running the renamed file?

With Folder Guard, you can set up a *filter* that would prevent all access to the files named Setup.exe or Install.exe, if they are located on a floppy or a CD-ROM drive, while allowing other files to be accessed without limitations. (Folder Guard comes pre-configured with a filter that does just that.) Users would be prevented from accessing such files in any way, be it running, renaming, deleting them, etc. Yet, your users would be able to continue using the floppy drive to backup their files, as well as using CD-ROM drive to access databases and run allowed applications, etc.

Preventing users from running programs from the floppy disks

Suppose you want your users to be able to use the floppy disks to save/open their document files, but you do not want them to run programs from the floppy disks. With Folder Guard, you can set up a filter that would prevent access to the program files located on the floppy disks while allowing access to other files. (Folder Guard comes pre-configured with such a filter.) This filter would also help you fight software piracy, because it would prevent the users from copying the program files onto the floppies, too!

Monitoring the logon

You can use the built-in capabilities of Windows to setup passwords for multiple users working with your computer. The problem is, however, that unless your computer is connected to a secure network, anyone can logon to Windows as a new user - simply by typing a new user name at the logon prompt. Or an unauthorized user can just press the Cancel button at the logon prompt and start using the computer as the *default* user.

Folder Guard provides a means to validate every user's name before letting him or her log on to Windows. Also, you can optionally disable the *Cancel* button on the Windows logon prompt or set up a separate password for the *default* user. This helps ensure that authorized users are the only ones able to access Windows on your computer.

Permissions

Folder Guard allows you to restrict access not only to folders, but also to some other Windows resources, such as Control Panel, commands of the Start Menu, items on the Desktop, the Run and Shut Down commands, etc. Unlike Policy Editor, Folder Guard does not require the user profiles to be enabled in order for the user-specific permissions to work.

You will find Folder Guard indispensable if you share your computer with others and you don't want any changes made to your files. Or, if you allow your kids to play games on your system from time to time, and want to be sure that everything will be OK when they finish. Or, if you don't want your parents to see some of your files. Or, if you are a network administrator and your users give you a headache messing the files up all the time. However you use Windows, you may have concerns about the security, privacy, or confidentiality of your files. And now you have a single, effective solution - Folder Guard.

CAUTION: Folder Guard is a powerful tool that should be used with care. Please take time reading Folder Guard Help before enabling the protection!

Folder Guard includes an automatic Setup utility, allowing you to painlessly install and uninstall Folder Guard. Extensive context-sensitive Help provides a complete user's guide to Folder Guard.

The way software should be! (TM)

Related topics:

[Folder Guard Help Contents](#)

[What's new in this version](#)

[System requirements](#)

[This is *Try Before You Buy* software](#)

[How to order a license for continued use of Folder Guard](#)



Introduction: What Folder Guard does NOT do

Folder Guard is a powerful, but not an omnipotent, tool. Here are some important limitations you should be aware of before you start using Folder Guard:

- Folder Guard cannot restrict access to the *virtual* folders such as My Computer. Only *real* files and folders - the ones which actually exist on your disk(s) - can be restricted with it. Folder Guard, however, does provide a way to restrict some common *virtual* folders, such as Desktop and Control Panel (see permissions in this Help for more information).
- The protection is not activated if you boot Windows in the *safe* or *command prompt only* mode. You can restrict booting Windows in these modes, though, by modifying the MSDOS.SYS file.
- Folder Guard does not protect information from system tools which directly access the contents of the drives. You can, however, prevent access to such tools by restricting access to them with Folder Guard.
- Folder Guard does not protect network resources, except for the shared folders mapped to drive letters. To protect other resources, use the built-in security features of the network.
- Folder Guard cannot protect your computer from a hammer, fire, or robbery <g>.

Note: Folder Guard helps you protect files and folders from the prying eyes of most Windows users. This protection, however, is not intended to withstand attack by anyone who has sufficient time (that is, unsupervised access to your computer) and expertise.



Introduction: What's new in this version

Version 4.11 (June 4, 1999)

General:

- A self-extracting installation packaging has been implemented.

Bug(s) fixed:

- If a root folder on a drive is protected with a password, it cannot be unlocked.

Version 4.10a (March 25, 1999)

Bug(s) fixed:

- In some situations, the protection cannot be enabled on the Far East versions of Windows 95/98.
- The View menu can disappear from the menu bar of Folder Guard after using the Tools - Enable Protection command.
- If a previous version (before 4.10) of Folder Guard is installed over an existing installation of version 4.10, the setup module of the previous version does not always prompt for the Administrator's password.

Version 4.10 (February 15, 1999)

- Folder Guard now lets you protect individual files within folders.
- Separate passwords may be now set up for each file or folder. This lets you unlock only the password protected items, leaving the rest of the system protected.
- Folder Guard now lets you restrict access to the whole classes of files, according to the file names, folders they are located in, and modules they are accessed by. For more information, see Filters.
- Better protection from the remote access: if you protect a file or a folder on a local drive, and you share the drive on a network, the remote users will not be able to access the restricted object. Be sure to remove the KERNEL32 module from the trusted modules list if you want the protection from the remote access!
- Better protection of information on the network drives: if you restrict access to a folder on a mapped network drive, the user will not be able to access the folder using the UNC path. Be sure to remove the MPREXE module name from the trusted modules list if you protect the network drives!
- You can now make the Windows folder read-only: simply add the REGSVR32 module to the trusted modules list. If you use older, 16-bit applications, you may also need to set up special filters to allow such applications access their appropriate INI files, located in the Windows folder.
- The formatting of the drives can now be restricted.
- More permissions implemented, allowing you control access to various elements of Active Desktop and Internet Explorer 4.0.

- The optional *inverse interpretation* of the Trusted Modules implemented.
- You can now customize the toolbar.
- Several other minor improvements made and features implemented.
- Our upgrade policy has been changed.

Version 4.08f (January 16, 1999)

- An incompatibility problem with software for Kodak Digital Camera DC200/DC210 has been fixed.

Version 4.08e (December 29, 1998)

- Documentation updated.

Version 4.08d (September 20, 1998)

- A new feature for FGKey.exe implemented: the folder access password can now be specified in its command line.

Version 4.08b,c

- Several minor changes to the code made to improve the compatibility with other software.

Version 4.08a (July 16, 1998)

- The Trusted Modules feature now works with the final version of Windows 98.

Version 4.08 (June 7, 1998)

General:

- A new feature implemented: Trusted Modules. It lets you designate some programs (such as the backup utilities, disk scanners and defragmenters, anti-virus scanners, etc.) as the *trusted* ones, that should always have full access to all folders on the computer. So now, for example, you don't have to manually disable the protection every time you want to backup all data on your PC!
- New Logon Monitoring Option added: *No empty user name* and *No empty password*, giving you even more flexibility in protecting your computer from intruders. The logon validation procedure itself is also improved: it now validates all logon prompts that may appear on the screen, not just the first one.
- A new option added: Allow protection on removable drives (such as SCSI or ZIP drives, but **not** floppy or CD-ROM ones).
- A new option added: Compatibility Mode. This option helps reduce the incompatibility problems with other software.
- The "system modal" *Disable Folder Guard* prompt, displayed by the unlicensed version, has been replaced by a regular GUI dialog, not interrupting the operation of other programs.
- The incompatibility problem with ZipMagic98 and PowerDesk98 software by Mijenix Corp. has been fixed.

- The Setup procedure has been updated and simplified.
- The documentation has been updated.

Version 4.07 (February 25, 1998)

General:

- We have changed our business name from ChaoSoft to WinAbility.Com. We regret any inconvenience or confusion this change may cause.
- New commands added: Edit - Copy All Folders, Copy Permissions (in the Edit - Permissions dialog).

Bug(s) fixed:

- FGWARD caused an invalid page fault in module FGWARD.EXE at 0137:0040467d. (When saving changes to FGA files on some systems.)
- An incompatibility problem with the BigBin utility (and, probably, with some other utilities). If you are still experiencing problems when running BigBin, you need to upgrade to its version newer than 1.1.

Version 4.06 (December 9, 1997)

General:

- The logon monitoring feature of Folder Guard can now be used with the *Microsoft Family Logon*.
- A new command line switch, /C, is implemented for the FGKey.exe utility.
- The permission *Include folders in 'Settings' on Start Menu* is renamed to more adequate *Allow Control Panel*. Also, *Include Taskbar in 'Settings' on Start Menu* is renamed to *Allow Taskbar Properties*.

Bug(s) fixed:

- The logon monitoring does not always work the first time after the computer boots up.
- An intermittent access violation in FGKey.exe or Explorer.exe during logoff while the logon monitoring feature is enabled.
- An intermittent access violation in FGuard.exe while saving an FGA file.
- In some situations, pressing the *Skip* button in the *Find Folder* dialog causes invalid folder names to be displayed in the prompt for the new path.

Version 4.05 (October 12, 1997)

- The user profiles are no longer required to be enabled on the computer for the user-specific protection to work. **Important:** if you used a previous version of Folder Guard and employed the *Validate user name at logon* feature, please review the changes to the algorithm of validating the user's names, which has been extended to include not only users for whom separate profiles were created, but also users without profiles. You may need to clean up your System.ini file to prevent unwanted users from using your computer.
- The logon monitoring feature of Folder Guard can now be used during the logon to the primary

network, not only to Windows itself.

- The *Tools -- Enable Protection* command of Folder Guard has been extended to enable the protection for the user currently selected in the User List, not for the user currently logged onto the computer (as it worked before). This lets you test the protection for other users without having to logon under their names.
- A new indicator is added to the title bar of the main window of Folder Guard : *Logged on as <username>*, to indicate the user name which you used to logon to the computer. This indicator comes handy when you are testing the protection for many different users by logging onto the system under their names. It's not shown, however, if you have logged on as the *default* user (e.g. by pressing the Cancel button on the logon prompt).
- The *Autoscan subfolders* option has been eliminated: the corresponding code has been optimized so that there is no longer a need for this option.
- Bug fixed: an intermittent access violation in FGuard.exe or FGuard32.dll while processing network drives on some networks.
- Documentation updated.
- The periodicity of the *Disable Folder Guard* screen, shown during the evaluation period, has been increased, so that the screen is now shown not so often.

Version 4.04 (June 23, 1997)

Feature(s) added:

- The functionality of the Folder Guard shortcut menu is enhanced: if you right-click on the *visibility* icon for a folder in the Folder Guard window, only the part of the context menu that controls the visibility of the folder will be displayed. Similarly, right-clicking on the *access* icon of a folder displays the *access* commands of the shortcut menu. If you right-click on the name label of a folder, the full shortcut menu is shown.
- A list of users has been added to the *Permissions* dialog box, to make you able to set up the permissions for different users without closing and re-opening the dialog box.
- The *Permissions* button has been added to the toolbar.

Bug(s) fixed:

- Running FGuard.exe from a different folder doesn't prompt for the Administrator's password.
- When user profiles are not enabled but the *Logon Validation* option is turned on, then closing Windows causes an application error in the Explorer.
- Invalid page fault in Shell32.dll during setup if Internet Explorer 4.0 is running.
- The protection cannot be disabled if IE4 is running.

Version 4.03 (June 5, 1997)

Feature(s) added:

- The procedure of the logon validation is improved: It does not use a separate logon prompt

anymore. The validation is now performed using the *standard* Windows logon prompt. This not only simplifies the procedure but also solves the compatibility problems with some networks;

- New miscellaneous options added: *Preset system folders* and *Autoscan subfolders*.

Bug(s) fixed:

- User name is not fully validated if the *DontDisplayUserName* Windows option is set by a third party software tool;
- Revoking the *Allow save desktop settings* permission does not have effect;
- Revoking the *Allow addition and deletion of printers* does not prevent from adding printers;
- FGUARD caused an invalid page fault in module FGUARD.EXE at 014f:00406196.;
- The protection is not enabled if no folder has the *visibility* attribute different from its *default* visibility;
- The administrator's password is stored in the local registry instead of the CFG file.

Version 4.02 (February 25, 1997)

Feature(s) added:

- A log file can be now set up to keep track of users working with the computer;
- The time dependencies of the FGA and FGD files are now checked;
- No more than one instance of FGuard.exe can now be running at a time;
- New command added to the File menu: Build All
- More screens added to the Folder Guard Advisor.
- The documentation is updated.

Bug(s) fixed:

- The permissions for the Default User are not saved in the FGA file.
- Incorrect default title of the prompt for the default user's password while validating user name at logon.

Version 4.01 (February 8, 1997)

The first release of Folder Guard for Windows.



Introduction: System requirements

Folder Guard is designed for the Windows 95/98 operating system. It will NOT install or work under Windows NT (you can use the built-in security features of Windows NT instead to control access to the folders). At least 1 MB (one megabyte) of free space on your hard disk is required to install Folder Guard. Folder Guard can be used both on a stand-alone computer and on a network.



Introduction: How to install Folder Guard

If you already have a previous version of Folder Guard running on your computer, we recommend to back it up before installing the upgrade, in order to be able to return to the previous version if you don't like the updated one.

To backup the existing installation of Folder Guard, simply create a folder on your hard disk to keep its files (say, C:\Backup\FGuard) and copy all files from the folder where you have previously installed Folder Guard into the backup folder. Also, make sure you have a copy of your registration information saved or printed out on paper, since it may be erased if you decide to uninstall Folder Guard.

Having saved the existing files, install the updated version over the previous one, as described below in this file. If you decide to return to the previous version, do the following: 1) uninstall the updated version with Control Panel - Add/Remove Programs command; 2) restore the files you have backed up; 3) run Setup.exe to restore the shortcuts; 4) run FGuard.exe to reenale the protection.

To install Folder Guard:

- If you have obtained Folder Guard as a compressed file, uncompress the file into a temporary folder on a hard disk, or on a floppy diskette.
- Open folder containing the uncompressed set of Folder Guard files and double-click on *Setup* or *Setup.exe*

Note: If you have a previous version of Folder Guard already installed on your computer and have set up the administrator's password, you will be prompted for this password to continue the installation. Setup may also prompt you to restart Windows before the installation can be continued.

- The installation program will walk you through the process of setting up Folder Guard. It will prompt you to enter your registration information, and to specify installation options such as the folder where to copy the files.

IMPORTANT: When entering registration information, make sure you enter your name *exactly* as it is spelled on your Registration Acknowledgment. Otherwise, Folder Guard will not accept the registration code. If your name is not shown on the Registration Acknowledgment, you should enter your name *exactly* as you spelled it when placing the order (that is, if you ordered with a credit card, enter your name as it appears on the card, etc.)

NOTE: If you have registered version 4.01-4.08 of Folder Guard, an **updated registration code** is required to register this version. Please see README.TXT file for information on obtaining the updated registration code.

- After you press the Finish button, the installation program will copy the files into the specified folder and configure Windows for using Folder Guard.

Note: Except for the files copied into the destination folder and for the shortcuts added to the Start Menu and Desktop, Setup does not install or modify any other files on your computer.

- After the installation is complete, you may delete these files from the temporary folder (where you ran Setup.exe).

Note: At this point Folder Guard, although installed, in no way affects the operation of your computer. That is, all folders can be freely accessed, as before, and no other restrictions are imposed on the use of the computer. To enable the protection of folders you must run Folder Guard (FGuard.exe) and use

its commands to specify how exactly you want your computer to be protected.



Introduction: This is *Try Before You Buy* software

Folder Guard is NOT *free* or *public domain* software. It is **Try Before You Buy** software. This means that you may use the program during **14 days** (not necessarily constituting a contiguous sequence) to **evaluate** it and determine whether Folder Guard is suitable for your needs. At the end of this trial period, you must either register (**purchase** a license for continued use of the program) or discontinue using Folder Guard.

For corporate customers, wishing to evaluate Folder Guard in the *real-world* conditions, we can provide temporary registration information, upon request, which would suppress the registration reminder screen until a fixed date.

Related topics:

[Evaluation vs. Continued use](#)

[What do you get when you order a license for Folder Guard](#)

[How to order a license for continued use of Folder Guard](#)

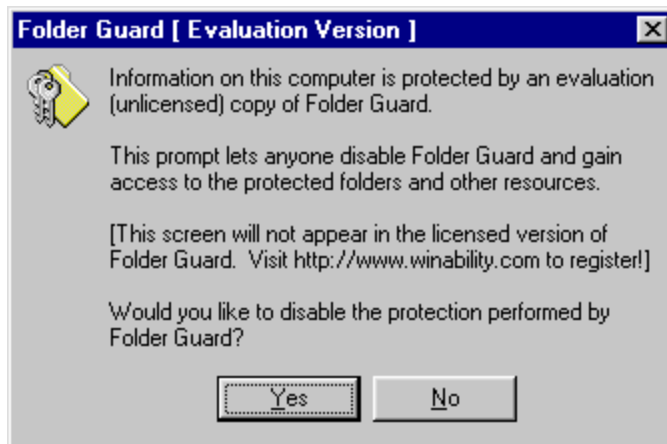
[How to enter your Registration Code](#)



Introduction: Evaluation vs. Continued Use

There is NO functional difference between the evaluation and the licensed versions of Folder Guard: **all features of the licensed version are available and can be used in the evaluation version**. Actually, it's the same program: you may convert an evaluation copy to a registered copy by entering your name and a Registration Code. Similarly, a registered copy of Folder Guard may be *unregistered* by deleting the Registration Code, or just by copying the program to another computer.

The only difference between the licensed and evaluation versions is the prompt to disable Folder Guard, displayed by the evaluation version from time to time:



While you are evaluating Folder Guard, you may reply *No* to this prompt and Folder Guard will continue its normal operation, restricting access to the folders you have chosen to protect. If someone else is using the computer, though, that user may reply *Yes* to this prompt and thus restore access to the protected folders.

To prevent this prompt from being displayed, you must register Folder Guard -- either by supplying a valid Registration Code during the installation procedure, or by entering the Registration Code with the *Help | About* command of Folder Guard.

To obtain a Registration Code, you must purchase a license for continued use of Folder Guard.

Please refer to the file [Purchase.txt](#) for more information.

For corporate customers, wishing to evaluate Folder Guard in the *real-world* conditions, we can provide temporary registration information, upon request, which would suppress the *Disable Folder Guard* screen until a fixed date.

Related topics:

[This is *Try Before You Buy* software](#)

[What do you get when you order a license for Folder Guard](#)

[How to order a license for continued use of Folder Guard](#)

[Our upgrade policy](#)



Introduction: What do you get when you order a license for Folder Guard

1. A Registration Code, allowing you to remove the *Disable Folder Guard* prompt.
2. **FREE** upgrades to the updated versions of Folder Guard released within 1 year after the date of purchase.
3. **FREE** 90-day customer support.

Related topics:

[This is *Try Before You Buy* software](#)

[How to order a license for continued use of Folder Guard](#)

[How to enter your Registration Code](#)

[Our upgrade policy](#)



Introduction: [How to order a license for continued use of Folder Guard](#)

Please refer to the file [Purchase.txt](#) or visit <http://www.winability.com/> for the latest information on ordering our software.

Related topics:

[This is *Try Before You Buy* software](#)

[What do you get when you order a license for Folder Guard](#)

[Our upgrade policy](#)



Introduction: Our upgrade policy

Effective April 1, 1999, we're discontinuing the lifetime free upgrade policy. We will continue to provide lifetime free upgrades, as promised, to all our registered users who purchased their licenses before April 1, 1999.

If you have purchased a license on or after April 1, 1999, you are entitled to free upgrades to all future versions of Folder Guard which we may release within 12 month from the date of the purchase. If you would like to upgrade to a newer version after that period, you will be able to do so after purchasing an upgrade license.

The registration code you receive when you first register Folder Guard may not be valid for one of the next versions. However, we will provide you (upon your request) with updated registration codes within 12 months of your purchase, free of charge.

Please visit our web site <http://www.winability.com/> for the latest information.

Related topics:

[This is *Try Before You Buy* software](#)

[What do you get when you order a license for Folder Guard](#)



Introduction: Obtaining updates to Folder Guard

The latest evaluation versions of all our products can be downloaded from our web site:

<http://www.winability.com/>

An evaluation version may be converted into the licensed version by entering a valid registration code.



Introduction: [Getting customer support](#)

Before requesting customer support, *PLEASE* check out the on-line Help for Folder Guard. In particular, be sure to look through the [Answers to Frequently Asked Questions](#) section.

If you cannot find the information you need in the documentation, then send an email message to:
support@winability.com

In your message, please include information about versions of Windows and Folder Guard you are using and a detailed description of the problem. A reproducible sequence of steps leading to the problem would be of most help. *Please do not send any files at this address unless you have been instructed to do so.*



Introduction: Uninstalling Folder Guard

Note: To completely uninstall Folder Guard, you CANNOT simply delete the program files. Follow the procedure described below to uninstall Folder Guard and clean up your system configuration:

1. Open Control Panel.
2. Double click the *Add/Remove Programs* icon.
3. When the dialog box appears, make sure that the *Install/Uninstall* page is selected.
4. Select the *Folder Guard* line in the list of software that can be uninstalled.
5. Click the Add/Remove button.

Note: If you have set up the Administrator's password, you will be prompted for this password to continue. You may also be prompted to restart Windows before the uninstallation can be continued.

We hope you will change your mind!



Introduction: [How to access Folder Guard Help](#)

You can access Help for Folder Guard in several ways:

- By clicking on the **Start button** in the taskbar and choosing **Folder Guard Help** from the **Folder Guard** submenu of the **Programs** menu.
- By opening the **Folder Guard Help** shortcut from the **Folder Guard** folder on the Desktop.
- By using commands from Help menu while running Folder Guard.
- By opening file FGuard.hlp, located in the folder in which you have installed Folder Guard.
- By clicking on the Help button in any dialog box displayed by Folder Guard.



Introduction: Acknowledgments

I would like to thank Joe Narun for his valuable help in preparing the documentation for this program.

Andrei Belogortseff,
The author of Folder Guard



Quick Start Guide

Step 1. Getting your system ready.
Step 2. Installing Folder Guard.
Step 3. Starting Folder Guard
Step 4. Assigning attributes to the folder
Step 5. Setting up the passwords
Step 6. Saving the changes and building FGD file(s)
Step 7. Setting up the automatic enabling
Step 8. Testing Folder Guard
What you may wish to do next...
If anything goes wrong...

This section is intended to help you get started with Folder Guard. If you don't like reading manuals, or don't want to use all features of Folder Guard, or just want to give Folder Guard a test run, this is a good place to start.

Here you'll find step-by-step instructions on how to use Folder Guard to achieve a simple (and, probably, most common) goal: **preventing unauthorized access to the contents of a specific folder on your computer**. After you have performed the steps described below, a folder of your choice, as well as all files and subfolders contained therein, will be hidden and inaccessible for all users of your computer. Only you will be able to gain access to the folder at any time by entering a valid password.

Throughout this section, a sample folder - one you want to prevent others from accessing - is called C:\A *Private Folder*. If you want to restrict some other folder(s), make appropriate adjustments while following the instructions.



Quick Start Guide: Step 1. Getting your system ready

First of all, a word of **warning**: Folder Guard is a powerful tool and should be used responsibly. Using it thoughtlessly, you can inadvertently make your computer inaccessible. For example, it is very easy with Folder Guard to prevent access to the Desktop folder, and make Windows load with a blank screen after you boot.

Before you begin using Folder Guard, backup the Registry. By the way, it is a good practice to backup the Registry and other important Windows files before installing any new software. The procedure itself takes only a minute or two, but it will save you hours if anything goes wrong. You can backup the Registry before or after you have installed Folder Guard.

Also, **make sure** you can boot Windows in *Safe* mode. Folder Guard is not enabled at Windows startup in *Safe* mode, so you will be able to bypass it and correct any problems.



Quick Start Guide: [Step 2. Installing Folder Guard](#)

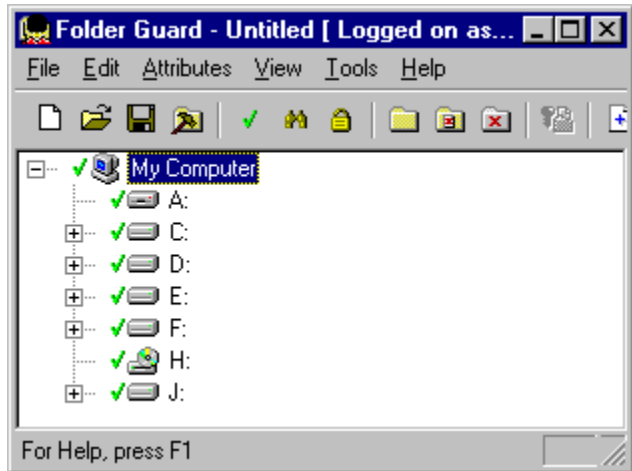
You have probably already installed Folder Guard. If not, [click here](#) for a brief review of the installation process.



Quick Start Guide: **Step 3. Starting Folder Guard**

Now run Folder Guard. You can do this by clicking on the **Start** button in the Windows Taskbar and choosing **Programs => Folder Guard => Folder Guard** in the Start menu. Or, by opening the **Folder Guard** folder created on your Desktop during the installation of Folder Guard, and double-clicking the **Folder Guard** shortcut. One more way to start Folder Guard is to open the folder in which you have installed Folder Guard, and double-click on the FGuard.exe file.

No matter which way you choose, the main window of Folder Guard should appear on your screen:



The window shows the hierarchy of folders on your computer, beginning from *My Computer*. Of course, your computer may have a different combination of drives than the ones shown here.



Quick Start Guide: Step 4. Assigning attributes to the folder

Before Folder Guard can hide or otherwise protect the folder you have chosen, you must let Folder Guard know which folder you want to protect, and how exactly you want Folder Guard to protect it. The way to supply this information to Folder Guard is by specifying the attributes of the folder you want to be protected. First of all, take a look at the toolbar located at the top of the window (right below the menu bar).

The following group of buttons is used to specify how you want a folder to be accessible to the users:



Full access

Makes all files contained in the folder accessible without limitations, as if Folder Guard were not present. Users can open files in this folder, modify them and save them back into the same folder, rename or delete files and subfolders, etc.



Read-only access

Allows opening files in the folder, so that their contents may be viewed, but prevents saving modifications to the files into the same folder. This also prevents creating, deleting, or renaming files or subfolders.



No access

The same restrictions as above, plus prevents opening files even for reading. That is, the contents of the folder can be viewed in an Explorer window (unless you have restricted its visibility, see below), but cannot be accessed or modified in any other way.

The following group of buttons is used to control the visibility of a folder and its contents when users browse your computer with Explorer or other similar application.



Visible

Makes all files and subfolders contained in the folder, as well as the folder itself, to be visible to the user.



Restricted

Leaves the folder itself to be visible in an Explorer window, but hides all files and subfolders contained therein, unless a subfolder is explicitly set to be visible.

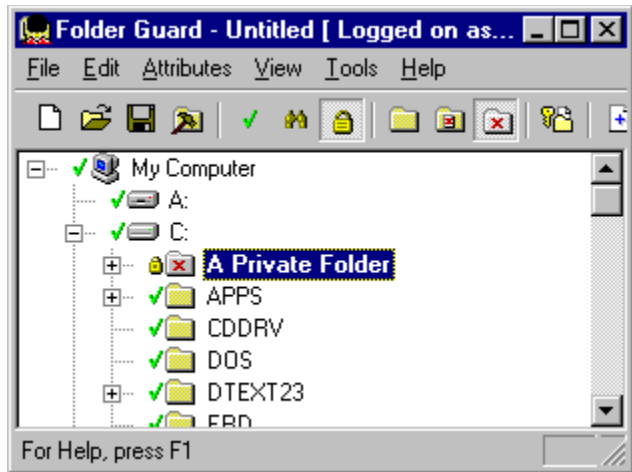


Hidden

Unconditionally hides the folder itself and all files and subfolders it contains.

Now use these buttons to assign the desired attributes to the folder you have chosen to restrict. Keep in mind, however, that at this point no actual protection is taking place. The protection will begin as soon as you enable it, later on. At this point you are only specifying how you would like the folder to be protected.

Use your mouse or arrow keys to highlight *A Private Folder* under drive C:, and click on the buttons **No access** and **Hidden** (each of the buttons will remain depressed after you click them):



That is, you have instructed Folder Guard to prevent all access to the folder, and hide the folder and its contents from browsing. Notice that the icons next to the name of the folder have changed, reflecting the attributes you have just assigned. Notice also that the name of the folder is now shown in a **bold** typeface; this indicates that the folder has non-default attributes assigned to it.



Quick Start Guide: Step 5. Setting up the passwords

Folder Guard uses two main passwords:

Administrator's password

You are prompted for this password whenever you run Folder Guard or its Setup utility. If you fail to set up the Administrator's password, anyone using your computer can run Folder Guard.

Master password

Allows a user to disable the protection at run time by running FGKey.exe, represented by the *Toggle Protection* command on the Start - Programs menu. If this password is not set up, the only way to disable the protection at run time is by running Folder Guard. You will probably want to set up this password to access the protected folder(s) for your own use while the protection is enabled for other users.

The commands to set up the passwords are located under the **File** menu of Folder Guard. Of course, you can use the same word for both of these passwords, if you wish.

Note There are also other passwords maintained by Folder Guard.



Quick Start Guide: Step 6. Saving the changes and building FGD file(s)

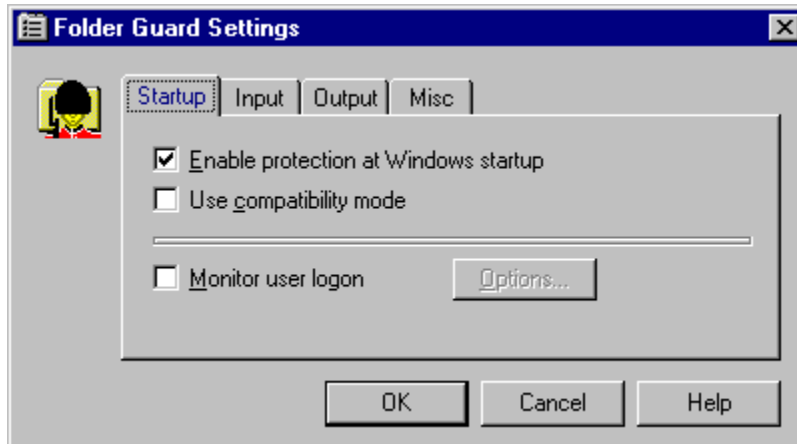
Now, when the attributes of the folder you want to protect and the passwords have been set up, choose the File - Save command from the menu, to save the changes in an FGA file on the disk. When the Save As dialog box appears, enter a name for the file (for example, FGuard.FGA) and press OK.

Folder Guard will save the file and prompt you to activate the file you just have saved. Reply **Yes** to this prompt, and Folder Guard will generate the FGD file(s) necessary for its work.



Quick Start Guide: Step 7. Enabling the protection on Windows startup

Now choose File - Settings in the menu bar of Folder Guard:



Check the **Enable protection at Windows startup** option and press OK. (Do not worry about other options of this dialog box - you will be able to use them later on).

Now everything is set up, and you may exit Folder Guard.

Before closing, Folder Guard will prompt you to confirm that you want the protection of folder(s) to be enabled automatically at Windows startup. Choose **Yes** to continue.

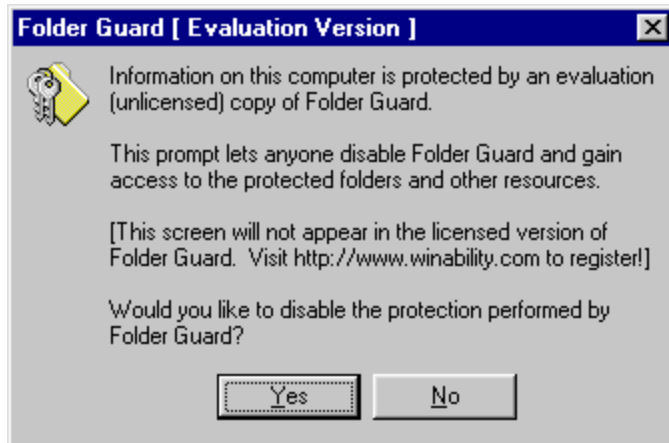
You may also be prompted to enable the protection. You may reply **Yes** to this prompt and Folder Guard will start to protect the folder(s) you have chosen immediately upon its exit. If you reply **No** to this prompt, the protection will be enabled only after you reboot Windows.



Quick Start Guide: Step 8. Testing Folder Guard

If you have enabled the protection (as described in the previous step), Windows loads the Folder Guard driver FGuard.VxD, which reads data from the FGD file(s) and starts to protect folder(s).

The driver also attempts to find the registration information for Folder Guard. If you are still evaluating Folder Guard and have not purchased a license for its continued use, such information does not yet exist. In this situation, Folder Guard may show the following prompt:



You may reply **No** to this prompt and continue the evaluation of Folder Guard in its normal operation, restricting access to the folder(s) you have chosen. If someone else is using the computer, though, that user may reply **Yes** to this prompt and thus restore access to the protected folders.

Attention corporate customers: If you would like to evaluate Folder Guard in the *real* working environment, please let us know and we will provide you with temporary registration information, which will disable this screen until a specific date. Please refer to the file README.TXT or PURCHASE.TXT for information on how to contact us).

To verify that Folder Guard does prevent access to the folder you have chosen, run Windows Explorer and make it display the contents of the C: drive. The folder you have restricted with Folder Guard (*A Private Folder* in our example) should not appear among other folder you may see in the root folder of the C: drive. **Note:** You may need to press F5 while in the Explorer window, to force it refresh the list of files and folders displayed. If, however, you see the protected folder, go back to Step 3 and repeat the procedure.

Now run Notepad (or any other Windows application which uses Common Dialogs to open and save documents) and choose File - Open from its menu. Make the Open dialog box to display the contents of the C: drive; *A Private Folder* should not be visible in the listing either.

Try also to view the contents of the root directory of the C: drive using the MS-DOS prompt window (or run any other MS-DOS program that allows browsing the directories). The folder you have protected with Folder Guard should not appear in the directory listing (unless you have run the program after switching Windows into the MS-DOS mode).

Now, as you have made sure that *A Private Folder* is indeed hidden and inaccessible, try to restore access to it. Click on the **Start** button in the taskbar and choose **Programs => Folder Guard => Toggle Protection** or run FGKey.exe from the folder in which you have installed Folder Guard. You will be prompted to enter the folder access password (which you have set up during Step 5), and, if you have entered it correctly, the protection of the folder will be disabled. Now try to find *A Private Folder* using

Explorer (you may need to press F5 in an Explorer window to refresh its contents), the folder should become visible again, and you should be able to access its contents.

To re-enable the protection of the folder, you do not have to reboot Windows. Click on the **Start** button in the taskbar and choose **Programs => Folder Guard => Toggle Protection** again. After you have replied **Yes** to the prompt to enable the protection, *A Private Folder* should disappear from the folder listing again (you may need to press F5 in an Explorer window again to refresh its contents).

This is how Folder Guard works.



Quick Start Guide: What you may wish to do next...

If you want to set up protection for other folders on your computer, or change attributes of the previously protected folders, you can do so with Folder Guard. You do not have to disable the protection before running Folder Guard: as part of its initialization process, Folder Guard checks the status of the protection, and, if it is enabled at that time, disables it. When you exit Folder Guard, it automatically re-enables the protection.

When setting up attributes of the folders, keep in mind that a folder may have no attributes assigned (that is, have *default* attributes). The visibility and access rights to such a folder are determined by the attributes of its *parent* folder. This means that if you assign the *read-only* access to a folder, all its subfolders with *default* attributes will have *read-only* access, too. Whenever possible, try to reduce the number of folders with *non-default* attributes; doing so will increase the efficiency of work performed by Folder Guard while protecting the folders.

Also please be aware that Windows treats the *My Computer* folder, as well as the drive folders, slightly differently than the *real* folders. If you assign the *hidden* attribute to *My Computer* or to a drive, it will NOT be hidden in an Explorer window. To hide these items, you must use additional means provided by Folder Guard, the permissions, which you can control with the Edit - Permissions command.

If you assign a non-default attribute to a folder, the effect of that attribute is applied to all files located in that folder, as well. For example, if you make a folder *read-only*, all files within this folder will be treated and protected by Folder Guard as *read-only*, too.

There may be situations, however, when you would like some files within the folder to be protected differently than the rest of the files residing in the same folder. Or, you may need to protect only certain files, leaving the rest of them fully accessible.

To accommodate for these possibilities, Folder Guard lets you add files to the list of folders it displays in its main window (with the Edit - Add File command), and assign separate attributes to the files, in the same way as you would do so for the subfolders of the folder. If you assign a non-default attribute to such a file, it will override the appropriate attribute of the *parent* folder (the folder where the file in question is located), and will be used when protecting the files. For the files with default attributes, or for the files not listed in the main window, the attributes of the *parent* folder will be applied.

While working with Folder Guard, you may wish to explore its possibilities by using its context-sensitive Help. In most dialog boxes, press the **Help** button, and a Help screen with information related to the dialog box will open.

With Folder Guard, it is possible to set up different attributes of the files and folders for different users of your computer. To set up the protection for a specific user, select that user's name in the User List. Then use Folder Guard commands to set up the desired visibility and access rights of the files and folders for the selected user. While making the changes, keep in mind that if an object's attributes are set to be *default* for the selected user, the attributes of that object set for the *Default User* will be used instead. The icons displayed next to the names show the resulting attributes of the objects for the selected user. Click here for more information on using Folder Guard in a multi-user environment.

With Folder Guard, you can control access not only to folders, but also to some other Windows resources. You can do this by using the Edit - Permissions command of Folder Guard. The permissions provided by Folder Guard are equivalent to a subset of the system restrictions, which you can set up using the System Policy Editor.



Quick Start Guide: If anything goes wrong...

If you have set up Folder Guard so that the protection is enabled at Windows startup, and Windows fails to boot properly, this means that Folder Guard is incompatible with some hardware or software already installed on your computer.

In such a case, try to boot Windows in the *safe* mode (by pressing F8 while the *Starting Windows 95...* text is shown on the screen or keeping the *Ctrl* key depressed while Windows 98 reboots, and then choosing *safe mode* from the menu). After Windows loads in the *safe* mode, run Folder Guard and turn OFF the *Enable protection at Windows startup* option. This should make Windows bootable again.

Alternatively, boot Windows in the *command prompt only* mode or from a bootable floppy disk. When the command prompt appears, change directory to the folder in which you have installed Folder Guard and rename FGuard.VxD to some other name, for example, FG.VxD. Then try to boot Windows as usually, ignoring the message about a missing FGUARD.VXD driver.

After Windows is ready to use, open the *Add/Remove Programs* icon in the Control Panel, and uninstall Folder Guard.



Folder Guard Basics

The following topics provide the basic information on Folder Guard, and explain the terminology used in this Help. Refer also to the [Quick Start Guide](#), that helps you set up the program and gives you a basic feel for how the program is operated.

[Running Folder Guard](#)

[Main window](#)

[Attributes](#)

[Protecting files](#)

[Filters](#)

[Passwords](#)

[User List](#)

[Trusted Modules](#)

[Permissions](#)

[FGA files](#)

[FGD files](#)

[Active FGA file](#)

[Working folder](#)

Throughout this Help, the term *Folder Guard* has two slightly different meanings, depending on the context in which it is used:

- First, Folder Guard is used to refer to all files and tools included with the software. For example, the phrase *Installing Folder Guard* refers to the entire set of associated files.
- Second, Folder Guard is used to refer to the main application, the FGuard.exe file. This meaning is assumed in phrases like *Running Folder Guard* or *A command of Folder Guard*.

Folder Guard (as a whole set) is used to perform two separate (although related) tasks:

- You, the Administrator of the computer (or a computer site), are using the main application of Folder Guard, FGuard.exe, to specify which folders, files, and other Windows resources should be protected, and how exactly you want them to be protected. We refer to this process as **running Folder Guard**.
- While other users work with the computer, Folder Guard performs the protection of folders and files according to the decisions you made. Help refers to this process as **the protection**.

The following terms are also used:

Players	Description
You	You are the Administrator. You decide how other users may access and view the information stored on your computer. You run Folder Guard to set up the access rights to the files and folders, and enable/disable the protection, when needed.
User	The end user who uses your computer. When the protection is enabled, Folder Guard monitors the user's activity and restricts or allows access to the files and folders according to the attributes you have assigned.
Tools	Description
Explorer	The file management component of Windows, Explorer lets you work with files, folders,

and subfolders -- as well as drives and network connections. Help uses Explorer to refer solely to this particular Windows component, and NOT to the Microsoft Internet Explorer.

- | | |
|------------|---|
| FGuard.exe | Folder Guard, the main application you use to set up the desired protection of information on your computer and control other settings of Folder Guard. |
| FGKey.exe | A utility allowing you (or anyone else who knows the <u>disable protection password</u>) to turn on and off the protection performed by Folder Guard. |
| FGuard.VxD | The virtual device driver that actually performs the protection. |

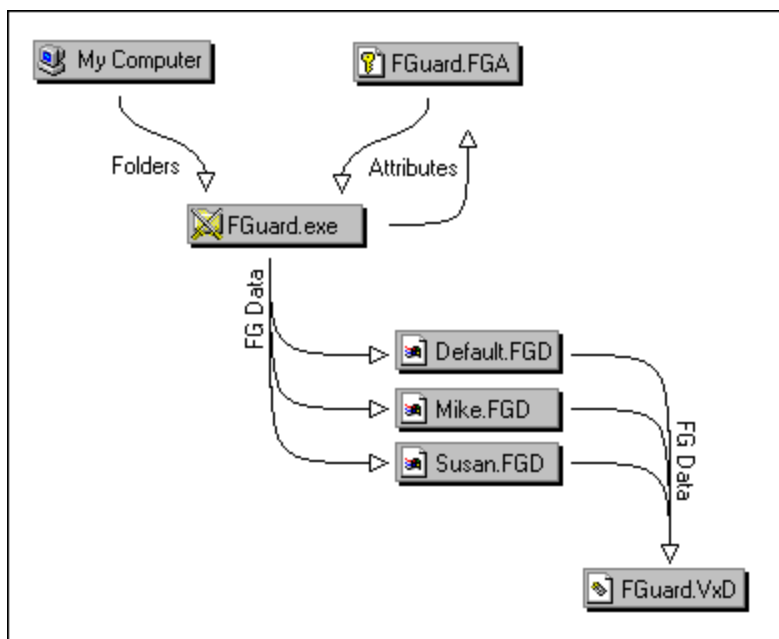


Folder Guard Basics: Running Folder Guard

You can run Folder Guard by choosing the *Folder Guard* item in Windows Start Menu, by opening the *Folder Guard* shortcut in the folder created on the Desktop during the installation of Folder Guard, or directly, by opening file FGuard.exe in the folder where you have installed Folder Guard.

When you run Folder Guard, it analyzes the structure of folders on your computer and displays them in its main window. Using commands of Folder Guard, you can specify how folders can be accessed and/or viewed by the user by assigning appropriate attributes to selected folders.

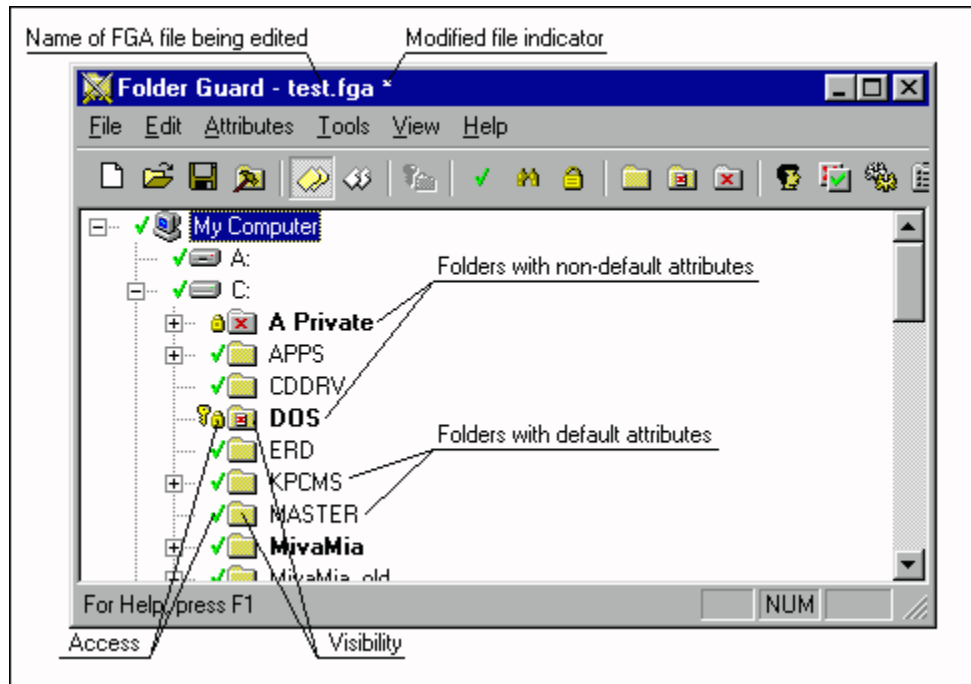
The attributes you assign to the folders and filters are stored in an FGA file. Based on this information, Folder Guard prepares FGD files to be used by its driver, FGuard.VxD, when you enable the protection. The following diagram illustrates the interaction between these components of Folder Guard:





Folder Guard Basics: Main window

When you run Folder Guard, it analyzes the structure of folders on your computer and displays them in its window. The information displayed in the window is presented in the way similar to that of Windows Explorer, in a tree-like form:



When working with Folder Guard, you can see that names of some folders are shown in its window in **bold** typeface. This indicates that such a folder has a non-default attribute assigned to it. Names of folders which have only *default* attributes are displayed in the regular typeface.

The icons shown next to the names of the folders represent their attributes:

Access Attributes:

- ✓ **Full access**
- 🔒 **Read-only access**
- 🔒 **No access**

Visibility Attributes:

- 📁 **Visible**
- 📁 **Restricted**
- 📁 **Hidden**

If you change an attribute of a folder, its icons also change to reflect the new attributes of the folder. Note that while you are assigning the attributes, no actual protection of folders is performed, until you have built the FGD files and have explicitly enabled the protection.

Whenever you use Folder Guard to create a new FGA file, Folder Guard assigns the *default* attributes to all folders, and, unless you have turned off the Preset system folders option, it assigns the *Full access*

and *Visible* attributes to some system folders. [Click here](#) for more information on this procedure.



Folder Guard Basics: Attributes

You probably know that each file or folder on your computer has several attributes maintained by the Windows operating system. These attributes are: Read-only, Archive, Hidden, System. You can see the attributes of any particular file or folder by highlighting the file or folder in question in an Explorer or My Computer window, and then choosing the *Properties* command from the main menu of Explorer.

You can use these standard attributes to make any file or folder read-only, or hidden, to protect certain files or folders from other users. The problem is, however, that any user can easily remove these attributes, and get full access to the files and folders you have protected.

That's where Folder Guard comes into play. It maintains a separate set of attributes which you can assign to files and folders, to protect them from other users. Unlike the standard Windows attributes, the attributes maintained by Folder Guard are stored in a separate file (see [FGA files](#)). Only you, the Administrator, can change these attributes and thus ensure the files and folders are indeed protected the way you want them to be. Other users cannot change these attributes (unless they know the password and know how to use Folder Guard!).

Note: Throughout this documentation, unless otherwise noted, *attributes* refers to the Folder Guard Attributes, not to the standard file/folder attributes maintained by Windows. Folder Guard Attributes are completely independent from the standard attributes, even though some of them have the same names.

The attributes defined by Folder Guard are divided into two groups - the *access* attributes and the *visibility* attributes.

Access Attributes

Attributes	Description
Full Access	Allows full access to the file, or to the files stored in the folder and its subfolders. All operations, such as opening and saving files, renaming or deleting them, modifying their properties, etc., are permitted, as if Folder Guard was not present in the system.
Read-only	Allows the opening the file, or the files in the folder, so that their contents may be viewed, but prevents saving any modifications to the files into the same folder. Also prevents creating, deleting, or renaming files or subfolders.
No Access	Imposes the same restrictions as the read-only attribute, plus prevents the opening of files even for reading. Therefore, when you specify No Access, a user can view the contents of the folder in an Explorer window (unless you have restricted its visibility, see below), but the user cannot access or modify the individual files in any other way.

Visibility Attributes

Attributes	Description
Visible	Makes the file, or all files and subfolders contained in the folder, as well as the folder itself, to be visible in an Explorer window.
Restricted	Leaves the folder itself to be visible in an Explorer window, but hides all files and subfolders contained therein, unless a subfolder is explicitly set to be visible. (This attribute cannot be assigned to a file).
Hidden	Unconditionally hides the file or the folder itself (and all files and subfolders the folder contains).

An object (file or folder) may have *default* attributes. Such an object inherits the attributes from its parent folder. For example, if you assign the Read-only attribute to a folder, this attribute is also applied to all its subfolders which have the *default* access attribute. Likewise, if you make a folder Hidden, all its subfolders with the default visibility attribute will be considered hidden as well, unless you explicitly assign some other visibility attribute to a subfolder. There is one exception to this rule: assigning the *Restricted* attribute to a folder makes all its subfolders Hidden by default. This is consistent with the description of the *Restricted* attribute given above.

You can assign attributes to the files and folders by running Folder Guard and using its Attributes - Access, Attributes - Visibility, and Attributes - Modify commands. You can access these commands via menu bar, Toolbar or Shortcut menu. You may need to use the Edit - Add File command first in order to be able to assign an attribute to a file.

You don't have to assign one or another attribute to every file or folder on your computer. You will probably want most files and folders to have the *default* attributes, and assign some other attributes only to those objects you want to restrict.



Folder Guard Basics: Protecting files

If you assign a non-default attribute to a folder, the effect of that attribute is applied to all files and subfolders of that folder, as well. For example, if you make a folder *read-only*, all files within this folder will be treated and protected by Folder Guard as *read-only*, too.

There may be situations, however, when you would like some files within the folder to be protected differently than the rest of the files residing in the same folder. Or, you may need to protect only certain files, leaving the rest of them fully accessible.

To accommodate for these possibilities, Folder Guard lets you add files to the list of folders it displays in its main window, and assign separate attributes to the files, in the same way as you would do so for the subfolders of the folder. If you assign a non-default attribute to such a file, it will override the appropriate attribute of the *parent* folder (the folder where the file in question is located), and will be used when protecting the files. For the files with default attributes, or for the files not listed in the main window, the attributes of the *parent* folder will be applied.

To add one or more files to the list of folders, use the command Edit - Add File. To assign the attributes to the files, use the commands of the Attributes menu. (Since the Restricted attribute does not make sense for the files, the appropriate command is not available for the files). To remove a file from the list of folders, use the command Edit - Remove File.

See also:

[Filters](#)



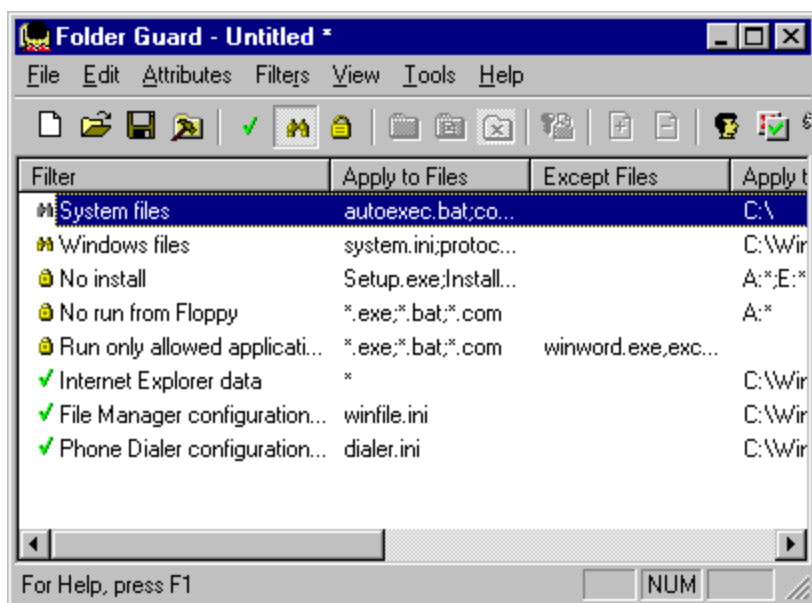
Folder Guard Basics: Filters

Folder Guard lets you control access not only to separate files and/or folders, but also to the whole classes of files. For each class of files you want to control access to, you first need to create a *filter* that defines which files it should be applied to, and then assign appropriate access attributes to the filter (in the same way as you would assign the access attributes to the individual files or folders).

A *filter* is a set of data that defines which files it applies to (according to the names of the files), the folders they are located in, and modules that are accessing the files. You may define several different filters, or have no filters at all, depending on how exactly you want your computer to be protected.

After you have set up the filters and enabled the protection, Folder Guard begins to monitor the events of accessing the files on your computer. Whenever a program attempts to access a file, Folder Guard walks through the list of filters to determine whether the file name, the name of the folder where the file is located, and the module name of the program that is accessing the file match any of the filters. If Folder Guard finds such a filter, it uses its attribute (*full access*, *read-only*, or *no access*) to allow or deny access to the file. If no match is detected, the *access attribute* of the folder where the file is located is used to determine whether to allow or deny the access to the file.

Folder Guard comes with a pre-loaded set of filters, which you can use as they are, or modify them to better suit your needs. To see the currently defined filters, use the command View - Filters. When you choose this command, Folder Guard hides the list of folders, and shows the list of filters instead:



You can create a new filter or modify an existing one by using the commands of the Filters menu. (This menu appears on the menu bar only when the filter list is displayed in the main window of Folder Guard). To return back to the list of folders, use the command View - Folders.

Tip You can switch between the *folder view* and *filter view* of the main window of Folder Guard by pressing any of the following keys: CTRL+TAB, CTRL+SHIFT+TAB.

Note that only the access attributes may be applied to the filters; the visibility of the files defined by the filters is always the same as the visibility of the appropriate folder where the files are located.

See also:

[Filters](#)

[Using the Filters](#)

[Filter properties](#)

[How Folder Guard applies the Filters](#)



Folder Guard Basics: Passwords

Folder Guard uses the following passwords:

Password	Description
<i>Administrator's password</i>	If you set up this password, Folder Guard will prompt you to enter it whenever you run Folder Guard or its Setup utility. You must also enter the old Administrator's password before changing it. If this password is not set up, Folder Guard and its Setup utility can be run by any user. (Command: <u>File - Password - Administrator's</u>)
<i>Master password</i>	If you set up this password, you will need to enter it whenever you want to disable the protection performed by Folder Guard, by running FGKey.exe file or using the <i>Toggle protection</i> command in the Start Menu. If this password is not set up, FGKey.exe does not prompt for it and leaves the protection enabled. Unlike the <i>Item passwords</i> (see below), the Master password all protection performed by Folder Guard, including the file filters and permissions. (Command: <u>File - Password - Master</u>)
<i>Item password</i>	You can assign such a password to any file or folder listed in the Folder Guard main window, to be able to <u>unlock</u> that object only, leaving the rest of the objects protected. Unlike the <i>Master password</i> (see above), the Item password lets you unlock only the object it has been assigned to. (Command: <u>Edit - Item Password</u>)
<i>Default user password</i>	This password is used with <u>Logon Monitoring</u> , to prevent unauthorized users from logging onto the computer as the default user. (Command: <u>File - Settings - Startup - Logon Monitoring Options</u>)

The passwords is stored in the FGuard.FGP file, created in the working folder of Folder Guard.

Note: The length of a password must be between 1 and 64 characters (At least 6 characters is recommended). Any characters are allowed, including spaces and punctuation. The passwords are case sensitive: If, for example, you have chosen the word *Apple* as the password, Folder Guard will not accept the words *APPLE* or *apple* as the valid passwords.

Forgot your password? [Click here for more information.](#)

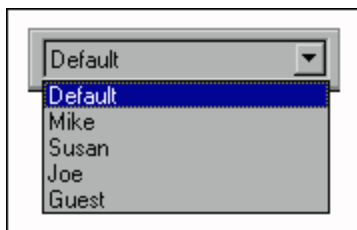


Folder Guard Basics: User List

Folder Guard allows you to specify different attributes of files and folders for different users of your computer. To set up different protection for a specific user, you must first add the user's name to the User List, and then use Folder Guard commands to assign desired attributes and permissions to the files and folders, while that user's name is active (that is, displayed in the User List) .

Tip: You may also wish to enable and create user profiles for each users to let Windows maintain other user-specific settings.

User List is initially not shown in the Folder Guard window; to make it visible, use the View - User List command in the menu bar. The User List initially appears as a separate toolbar, but you can drag it with the mouse to any other place on the screen.



Tip You can switch the input focus between the main window of Folder Guard and User List by pressing any of the following keys: TAB, F6, CTRL+F6.

The User List initially contains a single entry, *Default*, created by Folder Guard automatically whenever you create a new FGA file. This entry is always present in the User List; you cannot delete or rename it. You can use this entry to set up folder attributes and permissions common to all users of your computer.

To add additional entries to the User List, or modify the existing ones, use the Edit - User List command of Folder Guard. To set up the attributes of folders or permissions for a particular user, select this user's name in the User List. Folder Guard will automatically update its window to reflect the attributes of folders as they have been assigned for the selected user.

When specifying the folder attributes for different users, remember the following rule: If you assign the *default* attribute to a folder for a particular user, the attribute of this folder which was assigned for the *Default* user will be used instead. You can take advantage of this feature to simplify your work: First assign the attributes of folders which are common to all users of your computer to the *Default* user, then use other entries in the User List to specify those attributes applicable to each user.

You don't have to add all users of your computer to the User List: If a user logs on to Windows under a name not listed in the User List, the settings specified for the *Default* user will be applied.



Folder Guard Basics: Trusted Modules

Folder Guard maintains a list of *trusted modules*, that is modules that should not be restricted from accessing the protected folders. When performing the protection, Folder Guard intercepts the requests from programs to open files, list the contents of folders, etc. If such a request comes from a module that is designated by you as a *trusted* module, Folder Guard passes the request on to the operating system without any intervention, thus allowing the module to have full access to all folders on your computer. If the name of the module is not in the trusted modules list, Folder Guard allows or denies such request according to the attributes of the folders set up by you.

Originally, the trusted modules list contains the names of several system modules (REGSVR32, MSGSRV32, etc.), that must have full access to all files and folders on your computer in order for Windows to operate properly. You may change the set of the trusted modules by using the Edit - Trusted Modules command.

Note that **only Windows applications** (32 bit or 16 bit) can be designated as the trusted ones. You may add a name of a DOS program or a console application to the trusted modules list, but it will be ignored by Folder Guard.

See also:

Which modules should or should not be made trusted?



Folder Guard Basics: Permissions

Folder Guard allows you to restrict the user's access not only to files and folders, but also to some other Windows resources. You can accomplish it with Folder Guard by assigning desired permissions to the users.

The permissions provided by Folder Guard are divided into the following groups:

General

used to specify the user's access to some common elements of the Windows user interface and tools, such as the Start Menu, Control Panel, etc.

Advanced

used to control the user's access to the elements of Active Desktop and related resources. Note that you must run Windows 98 or have Internet Explorer 4.0 or later (with the shell integration option) installed onto your system in order for these permissions to be usable.

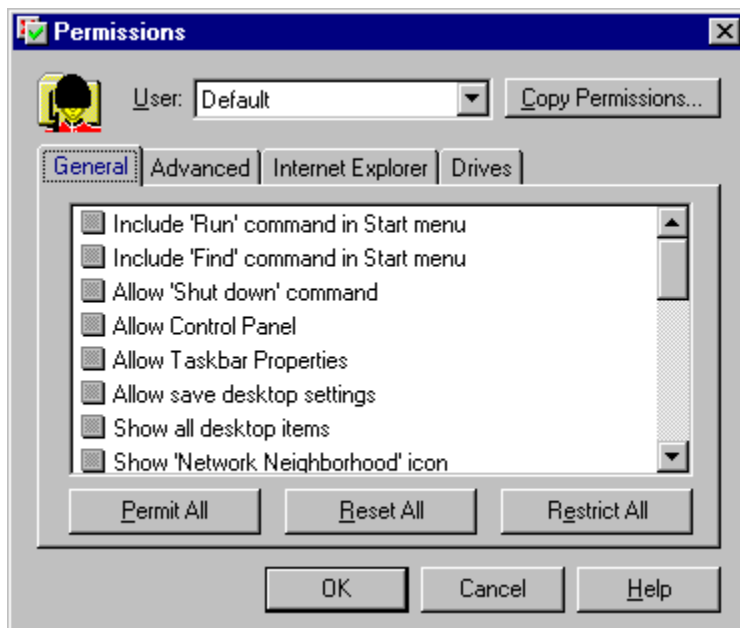
Internet Explorer

used to control the user's access to some functions of Internet Explorer 4.0. Note that you must run Windows 98 or have Internet Explorer 4.0 or later installed onto your system in order for these permissions to be usable.


Drives

used to control the visibility of the drive icons in the shell windows, such as My Computer, as well as the access to the drive formatting commands.



To set up the permissions, use the Edit - Permissions command of Folder Guard.



To set up the permissions for a particular user, first select the user's name in the *User* list.

To allow the user to access a resource, click the box next to the appropriate text in the list of permissions until a check mark appears on the box: . To restrict the user's access to the resource, make the cross

mark appear on the box:

. To prevent Folder Guard from affecting the user's access to the resource (that is, to assign the *default* permission), make the box appear grayed:
.

If you are familiar with System Policies, you will notice the similarity between the permissions provided by Folder Guard and the restrictions provided by System Policies. For example, the permission *Include 'Run' command in Start menu* corresponds to the restriction *Remove Run command*. In fact, Folder Guard permissions represent a most common subset of restrictions available with System Policies.

You don't have to use Folder Guard permissions if you are already using restrictions provided by System Policies. You may find, however, that using Folder Guard permissions is more convenient:

- With Folder Guard permissions, you can hide specific drive icons in My Computer. System Policies allow you only to hide or show all drive icons as a group;
- Folder Guard provides more flexible control over permissions assigned to different users. For instance, if you assign the *default* permission to a resource for a specific user in the User List, the permission assigned to the resource for the *Default* user is applied instead. This is in contrast to the algorithm used by System Policies - if a policy for a specific user exists, the policy for the Default user is ignored altogether.
- If the set of permissions provided by Folder Guard is sufficient for your needs, you don't have to install and configure System Policies. Of course, if you want to set up restrictions to other resources, you must use System Policies.

Note: Although permissions provided by Folder Guard are similar to the restrictions provided by System Policies, the two are completely independent. You may use Folder Guard permissions and System Policies simultaneously on the same computer, if you wish. Remember, however, that non-default Folder Guard permissions take precedence over the corresponding restrictions provided by System Policies. If, for example, you have set up System Policies to remove the *Run* command from the Start Menu, and at the same time set up Folder Guard permission for the same user allowing him or her to have the *Run* command in the Start Menu, then the *Run* command will be included in the Start Menu when this user logs on to Windows.

Note: Some permissions (such as *Show all desktop icons*) take effect only during the logon and therefore the access to the resource cannot be restored by running FGKey.exe.



Folder Guard Basics: FGA files

Folder Guard uses files with extension FGA to store the restrictions you have specified. After you have set up the restrictions, Folder Guard prompts you to save the changes in an FGA file. When you run Folder Guard next time, you can open the file and restore the restrictions.

The information stored in the FGA files includes the attributes you have assigned to the files, folders and filters, the list of users (if any) you have added to the User List, the permissions assigned to each user, as well as other related information.

In most cases it is sufficient to have only one FGA file to store the information, but you may wish to create several such files, containing different data, to be used on different occasions.

To simplify and automate your work, you may find it convenient to assign one of the FGA files (usually the file you use most often) to be the active FGA file.

Note that FGA files are NOT used by Folder Guard while performing the protection. Instead, Folder Guard generates one or more FGD files, which ARE used to perform the protection:





Folder Guard Basics: FGD files

FGD files contain information about the attributes of the files and folders, as well as the permissions for a particular user. Each of these files is prepared by Folder Guard in a format understandable by the Folder Guard driver, FGuard.VxD. In addition to the attributes, an FGD file also contains the following information, needed by FGuard.VxD to efficiently perform the protection:

- For each folder that you have chosen to be protected, both its long file name and the 8.3 alias (MS-DOS name) are stored.
- For root folders of the network drives, the UNC name of the drive is stored as well.
- If your computer contains only one floppy drive, then the attributes you have assigned to the A: drive are duplicated for the B: drive (and vice versa), to prevent users from accessing the floppy drive using an alternative drive letter.

In additions to the FGD files, the FGuard.FGP file is also used while performing the protection (the latter contains the passwords used by Folder Guard).

Folder Guard generates *.FGD and FGuard.FGP files when you use the File - Build or File - Build All command. (The File - Build All command is also executed automatically by Folder Guard when you save the active FGA file).

A separate FGD file is generated for each user listed in the User List, and placed into the working folder. Each FGD file is named for a particular user (that is, the user for which the FGD file was generated), and the FGD extension is appended to the file name. For example, Folder Guard places data for the Default user into the Default.FGD file. Similarly, if the User List contains the name *John*, Folder Guard will place data for this user into the John.FGD file.

Note: While generating an FGD file for a particular user, Folder Guard examines the folder attributes and permissions assigned to this user, and compares these values to those assigned to the Default user. If all such user settings are identical to the settings for the Default user, Folder Guard generates a 0-length FGD file for this user. When performing the protection for such a user, Folder Guard uses the Default.FGD file. This approach enables Folder Guard to operate more efficiently. You cannot alter this default behavior.



Folder Guard Basics: Active FGA file

When you need to make changes to the restrictions set up with Folder Guard, you usually go through the following steps:

- Running Folder Guard (FGuard.exe).
- Opening the FGA file in which you have saved the restrictions last time.
- Making changes to the restrictions.
- Generating the FGD files with the File - Build All command.
- Saving the changes to the FGA file.
- Exiting Folder Guard.

Folder Guard allows you to automate several steps of this cycle by supporting the *Active file* paradigm. If you assign the status of *Active file* to the FGA file you are using (or to one of such files, if you have created several of them), Folder Guard does the following:

- Whenever you run Folder Guard, it automatically opens the active file for you during its initialization. Thus you don't have to remember which FGA file you used last time, and don't have to manually open it.
- Whenever you save the active file, Folder Guard automatically performs the File - Build All command for you, generating the FGD file(s). This keeps the FGD files consistent with the active FGA file.

Now you have a more streamlined way of working with Folder Guard:

- Running Folder Guard (the active FGA file is automatically opened for you at startup).
- Making changes to the restrictions as desired.
- Saving the file (the FGD files are automatically updated as well).
- Exiting Folder Guard.

To set up the active FGA file and control other related settings, use the File - Settings command of Folder Guard.



Folder Guard Basics: Working folder

Working folder is the folder which contains files used by Folder Guard while it is performing the protection. By default, Folder Guard chooses the folder in which it has been installed to be the working folder. You have the option of assigning a different folder for this purpose, if you like, by using the File - Settings command of Folder Guard.

The working folder must contain the following files:

- The FGuard.VxD file.
- The FGuard32.DLL and FGKey.EXE files - if the Monitor user logon option is used.
- All the FGD and FGuard.FGP files generated with the File - Build All command.
- The FGuard.UNM file - if it has been generated by Folder Guard.



Using Folder Guard

The restricting capabilities of Folder Guard can be divided into three groups:

- Restricting access to files and folders.
- Permissions to access some other resources.
- Monitoring the logon process.

The following sections discuss some typical models of using these features of Folder Guard:

Model 1: Stand-alone computer, single user account

Model 2: Stand-alone computer, multiple user accounts

Model 3: Multiple users on a network

The following sections discuss some general issues related to using Folder Guard:

To protect or not to protect?

Monitoring the logon

Using the Filters

Locking files and folders with passwords

Giving your computer *bullet-proof* protection

Using backup and disk utilities



Using Folder Guard: **Model 1: Stand-alone computer, single user account**

This model represents the simplest way of sharing a computer between several users. It can be divided into two slightly different *sub-models*:

a) If you are the primary user of the computer and only occasionally let some other people use the computer for limited time, you will probably want all folders and other resources of the computer to be fully accessible most of the time, for your own use. Only when you let someone else use the computer, you would like to lock some files or folders with sensitive information, and when that person finishes the work, you want to quickly restore access to the protected areas and continue your work as usual.

If this is the case, then you can use Folder Guard to assign the *hidden* and *no access* attributes to the files and folders you want to be hidden from other users, but you don't set it up so that the protection would be enabled at Windows startup. Instead, you are enabling and disabling the protection at will, using the *Toggle Protection* command, added to the Start Menu and/or to the *Folder Guard* folder on the Desktop during the installation.

The advantage of this method of protection is that you have full access to all information stored on your computer, and Folder Guard does not appear in the way, as if it were not present at all. You only need to remember to turn the protection ON before letting someone else use the computer, to hide the areas with sensitive information.

The main disadvantage of this method is that protection enabled with the *Toggle Protection* command lasts only until the computer reboots. So, if you are not supervising the work of others with your computer, they may simply reboot the computer to gain full access to your system.

b) If your computer is likely to be used by someone else in your absence, you need to set up Folder Guard so that the protection would be enabled at Windows startup. This adds a bit of hassle to your everyday work: you must explicitly unlock the protected areas with the *Toggle Protection* command in order to access the files stored therein. However, this method ensures that other users will have no access to the protected folders (unless you tell them the folder access password).



Using Folder Guard: Model 2: Stand-alone computer, multiple user accounts

If several users use the same computer on a regular basis, you will probably want to set up separate user accounts, so that each user would have to enter his or her login name and password in order to start using the computer.

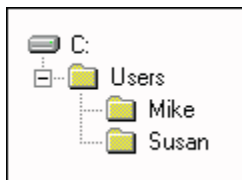
Creating multiple user accounts lets you use Folder Guard to set up different access rights to folders and other resources for different users. For example, you will probably want to set up no restrictions for yourself, but restrict access to your personal folders for the rest of the users. After you have set up separate user accounts, you no longer need to remember to use the *Toggle Protection* command to turn the protection on and off - Folder Guard enables and disables the restrictions automatically, based on the name of the user who has logged onto the computer.

Another advantage of creating multiple user accounts is that you can use Folder Guard to validate user's name at logon, and thus ensure that only authorized users (that is, only users for whom you have created user accounts) will be able to use Windows.

Before starting to create the user accounts, you may wish to enable the user profiles. Although Folder Guard itself does not depend on this feature, user profiles are useful if you want each user to have a personal Desktop, Start Menu, etc., independent on other users. That is, if you create a separate profile for a user, that user may customize his or her working environment not influencing the environments of other users.

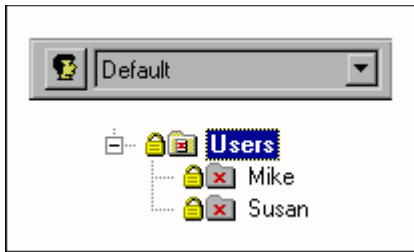
The disadvantage of the user profiles is that they require additional efforts to maintain them from your side. For example, if you install a new software after the profiles have been created, that software may not become enabled automatically for other users, and you may need, for instance, copy the Start Menu items created for your account to the accounts of other users, etc.

You will probably want to assign separate folders for each of the users, in which they would keep their personal files. For example, if your computer is to be used by two users, Mike and Susan, you may wish to create the following folders:



Now, you will probably want Mike and Susan each to have full access to the files in their own folders (C:\Users\Mike for Mike and C:\Users\Susan for Susan). But you also probably want Mike and Susan each to have no access to folders assigned to any other user. You can do this by running Folder Guard and assigning appropriate attributes to the folders:

- First select the root folder common to all users (C:\Users in our example), select the *Default* user in the User List, and assign the *No access* and *Restricted* attributes to the folder:



- Now select *Mike* in the user list, select the folder you have assigned to Mike (C:\Users\Mike), and set the *Full access* and *Visible* attributes for this folder:



- Repeat the above step for Susan, assigning the *Full access* and *Visible* attributes to her private folder:



Now, after you build the FGD files and enable the protection, Mike and Susan will have access only to his or her private subfolder of the C:\Users folder; neither will be able to see or modify files in the subfolders assigned to other users.

IMPORTANT: If you want Folder Guard to perform the protection differently for different users, you should enable the *Monitor user logon* option. If for some reason you don't want this option to be used, then you must enable the *Compatibility mode* option. At least one of these options must be selected, otherwise Folder Guard may not be able to distinguish the users correctly!

See also:

[How do I protect user profiles?](#)



Using Folder Guard: **Model 3: Multiple users on a network**

When using Folder Guard on a network, we recommended that you use the built-in security features of the network, wherever possible, to manage the user accounts and restrict access to the resources. For example, if your network provides for the user validation before letting him or her logon to system, you should use this feature instead of a similar feature of Folder Guard.

Other than that, using Folder Guard on a network is about the same as on a stand-alone computer with multiple user accounts.

Note that if you restrict access to files or folders, they will be restricted to all network users even if they (files and folders) are located on the *shared* drives. Thus Folder Guard provides an extra level of protection of your information, in addition to the standard protection offered by Windows networking.

Note also that if you want to restrict access to the files and/or folders located on a network drive, you should map such a network drive to a local drive letter, and then use Folder Guard to setup the desired access rights to the files and folders located on the drive.

IMPORTANT: If you want Folder Guard to perform the protection differently for different users, you should enable the *Monitor user logon* option. If for some reason you don't want this option to be used, then you must enable the *Compatibility mode* option. At least one of these options must be selected, otherwise Folder Guard may not be able to distinguish the users correctly!



Using Folder Guard: To protect or not to protect?

When deciding which folders you want Folder Guard to protect, consider the following issues:

- The folder in which Windows is installed (usually C:\Windows) must NOT be restricted with the *no access* or *hidden* attributes. [Click here](#) for more information on restricting this folder.
- Most subfolders of the folder in which Windows is installed (usually C:\Windows) must have their access attribute set no higher than *read-only*. You can try assigning *no access* and *hidden* attributes to such folders, but first make sure you have [backed up the Registry](#).
- Many Windows applications on your computer are installed into subfolders of the Program Files folder (usually C:\Program Files). If you restrict access to this folder, the applications installed in its subfolders may become inaccessible.
- You can assign the *no access* and *hidden* attributes to the [working folder](#) of Folder Guard. However, if you want to be able to disable the protection of your system with FGKey.exe, make the working folder *read-only* and *restricted*.
- If you assign the *restricted* attribute alone to a folder, it does not make the folder inaccessible. The contents of such a folder will be invisible for Explorer, but the user will still be able to access files in the folder by other means, such as shortcuts. To make the contents of a folder inaccessible, use the *no access* attribute as well.



Using Folder Guard: **Monitoring user logon**

If you have enabled the logon prompt on a stand-alone computer, Windows verifies the user's password before letting that user begin a Windows session. This feature, however, does not make your computer secure:

- Any user can type a new name in the logon prompt. Windows will simply allow this user to logon under the new name.
- Any user can press the Cancel button in the logon prompt (or press the Escape key). Windows permits this user to logon as the *default* user - without requiring a password.

Even if the computer is connected to a secure network, it is sometimes possible to bypass the network logon procedure and start using the computer in a stand-alone mode, without logging on to the network.

With Folder Guard, you can overcome these shortcomings of Windows by monitoring user logon at Windows startup. You can set up Folder Guard to validate the name entered by the user in the Windows logon prompt, and thus prevent from logging on under a new name. You can disable the Cancel button on the Windows logon prompt or set up a logon password for the default user. You can also customize the texts of the messages displayed by Folder Guard, while monitoring the logon.

Note: In order for a user name to be considered valid by Folder Guard, this user must have logged onto the computer at least once, before you enable the *Monitor user logon* option. [Click here](#) for information on how to add a new user to the list of *valid* users after you have enabled Folder Guard.

Note: If the computer is connected to a network, we recommend using the built-in security features of the network, if any, to prevent the unauthorized use of the computer, instead of the logon monitoring provided by Folder Guard.



Using Folder Guard: Using the Filters

The filters offered by Folder Guard is a powerful means to control access to the files on your computer. To see the list of existing filters, use the command View - Filters . To change the filters, use the commands on the Filters menu.


Folder Guard comes with several pre-configured filters discussed below. You can use them as they are, modify them to better suit your needs, delete them or create new ones. If you don't want the filters to be used, you can reset their attributes with the Attributes - Reset command.

Example 1: System files.

This is a very simple filter that is designed to restrict access to the files AUTOEXEC.BAT and CONFIG.SYS, located in the root folder of the drive C:

Apply to files:	Except for files:
autoexec.bat;config.sys	
Apply to folders:	Except for folders:
C:\	
Apply to modules:	Except for modules:

If you don't want your users to modify these files (directly, or by installing other programs that may modify these files), assign the *read-only* (or *no access*) attribute to this filter:

Filter	Apply to Files	Except Files	Apply to Folders	Except Folders
 System files	autoexec.bat;co...		C:\	

If you want only some of your users to be restricted from modifying these files, select each user's name in the User List and apply the *read-only* attribute to this filter for each such user, one user at a time.

Note that if you want to restrict access to particular files (as in this case), you could also do so by adding the files in question to the folder list of Folder Guard (using the Edit - Add File command) and assigning appropriate attributes to such files.

Example 2: No Install.

Suppose you don't want other users to install any new software on your computer without your permission (assuming that users have access to the floppy disk drive (A:) and to the CD-ROM drive (E:)). One solution could be to assign the *no access* attribute to the root folders of the A: and E: drives with Folder Guard, however this would also prevent the users from saving their work on the floppies, and from using any CD-ROMs.

This is a typical situation where filters provided by Folder Guard offer a more effective solution. Since installing new software usually involves running the *Setup.exe* or *Install.exe* program (and using the *autorun.inf* files from CD-ROMs), you want to prevent users from running such programs while allowing them access other files on the floppy and CD-ROM drives.

To achieve this result, consider the **No Install** filter with the following properties:

Apply to files:	Except for files:
Setup.exe;Install.exe;	

autorun.inf

Apply to folders:


A:.*;E:.*

Except for folders:

Apply to modules:

Except for modules:

This filter would be applied only to the files named Setup.exe, Install.exe, or autorun.inf, and only if they are located on the A: or E: drives (in the root folders or any of the subfolders). Now assign the *no access* attribute to this filter for all users whose assess to these files you want to be restricted (by selecting user's name in the [User List](#) and applying the [Attributes - Access - No access](#) command). The *lock* icon will appear in front of the filter in the Folder Guard window, indicating the *no access* attribute:

Filter	Apply to Files	Except Files	Apply to Folders	Except Folders
 No install	Setup.exe;Install...		A:.*;E:.*	

If you want yourself to be able to run Setup.exe and Install.exe, assign the *full access* attribute to this filter while your user name is selected in the [User List](#).

Example 3: No run from floppy.

Suppose you don't want other users to run programs from floppy drive. Yet, you would like them to be able to open and save their documents on the floppy disks.

To achive this result, consider the **No run from floppy** filter with the following properties:

Apply to files:

.exe;.bat;*.com

Except for files:

Apply to folders:

A:.*

Except for folders:

Apply to modules:

Except for modules:

This filter would be applied only to the program files (since their file names have the extensions *exe*, *com*, and *bat*), and only if they are located on the A: drive (in the root folder or any of its the subfolders). Now assign the *no access* attribute to this filter for all users whose assess to these files you want to be restricted (by selecting user's name in the [User List](#) and applying the [Attributes - Access - No access](#) command). If you want yourself to be able to run programs from the floppy disks, assign the *full access* attribute to this filter while your user name is selected in the [User List](#).

Note that this filter will also prevent copying program files onto the floppy disks (and thus help us all fight software piracy!).

Example 4: Run only allowed applications.

Suppose you don't want other users to run any programs other than MS Word and Excel. Consider the following filter:

Apply to files:

.exe;.bat;*.com

Except for files:

winword.exe, excel.exe

Apply to folders:

Except for folders:

C:\Windows*;
"C:\Program Files\WinAbility\Folder Guard"

Apply to modules:

Except for modules:

This filter would be applied to all program files (that is the files with extensions *exe*, *bat*, and *com*), but not to the files *winword.exe* (MS Word) and *excel.exe* (MS Excel). Also, this filter would not apply to the files located in the folders that begin with C:\Windows (since these folders contain system files such as *kernel.exe*, that should be accessible in order for Windows to work properly). The programs located in the folder "C:\Program Files\WinAbility\Folder Guard" would also be exempt from this filter, since you want to be able to run Folder Guard files to change or disable the protection as needed.

Now, if you assign the *no access* attribute to this filter for a particular user, that user would not be able to run any programs other than MS Word and Excel, and the programs located in the Windows folder, or its subfolders.

Example 5: Internet Explorer data.

Suppose you want your users to be able to use Internet Explorer (IE), however you want to prevent them from accessing or deleting the files IE uses during its operation. Since IE is usually installed in folder "C:\Program Files\Internet Explorer", you can protect part of its files by assigning the *read-only* attribute to this folder. However, IE also stores its data into the folders "C:\Windows\Cookies" and "C:\Windows\Temporary Internet Files", what about them? If you make these folders *read-only*, this may cause IE to fail, since it expects these folders to be fully accessible.

The solution is to make these data folders *read-only*, and also set up a filter that would grant IE full access rights to the files in these folders:

Apply to files:

*

Except for files:

Apply to folders:

C:\Windows\Cookies,
"C:\Windows\Temporary Internet Files"

Except for folders:

Apply to modules:

iexplore

Except for modules:

If you assign the *full access* attribute to this filter, then Folder Guard would allow full access to all files located in the IE data folders, if they are accessed by the IE module, iexplore. If the files are accessed by other programs, the filter would not be applied, and the *read-only* attributes of the IE data folders would be used instead.

See also:

[Dialog boxes: Properties for the Filter](#)

[Filter properties](#)

[How Folder Guard applies the Filters](#)



Using Folder Guard: Locking files and folders with passwords

If you would like to be able to lock/unlock a particular file or folder with a password while it's protected by Folder Guard, first you should use Folder Guard to set up the protection for the file or folder in question, as needed (that is, assign the *read-only* or *no access* attribute to it, as desired. However, do not make the object *hidden*, because if it is invisible, you cannot unlock it!) If it's a file or a shortcut, you may need to add it to the list of folders with the Edit -Add File command of Folder Guard.

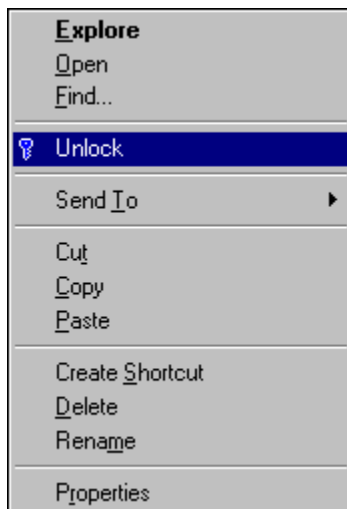
Having assigned the desired attribute, assign also a password to this object with the Edit -Item Password command. After you do so, a small *key* icon appears next to the object, indicating that there is a password assigned to it:



(If you decide to remove the password from this object later on, you can do so by using the Edit -Item Password command and entering an empty password. The *key* icon will disappear if you do so.)

Finally, use the File - Settings command to open the Settings dialog, select the Misc page, and make sure that the *Add lock/unlock commands to the Windows shortcut menu* option is checked.

Now, whenever the protection is enabled, Folder Guard will restrict access to this file or folder, as usual. If you want to unlock the object with the password, leaving the rest of the protection in effect, click the object with the right mouse button. The Windows shortcut menu should appear on the screen, and there should be the *Unlock* command on it:



(If the *Unlock* command is not present, it is because: 1) the protection is not in effect, or 2) the item has not been assigned the *item password*, or 3) the *Add lock/unlock commands to the Windows shortcut menu* option is not set. See above for more information).

If you choose the *Unlock* command, Folder Guard prompts you for the password and, if you have entered it correctly, removes the protection from this file or from folder and all its subfolders. The other files and folders remain protected. Note that you may need to refresh the list of files shown in an Explorer window (by pressing F5) in order to be able to see the unlocked object.

Now, if you want to lock the object back, right-click on it with the mouse and select the *Lock* command

from the shortcut menu.

An alternative way to lock/unlock files or folders is by using the FGKey.exe file with appropriate command line switches. For example, the command

```
FGKey.exe /D /P:"C:\A Private"
```

unlocks the folder C:\A Private, whereas the command

```
FGKey.exe /E /P:"C:\A Private"
```

locks it back. For more information, refer to the description of the [FGKey.exe](#) file.

Note that you can also use the *Toggle protection* command (installed on the *Start - Programs* menu) to enable/disable protection of all files and folders at once. In such a case, Folder Guard prompts you to enter the Master password.



Using Folder Guard: **Giving your computer *bullet-proof* protection**

The following recommendations will help you prevent others from bypassing the protection of folders performed by Folder Guard:

- **Restricting access to Registry editing tools.** A user can disable the protection by editing the Registry and then rebooting Windows. You can deny users access to the Registry Editor by using permissions provided by Folder Guard or by setting up appropriate restrictions with the System Policy Editor. Keep in mind, however, that you will similarly need to restrict access to the Registry editing components of third-party utilities on your computer (if any).
- **Restricting access to the working folder of Folder Guard.** While setting up folder attributes with Folder Guard, assign the *read-only* attribute to the working folder of Folder Guard. This will prevent other users from deleting or modifying Folder Guard files.
- **Preventing users from running MS-DOS programs in the MS-DOS mode.** You can achieve this by setting up the appropriate permissions provided by Folder Guard or by using the Windows System Policies.
- **Preventing users from booting Windows in the *safe mode* or *command prompt only*.** Because the protection is not enabled at Windows startup in either of these cases, it is important to restrict a user's ability to boot Windows in any of these modes. You can force Windows to boot in the GUI mode only by modifying the MSDOS.SYS file, located in the root folder of the boot drive. Be sure to have a text editor on a bootable floppy disk, so that you will be able to modify this file and boot Windows in the *safe mode* or *command prompt only*, if needed.
- **Preventing access to Task Manager during logon to Windows.** [Click here](#) for more information.
- **Preventing canceling Windows boot-up with Ctrl+C.** [Click here](#) for more information.
- **Preventing access to the Windows folder.** This folder is probably the most vulnerable one, from the system integrity point of view. Yet, this folder is the most tricky to protect, since many programs (including Windows itself) require full access to its contents. [Click here](#) for more information on restricting this folder.
- **Preventing modifications to the system files in the root folder on the boot drive (usually C:\).** Mark this folder *read-only*, otherwise a user can modify the AUTOEXEC.BAT and other important files.

Note: Folder Guard helps you protect files and folders from the prying eyes of most Windows users. This protection, however, is not intended to withstand attack by anyone who has sufficient time (that is, unsupervised access to your computer) and expertise.



Using Folder Guard: Using backup and disk utilities

The protection of folders performed by Folder Guard may confuse some of the system utilities, such as backup or disk managing software. For example, if your backup software allows you to specify which folders to backup, and you leave the protection in effect during the backup, the folders you've made invisible or restricted with Folder Guard may not be backed up. On the other hand, if the backup software stores a complete image of the disk disregarding its folder structure, it may be safe to leave the protection on, since Folder Guard does not prevent the direct access to the disk sectors.

To avoid such problems, you should add the module names of such utilities to the trusted modules list. (Folder Guard allows the trusted modules to have full access to all folders.) The best way to do so is by running the software in question while Folder Guard is running, and then selecting the module name of the program using the *Add: Task* button on the Trusted Modules dialog box.



Reference

Commands

Shortcuts

Dialog boxes

Filter properties

Files



Reference: [Commands](#)

File menu

Edit menu

Attributes menu

Filters menu

View menu

Tools menu

Help menu



Reference: Commands: File menu

The File menu offers the following commands:

New

Creates a new FGA file.

Open

Opens an existing FGA file.

Save

Saves an opened FGA file using the same file name.

Save As

Saves an opened FGA file to a specified file name.

Build

Builds *.FGD file(s) for all or a specific user in the User List.

Build All

Builds *.FGD file(s) for all users in the User List.

Settings

Opens the Folder Guard Settings dialog box.

Password

Allows to set up the passwords used by Folder Guard.

Exit

Exits Folder Guard.



Reference: Commands: File menu: New

Use this command to create a new FGA file in Folder Guard.

You can open an existing FGA file with the Open command.

Shortcuts

Toolbar:



Keys: CTRL+N



Reference: Commands: File menu: Open

Use this command to open an existing FGA file in Folder Guard.

You can create new menu files with the New command.

Shortcuts

Toolbar:



Keys: CTRL+O



Reference: Commands: File menu: Save

Use this command to save an FGA file you are editing to its current name. When you save a file for the first time, Folder Guard displays the **Save As** dialog box so you can name your file. If you want to change the name and location of an existing file before you save it, choose the Save As command.

Shortcuts

Toolbar:



Keys: CTRL+S



Reference: Commands: File menu: Save As

Use this command to save and name the FGA file you are editing. Folder Guard displays the **Save As** dialog box so you can name the file.

To save a file with its existing name, use the Save command.



Reference: Commands: File menu: Build

Use this command to generate the FGD file(s) for all users or for a specific user in the User List. When you choose this command, Folder Guard displays the Build dialog box.

Shortcuts

Toolbar:



Keys: CTRL+B



Reference: Commands: File menu: Build All

Use this command to generate the FGD file(s) for all users in the User List.

Shortcuts

Keys: CTRL+D



Reference: Commands: File menu: Settings

Use these commands to change settings for Folder Guard. When you choose this command, Folder Guard displays the Folder Guard Settings dialog box.

Shortcuts

Toolbar:



Keys: CTRL+E



Reference: Commands: File menu: Password

Use these commands to set up the Administrator's and Master passwords used by Folder Guard.



Reference: Commands: File menu: 1, 2, 3, 4 command

Use the numbers and filenames listed at the bottom of the File menu to open the last four FGA files you closed. Choose the number that corresponds with the FGA file you want to open.



Reference: Commands: File menu: Exit

Use this command to end your Folder Guard session. You can also use the Close command on the application Control menu. Folder Guard prompts you to save the FGA file, if necessary.

Shortcuts

Mouse:	Double-click the application's Control menu button.
Keys:	ALT+F4



Reference: Commands: Edit menu

The Edit menu offers the following commands:

Undo

Reverses previous editing operation, if possible.

Cut

Deletes (resets) attributes of the selected folder and moves them to the Clipboard.

Copy

Copies attributes of the selected folder to the Clipboard.

Paste

Pastes folder attributes from the Clipboard into the selected folder.

Add File

Adds one or more files to the list of folders.

Remove File

Removes the selected file from the list of folders.

Item Password

Lets you set up a password to remove protection from the selected folder and its subfolders.

User List

Opens the Modify User List dialog box.

Permissions

Opens the Permissions dialog box.

Trusted Modules

Opens the Trusted Modules dialog box.



Reference: Commands: Edit menu: Undo

Use this command to reverse the last command, if possible.

Shortcuts

Toolbar:



Keys: CTRL+Z or ALT-BACKSPACE



Reference: Commands: Edit menu: Cut

Use this command to remove all attributes of the currently selected folder and put them on the Clipboard.

Cutting data to the Clipboard replaces the contents previously stored there.

Shortcuts

Toolbar:



Keys: CTRL+X



Reference: Commands: Edit menu: Copy

Use this command to copy all attributes of the currently selected folder to the Clipboard.

Copying data to the Clipboard replaces the contents previously stored there.

Shortcuts

Toolbar:



Keys: CTRL+C



Reference: Commands: Edit menu: [Paste](#)

Use this command to replace all attributes of the currently selected folder with the attributes from the Clipboard. This command is unavailable if the Clipboard is empty.

Shortcuts

Toolbar:



Keys: CTRL+V



Reference: Commands: Edit menu: [Add File](#)

Use this command to add one or more files to the list of folders displayed in the main window.

Shortcuts

Toolbar:
Keys: INS





Reference: Commands: Edit menu: [Remove File](#)

Use this command to remove the selected file from the list of folders displayed in the main window.

NOTE: The file itself is NOT deleted when you use this command!

Shortcuts

Toolbar:
Keys: DEL





Reference: Commands: Edit menu: [Item Password](#)

Use this command to set up a password for the currently selected file or folder. If you set up such a password, you will be able to remove protection from the file or folder (and its subfolders), leaving other files and folders protected by Folder Guard.

This command is unavailable if the selected item is not a file or a file system folder.

Shortcuts

Toolbar:



Keys: CTRL+W



Reference: Commands: Edit menu: User List

Use this command to manipulate the contents of the User List. When you choose this command, Folder Guard displays the Modify User List dialog box.

Shortcuts

Toolbar:



Keys: CTRL+L



Reference: Commands: Edit menu: Permissions

Use this command to set up permissions for users. When you choose this command, Folder Guard displays the Permissions dialog box.

Shortcuts

Toolbar:



Keys: CTRL+P



Reference: Commands: Edit menu: [Trusted Modules](#)

Use this command to modify the list of the trusted modules. When you choose this command, Folder Guard displays the Trusted Modules dialog box.

Shortcuts

Toolbar:



Keys: CTRL+T



Reference: Commands: [Attributes menu](#)

The Attributes menu offers the following commands:

Access

Visibility

Modifies attributes of the selected folder for the selected user.

Reset

Resets attributes of the selected folder to *default* for all users.

Copy All

Copies attributes of all folders between different users in the User List.

Reset All

Resets attributes of all folders to *default* for the user currently selected in the User List.

Modify

Opens the Attributes for the selected item dialog box.



Reference: Commands: Attributes menu: Access

Use these commands to assign an access attribute to the selected item (folder, file, or filter) for the user currently selected in the User List.



Reference: Commands: Attributes menu: Visibility

Use these commands to assign a visibility attribute to the selected item (folder or file) for the user currently selected in the User List.



Reference: Commands: Attributes menu: [Reset](#)

Use this command to assign the *default access* and *default visibility* attributes to the selected item for all users listed in the User List.

Shortcuts

Keys: CTRL+R



Reference: Commands: Attributes menu: Copy All

Use this command to copy the attributes of all items (folders, files, and filters) between different users listed in the User List. When you choose this command, Folder Guard displays the Copy All Attributes dialog box.

Tip: To copy permissions between different users as well, use the *Copy Permissions* button on the Permissions dialog box.

Shortcuts

Keys: CTRL+A



Reference: Commands: Attributes menu: [Reset All](#)

Use this command to assign the *default* attributes to all items (folders, files, and filters) for the user currently selected in the User List.

Shortcuts

Keys: CTRL+U



Reference: Commands: Attributes menu: Modify

Use this command to modify the attributes of the currently selected item (folder, file, or filter). When you choose this command, Folder Guard displays the Attributes dialog box.

Shortcuts

Keys: ALT+ENTER



Reference: Commands: Filters menu

The Filters menu appears on the menu bar whenever the main window is switched into the filter view. This menu offers the following commands:

New

Creates a new filter.

Rename

Lets you rename the currently selected filter.

Delete

Deletes the currently selected filter from the list.

Modify

Opens the Properties for the filter dialog box.

Move Up

Move Down

Moves the currently selected filter in the list.

Reset list

Resets the list of filters as it was when you first installed Folder Guard.



Reference: Commands: Filters menu: New

Use this command to create a new, empty filter. When you choose this command, Folder Guard displays the Properties for the filter dialog box.

Shortcuts

Toolbar:
Keys: INS





Reference: Commands: Filters menu: [Rename](#)

Use this command to rename the selected filter.

Shortcuts

Toolbar:



Keys: F2



Reference: Commands: Filters menu: Delete

Use this command to delete the selected filter. You will be asked to confirm the command before the filter is actually deleted from the list.

Tip: Instead of deleting a filter, you may wish to simply reset its attributes to the *default* ones, using the Attributes - Reset command. (Folder Guard does not use filters with the default attributes).

Shortcuts

Toolbar:
Keys: DEL





Reference: Commands: Filters menu: Modify

Use this command to change the properties of the selected filter. When you choose this command, Folder Guard displays the Properties for the Filter dialog box.

Shortcuts

Toolbar:



Keys: ENTER



Reference: Commands: Filters menu: Move Up

Use this command to move the selected filter one step closer to the beginning of the filter list.

Shortcuts

Toolbar:



Keys: CTRL+UP



Reference: Commands: Filters menu: Move Down

Use this command to move the selected filter one step closer to the end of the filter list.

Shortcuts

Toolbar:



Keys: CTRL+DOWN



Reference: Commands: Filters menu: [Reset list](#)

Use this command to reset the filter list, that is make it the same as it was when you first installed Folder Guard. All changes you might have made to the list of filters will be lost! This command cannot be undone, unless you have saved the changes in a separate FGA file.

When you choose this command, Folder Guard prompts you to confirm the action.



Reference: Commands: View menu

The View menu offers the following commands:

Folders

Switches to the *folder view* (Hides the list of filters and shows the list of folders instead).

Filters

Switches to the *filter view* (Hides the list of folders and shows the list of filters instead).

Toolbar

Shows or hides the toolbar.

Status Bar

Shows or hides the status bar.

User List

Shows or hides the User List.

Customize Toolbar

Lets you change the set and order of buttons on the toolbar.

Compact Tree

Collapses all branches which have only subfolders with default attributes; also expands all branches which have subfolders with non-default attributes.

Refresh All

Updates the folder tree.



Reference: Commands: View menu: Folders

Use this command to display the list of folders of your computer. (If the list of folders is already shown, this command does nothing.)

Shortcuts

Toolbar:



Keys: CTRL+TAB



Reference: Commands: View menu: Filters

Use this command to display the list of filters. (If the list of filters is already shown, this command does nothing.)

Shortcuts

Toolbar:



Keys: CTRL+TAB



Reference: Commands: View menu: Toolbar

Use this command to display and hide the Toolbar, which includes buttons for some of the most commonly used Folder Guard commands. A check mark appears next to the menu item when the Toolbar is displayed.

See Toolbar for help on using the toolbar.



Reference: Commands: View menu: Status bar

Use this command to display and hide the Status Bar. The Status Bar describes the action that Folder Guard will next execute - after you select a menu item or depress a Toolbar button. It also reports on the keyboard state (Caps Lock, Num Lock, and Scroll Lock). A check mark appears next to the menu item when the Status Bar is displayed.

See Status Bar for help on using the Status Bar.



Reference: Commands: View menu: [User List](#)

Use this command to display and hide the User List. A check mark appears next to the menu item when the User List is displayed.



Reference: Commands: View menu: [Customize Toolbar](#)

Use this command to open the Customize Toolbar dialog box, that lets you add and remove buttons to/from the toolbar. You can also use this command to change the order in which the buttons appear on the toolbar .



Reference: Commands: View menu: [Compact Tree](#)

Use this command to show all files and folders with non-default attributes, and collapse all folders which contain no items with non-default attributes.



Reference: Commands: View menu: Refresh

Use this command to update the list of files and folders displayed in the main window of Folder Guard.
Use this command after you have renamed or moved a file or a folder with Windows Explorer.

Shortcut

Key: F5



Reference: Commands: Tools menu

The Tools menu offers the following commands:

Policy Editor

Runs the Windows Policy Editor (PoEdit.exe).

Registry Editor

Runs the Windows Registry Editor (RegEdit.exe).

System Editor

Runs the Windows System Configuration Editor (SysEdit.exe).

Control panel

Opens the Control Panel.

Explorer

Runs Explorer.

Enable/Disable Protection

Toggles the protection on and off for the current user.



Reference: Commands: Tools menu: [Enable/Disable Protection](#)

Use this command to dynamically load/unload the Folder Guard driver (FGuard.VxD) and, therefore, to enable/disable the protection for the user currently selected in the User List. This command is useful for *on the fly* testing of the protection - while you are running Folder Guard.

Shortcuts

Toolbar:





Reference: Commands: [Help menu](#)

The Help menu offers the following commands, which provide you assistance with this application:

Help Topics

Presents an index to the topics on which you can get help.

Reset Advisor

Resets Folder Guard Advisor to its original state.

WinAbility.Com on the web

Launches your default web browser and visits WinAbility.Com web site.

Registration Information

Displays/accepts the registration information for your copy of Folder Guard.

Upgrade

Takes you to the Upgrade Center on the WinAbility.Com web site.

About Folder Guard

Display program information, version number and copyright for your copy of Folder Guard.

Note: Press SHIFT+F1 to access the Context Help command of Folder Guard. When you choose this command, the mouse pointer will change to an arrow and question mark. Then click somewhere in the Folder Guard window, such as a Toolbar button. The Help topic will be shown for the item you clicked.



Reference: Commands: Help menu: [Help Topics](#)

Use this command to display the opening screen of Help. From the opening screen, you can jump to step-by-step instructions on using Folder Guard and various types of reference information.

Once you open Help, you can click the Contents button, at any time, to return to the opening screen.



Reference: Commands: Help menu: Context Help

Press SHIFT+F1 to access the Context Help command of Folder Guard. When you choose this command, the mouse pointer will change to an arrow and question mark. Then click somewhere in the Folder Guard window, such as a Toolbar button. The Help topic will be shown for the item you clicked.

Shortcuts

Toolbar:





Reference: Commands: Help menu: [Reset Advisor](#)

Use this command to reset Folder Guard Advisor in its original state, so that those messages for which you have chosen the *Don't show this message again* option will start appearing.



Folder Guard Advisor

Folder Guard Advisor is designed to assist you while you are using Folder Guard. It detects some common situations which may require your attention and displays a message describing the situation.

The message box contains the *Don't show this message again* checkbox. If you select this option before closing the message box, this particular message will not be displayed again, until you perform the Help - Reset Advisor command of Folder Guard.

Each message displayed by Folder Guard Advisor has the *default* reply button associated with it. This button is indicated by a dashed rectangle when the message is initially displayed on the screen. If you have chosen the *Don't show this message again* option for a particular message, the *default* reply will be assumed to be chosen by you for this message thereafter.

Note: Pressing the **Enter** key while a Folder Guard Advisor message is displayed is equivalent to choosing the first reply button (such as **Do It** or **Yes**). Pressing the **Escape** key has the same effect as choosing the second reply button (such as **Ignore** or **No**). Pressing the **Space** key is equivalent to choosing the button which currently has the focus (indicated by a dashed rectangle).



Reference: Commands: Help menu: [WinAbility.Com on the web](#)

Use this command to launch your default web browser and visit WinAbility.Com web site.

Shortcuts

Toolbar:





Reference: Commands: Help menu: [Registration Information](#)

Use this command to display the licensing information for your copy of Folder Guard. You may also use it to open the order form for Folder Guard or enter your registration information.

Shortcuts

Toolbar:





Reference: Commands: Help menu: [Upgrade](#)

Use this command to visit the Upgrade Center at the WinAbility.Com web site, to request an updated registration code for this version of Folder Guard.

You will be asked to enter your existing registration information, so please have your registration acknowledgment ready before using this command.



Reference: Commands: Help menu: [About Folder Guard](#)

Use this command to display the copyright notice and version number of your copy of Folder Guard. To close the About window, use this command again, or click on the About window with the mouse.

Shortcuts

Toolbar:





Reference: [Shortcuts](#)

Shortcut menu

Keyboard shortcuts

Toolbar

Status bar



Reference: Shortcuts: [Shortcut menu](#)

Folder Guard offers a shortcut menu which provides quick access to some of the commands of Folder Guard. The Shortcut menu is displayed after you click with the right mouse button within the client area of the Folder Guard window. It offers the following commands:

For files and folders:

- Access**
- Visibility**
- Item Password**
- Cut**
- Copy**
- Paste**
- Reset**
- Attributes**

Duplicate commands of the **Edit menu** and **Attributes menu**.

For filters:

- Access**
- Reset**
- Cut**
- Copy**
- Paste**
- Attributes**

Duplicate commands of the **Edit menu** and **Attributes menu**.

- New**
- Rename**
- Delete**
- Modify**

Duplicate commands of the **Filters menu**.



Reference: Shortcuts: Keyboard shortcuts

You can use the following keyboard shortcuts while working with Folder Guard:

To	Press
Get help on the highlighted menu item	F1
Create a new FGA file	Ctrl+N
Open an existing FGA file	Ctrl+O
Save the FGA file	Ctrl+S
Build *.FGD file(s)	Ctrl+B
Build All *.FGD file(s)	Ctrl+D
Change Folder Guard settings	Ctrl+E
Exit Folder Guard	Alt+F4
Undo the last editing operation	Ctrl+Z, Alt+Backspace
Cut data to the Clipboard	Ctrl+X
Copy data to the Clipboard	Ctrl+C
Paste data from the Clipboard	Ctrl+V
Add a file to the folder list	Ins
Remove a file from the folder list	Del
Modify password for the selected file or folder	Ctrl+W
Modify User List	Ctrl+L
Modify Trusted Modules List	Ctrl+T
Modify permissions	Ctrl+P
Reset attributes	Ctrl+R
Copy all attributes between users	Ctrl+A
Reset all attributes for the current user	Ctrl+U
Modify attributes of a file or a folder	Enter, Alt+Enter
Modify attributes of a filter	Alt+Enter
Modify properties of filter	Enter
Create a new filter	Ins
Rename selected filter	F2
Delete selected filter	Del
Move selected filter up in the list	Ctrl+Up arrow
Move selected filter down in the list	Ctrl+Down arrow
Refresh the list of folders	F5
Switch between main window and User List	Tab, F6
Switch between folder view and filter view	Ctrl+Tab, Ctrl+Shift+Tab
Expand the selected folder	Right arrow
Collapse the selected folder	Left arrow
Toggle protection	Ctrl+G



Reference: Shortcuts: Toolbar

The toolbar is initially displayed across the top of the Folder Guard window, below the menu bar. The toolbar provides quick mouse access to some of the more commonly used commands of Folder Guard.

To hide or display the toolbar, choose the View -- Toolbar command from the main menu. You can also use the mouse to drag the toolbar to any position on your screen.

You can also choose to display the buttons on the toolbar using the *flat buttons* style. To change this option, use the File - Settings - Misc command. Note that older versions of Windows 95 do not support this style.

Note that not all buttons are initially included in the toolbar. You can add or remove the individual buttons, or change the order of the buttons, by using the View - Customize Toolbar command.

The following buttons are available for inclusion in the toolbar:

Button	Shortcut to the command
--------	-------------------------



File - New



File - Open



File - Save



File - Build



Edit - Undo



Edit - Cut



Edit - Copy



Edit - Paste



View - Folders



View - Filters



Edit - Item Password



Edit - File Add



Edit - File Remove

The following buttons provide shortcuts to the Edit - Access commands. Clicking on any already depressed button resets the access attribute of the selected folder to the *default* access.



Full access



Read-only



No access

The following buttons provide shortcuts to the Edit - Visibility commands. Clicking on any already depressed button resets the visibility attribute of the selected folder to the *default* visibility.



Visible



Restricted



Hidden

The following buttons may also be included in the toolbar:

Button	Shortcut to the command
	<u>Edit - User List</u>
	<u>Edit - Permissions</u>
	<u>Edit - Trusted Modules</u>
	<u>File - Settings</u>
	<u>Tools - Enable/Disable Protection</u>



Edit - User List



Edit - Permissions



Edit - Trusted Modules



File - Settings



Tools - Enable/Disable Protection



Filters - New



Filters - Rename



Filters - Delete



Filters - Modify



Filters - Move Up



Filters - Move Down



Help - WinAbility.Com on the Web



Help - Registration Information



Help - About Folder Guard



Context Help



Reference: Shortcuts: Status Bar

The Status Bar is displayed at the bottom of the Folder Guard window. To display or hide the status bar, use the Status Bar command in the View menu.

The left area of the Status Bar describes actions of menu items as you use the arrow keys to navigate through menus. This area similarly shows messages that describe the actions of toolbar buttons as you depress them (that is, before you release them). Suppose that, after viewing the description of the Toolbar button command, you decide not to execute the command. You do this simply by releasing the mouse button while the pointer is off that particular button on the Toolbar.

The right areas of the status bar indicate which of the following keys are ON:

Indicator	Description
CAP	The Caps Lock key is ON.
NUM	The Num Lock key is ON.
SCRL	The Scroll Lock key is ON.

Title Bar

The title bar is located along the top of a window. It contains the name of the application and file.

To move the window, drag the title bar.

Note: You can also move dialog boxes by dragging their title bars.

Scroll bars

The Scroll bars are displayed at the right and bottom edges of the window. Scroll boxes inside the Scroll bars indicate your vertical and horizontal location in the file. You can use the mouse to scroll to other parts of the file.

Size command (System menu)

Use this command to resize the active window with the arrow keys. When you choose the Size command, the pointer changes to a four-headed arrow.

After the pointer changes to the four-headed arrow:

1. Press one of the DIRECTION keys (left, right, up, or down arrow key) to move the pointer to the border you want to move.
2. Press a DIRECTION key to move the border.
3. Press ENTER when the window is the size you want.

Note: This command is unavailable if you maximize the window.

Shortcut

Mouse: Drag the size bars at the corners or edges of the window.

Move command (Control menu)

Use this command to display a move the active window or dialog box with the arrow keys. When you choose the Move command, the pointer changes to a four-headed arrow.

Note: This command is unavailable if you maximize the window.

Shortcut

Keys: CTRL+F7

Minimize command (application Control menu)

Use this command to reduce the Folder Guard window to an icon.

Shortcut

Mouse: Click the minimize icon on the title bar.

Maximize command (System menu)

Use this command to enlarge the active window to fill the available space on your screen.

Shortcut

Mouse: Click the maximize icon on the title bar; or double-click the title bar.

Close command (Control menus)

Use this command to close the active window or dialog box.

Double-clicking a Control-menu box is the same as choosing the Close command.

Restore command (Control menu)

Use this command to return the active window to the size and position it occupied before you chose the Maximize or Minimize command.

No Help Available

No help is available for this area of the window.

No Help Available

No help is available for this message box.



Reference: [Dialog Boxes](#)

The following sections describe the dialog boxes used by Folder Guard:

Settings

Build

Copy All Attributes

Modify User List

Permissions

Trusted Modules

Attributes

Customize Toolbar

Properties for the Filter



Reference: Dialog Boxes: [Folder Guard Settings](#)

Use this dialog box to specify settings for Folder Guard. This dialog box contains the following pages:

Startup

Input

Output

Misc



Reference: Dialog Boxes: Folder Guard Settings: [Startup page](#)

Use this page to specify how you want Folder Guard to operate during Windows startup. This page contains the following areas:

Enable protection at Windows startup

If checked, this option configures Windows so that it loads the Folder Guard driver (FGuard.VxD) during its boot process, and thereby enables the protection at Windows startup.

Note: If you change this option, you must reboot Windows in order for the new setting to take effect.

Use compatibility mode

If checked, this option causes Folder Guard to operate in the compatibility mode. Normally you don't need to use this option. In some cases, however, when you have other software that is incompatible with Folder Guard, this option may prevent such problems.

Note: The *logon monitoring* feature of Folder Guard (see below) is **not** available in the compatibility mode.

Monitor user logon

If checked, this option causes Folder Guard to monitor the logon procedure.

Note: This option is ignored if the *Enable protection at Windows startup* option above is not checked, or if the *Use compatibility mode* option is checked.

Options

Press this button to open the [Logon Monitoring Options](#) dialog box.



Reference: Dialog Boxes: Folder Guard Settings: Logon Monitoring Options

Use this dialog box to specify how you want Folder Guard to monitor the logon process. This dialog box contains the following areas:

Validate user name

If checked, this option causes Folder Guard to validate the user name during the Windows logon procedure. *This option has no effect if the Microsoft Family Logon feature is enabled on your computer.*

Hide previous user name

If this option is selected, Folder Guard clears the name of the user who logged on to Windows last time in the logon prompt. *This option has no effect if the Microsoft Family Logon feature is enabled on your computer.*

No empty user name

If checked, this option causes Folder Guard to display an error message if the user has not entered a name in the logon prompt. *This option has no effect if the Microsoft Family Logon feature is enabled on your computer.*

No empty password

If checked, this option causes Folder Guard to display an error message if the user has not entered a password in the logon prompt.

No Default User

If checked, this option causes Folder Guard to disable the Cancel button on the Windows logon prompt and thus prevent from logging on as Default user.

Ask password

If checked, this option causes Folder Guard to prompt for the Default user logon password, when the user presses the Cancel button on the Windows logon prompt. If you do not check this option, Folder Guard lets you logon as the default user - and does not prompt you for the password (unless you have checked the *No Default User* option, see above).

Password

Click this button to set up the logon password for the Default user.

Disable system keys during logon

If checked, this option causes Folder Guard to disable the system keys (such as Ctrl+Alt+Del, Ctrl+Esc, Alt+Tab) while the logon prompt is displayed on the screen. You may find this option handy if you use Windows 95 and you don't want users to run Task Manager (by pressing Ctrl+Esc) before they have log onto Windows. [Click here for more information](#)

Write Log File

If checked, this option causes Folder Guard to write a record in the file specified whenever a user logs on or off.

Max. # of lines

The maximum number of records the log file may contain (default is 100). When the number of lines in the log file reaches the maximum value specified, the first record (the oldest one) is deleted from the file, leaving room for the more recent records. Each record takes about 80 bytes in the log file.

Custom texts

Messages displayed by Folder Guard while monitoring the logon. This group contains the following

areas:

Type

The type of the message.

Default

The default text of the message used by Folder Guard. This text is not used if the *Custom* area is not empty.

Custom

The custom text of the message. If this field is empty, the text specified in the *Default* area will be used.

Reset All

Click on this button to clear all custom texts. This will restore the default values for all messages displayed by Folder Guard while monitoring the logon process.



Reference: Dialog Boxes: Folder Guard Settings: [Input page](#)

Use this page to specify the active FGA file. This page contains the following areas:

Active FGA file

Path to the FGA file you want to be active. If you want no FGA file to be active, clear this box.

Reload at startup

If checked, this option causes Folder Guard to automatically open the active FGA file during its initialization. This option is ignored if no active FGA file has been specified in the *Active FGA file* area.

Activate current file

Check this box if you want the path of file being edited to be inserted in the *Active FGA file* area. This control is disabled if the file being edited has no name (untitled).



Reference: Dialog Boxes: Folder Guard Settings: [Output page](#)

Use this page to specify how and where FGD files should be built when you use the File - Build or File - Build All commands. This page contains the following areas:

Build *.FGD files on saving the active FGA file

If checked, this option causes Folder Guard to build all *.FGD files every time you save the active FGA file. This helps you keep the *.FGD files consistent with the active FGA file.

Working folder

The path to the working folder of Folder Guard.



Reference: Dialog Boxes: Folder Guard Settings: [Misc page](#)

Use this page to change miscellaneous options of Folder Guard. This page contains the following areas:

Show full path in the title bar

If checked, this option forces Folder Guard to display the full path of the FGA file being edited in its title bar. If cleared, only the name of the file is displayed in the title bar.

Show 'splash screen' at startup

If checked, this option allows Folder Guard to display the *splash screen* with information about Folder Guard at its startup. If cleared, you will not see the splash screen at startup.

Re-enable protection at exit

If checked, this option causes Folder Guard to restore the status of the protection at exit. That is, when you run Folder Guard, it always disables the protection. When you exit Folder Guard, it re-enables the protection - providing that the protection was enabled before you ran Folder Guard. If this checkbox is cleared, the protection remains disabled when you exit Folder Guard.

Prompt to activate FGA file

If checked, this option causes Folder Guard to prompt you to activate the FGA file when you save the FGA file under a different name than the one for the currently active FGA file.

Add lock/unlock commands to the Windows shortcut menu

If checked, this option causes Folder Guard to add the *Lock/Unlock* commands to the Windows shortcut menu, as needed. These commands appear on the shortcut menu only if you right-click on a file or folder that has an Item Password assigned to it with Folder Guard.

Preset system folders

If this option is checked, then whenever you create a new FGA file, Folder Guard automatically assigns the *Visible* and *Full access* attributes to the system folders on the computer. You may wish to turn this option off to prevent Folder Guard from scanning the root folders of the drives and thus speed up the process of the creation of the FGA files.

Allow protection on removable drives

If checked, this option causes Folder Guard to display subfolders of the removable drives (such as SCSI or ZIP drives, but **not** floppy or CD-ROM ones), and thus lets you protect folders on such drives. [Click here](#) for more information on using this option.

Draw 'flat' toolbar

If checked, this option causes Folder Guard to display its toolbar using the *flat-button* style. Note that older versions of Windows 95 does not support this style. This option is available only if the operating system provides support for this.



Reference: Dialog Boxes: Build

Use this dialog box to generate *.FGD file(s) to be used by the Folder Guard driver, FGuard.VxD, while performing the protection. This dialog box contains the following areas:

Build *.FGD file(s) for:

All users in User List

When selected, this option causes Folder Guard to build *.FGD files for all users listed in the User List. This option has the same effect as the File - Build All command.

Selected user only

When selected, this option causes Folder Guard to build an FGD file for the specified user only.

Note: Whenever you build an FGD file for a particular user, the FGD file for the Default user is re-built as well.



Reference: Dialog Boxes: [Copy All Attributes](#)

Use this dialog box to copy the attributes of all items (folders, files, and filters) between different users. This dialog box contains the following areas:

Copy the attributes of all folders:

From User

The *source* user name, whose attributes should be copied to another user .

To User

The *destination* user name, whose attributes should be set.

Note: This operation makes the attributes of all folders, files, and filters for the user specified in the To User field identical to those of the user specified in the From User field.

Tip: To copy permissions between different users as well, use the *Copy Permissions* button on the [Permissions](#) dialog box.



Reference: Dialog Boxes: Modify User List

Use this dialog box to manipulate the contents of the User List. This dialog box contains the following areas:

Users

The list of users currently included in the User List.

Add

Click this button to add a new name to the User List. This will display the Add User dialog box.

Add Existing

Click this button to add a new name to the User List by choosing the name from the list of known users of your computer. This will display the Add Existing User dialog box.

Remove

Click this button to remove the selected name from the User List.

Rename

Click this button to rename the selected name in the User List. This will display the Rename User dialog box.

Move Up

Move Down

Use these buttons to change the order of names displayed in the User List.



Reference: Dialog Boxes: [Add User](#)

Use this dialog box to specify the name to be added to the User List. This dialog box contains the following areas:

Add new user to the User List

Enter the name of the user in this box.

Choose

Click this button to select the user's name in the list of known users of your computer. This will display the Choose Existing User dialog box.

Note: It is not sufficient to add a user's name to the User List to make such a user a *valid* user of the computer. By adding a name to the User List, you make this user name known to Folder Guard, but you still have to make this user known to Windows itself, by creating a separate user account.



Reference: Dialog Boxes: [Rename User](#)

Use this dialog box to change a name in the User List. This dialog box contains the following areas:

Rename user

Enter the new name in this box.

Choose

Click this button to select the user's name in the list of known users of your computer. This will display the Choose Existing User dialog box.



Reference: Dialog Boxes: [Choose Existing User](#)

Use this dialog box to choose the user's name from the list of known users of your computer.



Reference: Dialog Boxes: [Add Existing User](#)

Use this dialog box to choose the user's name from the list of known users of your computer. Click on the **Add All** button to add all known user's names to the User List.



Reference: Dialog Boxes: Permissions

Use this dialog box to assign permissions for users.

Click on the icons next to the descriptions of the permissions to control the availability of the corresponding resources for the user displayed in the *Users* list of this dialog box.

Icons Description



Makes the resource available for the current user.



Makes the resource unavailable for the current user.



Does not change the availability of the resource for the current user (the *default* availability).

Note: Some of the permissions take effect only after the user logs off and then logs back on to Windows, or after Windows reboots.

Note: If you assign the *default* availability of a resource to any user other than the *Default user*, Folder Guard instead uses the corresponding permission assigned to the *Default user*. The following icons are used to represent such permissions:



The resource will be available to the current user since it is made available for the *Default User*.



The resource will be unavailable to the current user since it is made unavailable for the *Default User*.

You can use this feature to simplify your work: First make the assignments of the permissions common to all users as the permissions to the *Default user*. Then assign to the other users only those permissions which you want to differ from the permissions set for the *Default user*.



Reference: Dialog Boxes: Permissions: Copy Permissions

Use this dialog box to copy all permissions between different users. This dialog box contains the following areas:

Copy all permissions:

From User

The *source* user name, whose permissions should be copied to another user .

To User

The *destination* user name, whose permissions should be set.

Tip: To copy the attributes of all folders, files, and filters between different users as well, use the Attributes - Copy All command.



Reference: Dialog Boxes: Trusted Modules

Use this dialog box to modify the list of the trusted modules. This dialog box contains the following areas:

Names

Shows the names of the modules that are currently chosen to be *trusted*. The module name is usually the same as the file name (without the name extension) of the appropriate executable file. If the file name is longer than 8 characters, the extra characters are truncated when making the module name. The module names are case-insensitive, that is REGSVR32 and Regsvr32 are the names of the same module.

Interpretation of the list

Lets you control how the list of the modules should be treated by Folder Guard while performing the protection. Normally, you should use the first option offered, *The listed modules are the trusted ones*. In some cases, however, you may find more suitable the second option, *All modules are trusted except the listed ones*. For example, you may make the list to contain only one entry, EXPLORER. In such a case, Folder Guard will protect the files and folders only if Windows Explorer is used by the user to browse the contents of the disks. If the user uses any other program, Folder Guard will NOT protect the folders.

Add to the list

This group of buttons lets you add new modules to the list. (Note that only Windows modules, 32-bit or 16-bit, can be made trusted. If you add a name of a DOS program or console application to the list, it will be ignored by Folder Guard.)

Task

Lets you choose the name from the list of the currently running modules. (This is the recommended method of adding new entries to the trusted modules list.) When you press this button, a menu appears on the screen, that contains the names of all the currently running modules that may be designated as the *trusted ones*.

File

Lets you browse for the executable module to designate as the *trusted* one. Use this method to add the name of a module that is not currently running.

Name

Lets you type in the name of the module. Note that Folder Guard does **not** verify that the name you have typed in is a valid module name. If you type in a name that does not correspond to the module that you would like to be *trusted*, it will be ignored by Folder Guard. To avoid possible errors while typing in the names, we recommend using the other two methods (*Task* and *File*, see above) instead of this one.

Modify

Use this button to modify the name currently selected in the list.

Delete

Use this button to delete the currently selected name from the list.

Reset

Use this button to reset the contents the trusted modules list.

Move item

Lets you change the order of modules in the list.



Reference: Dialog Boxes: Attributes

Use this dialog box to assign attributes to the currently selected file, folder, or filter. This dialog box contains the following areas:

User

Shows the user for whom the attributes of the item are displayed in the *Attributes* area. You may select any user in this list to modify the attributes of the selected item for a particular user.

Attributes

Shows the *access* and *visibility* attributes of the selected item for the user selected in the *User* area. Note that the *visibility* attributes are not available for the filters.

Reset...

Press this button to assign the *default* attributes to the selected item for all users. This is equivalent to the Attributes - Reset command.



Reference: Dialog Boxes: [Customize Toolbar](#)

Use this dialog box to change the set of buttons displayed on the toolbar. This dialog box contains the following areas:

Available buttons

The list of buttons that can be placed on the toolbar.

Toolbar buttons

The list of buttons that the toolbar currently contains.

You may use the mouse to drag buttons between these lists. Pressing the *Reset* button restores the toolbar to its original state -- just as it was when you first installed Folder Guard.



Reference: Dialog Boxes: Properties for the Filter

Use this dialog box to change properties of the currently selected filter. This dialog box contains the following areas:

Apply to files

One or more of the file name specifications defining the files the filter should be applied to. Empty area means ALL (the same as *), that is all files match the filter.

Except for files

One or more of the file name specifications defining the files the filter should NOT be applied to. Empty area means NONE, that is no files are excluded from the filter. If a file name matches the specification entered in this area, the filter will not be applied to such a file, even if its file name matches the *Apply to files* specification.

Apply to folders

One or more of the folder specifications defining the folders the filter should be applied to. Empty area means ALL (the same as *), that is all folders match the filter.

Except for folders

One or more of the folder specifications defining the folders the filter should NOT be applied to. Empty area means NONE, that is no folders are excluded from the filter. If the folder name matches the specification entered in this area, the filter will not be applied to the files in such a folder, even if the folder name matches the *Apply to folders* specification.

Apply to modules

One or more of the module specifications defining the modules the filter should be applied to. Empty area means ALL (the same as *), that is all modules match the filter.

Except for modules

One or more of the module specifications defining the modules the filter should NOT be applied to. Empty area means NONE, that is no modules are excluded from the filter. If the module name matches the specification entered in this area, the filter will not be applied to the files accessed by such a module, even if the module name matches the *Apply to modules* specification.

Comments

Any text (such as explanatory notes) may be entered here. The contents of this field is not used by Folder Guard when restricting access to files with the filters.

Note: The name of a filter can be changed by using the Filter - Rename command. **The name itself is not used by Folder Guard while performing the protection**, it is just a label to help you identify the filters.

See also:

Filters

Using the Filters

Filter properties

How Folder Guard applies the Filters



Reference: Filter properties

The following screens provide information on the syntax of the fields used to specify the filters (by using the Properties for the Filter dialog box).

Apply to/Except for files

Apply to/Except for folders

Apply to/Except for modules

All specifications are case-insensitive. When describing them, the following terms are used:

path, full path, complete path

the full DOS path, usually beginning with a drive letter, used to specify the exact location of files and folders on the computer disks. For example, **C:\Docs\Personal\Letter to mom.doc** is the path to the file named **Letter to mom.doc**, located in the subfolder **Personal** of the folder **Docs** on the drive **C:**. The full path to the folder where this file is located is **C:\Docs\Personal**.

folder part of a path

the full path to the folder where the file in question is located. In the previous example, **C:\Docs\Personal** is the folder part of the full path to the file **Letter to mom.doc**.

full file name, complete file name

the name of the file that uniquely identifies the file within the folder where it resides. In the previous example, **Letter to mom.doc** is the full file name of the file.

file name

the part of the full file name that does not include the file name extension. In the previous example, **Letter to mom** is the file name of the file **Letter to mom.doc**.

extension, file name extension

the part of the complete file name, following the last dot in the name, if any. The extension is used by Windows to identify the type of the file. In the previous example, **doc** is the complete file name extension of the file **Letter to mom.doc**.

Note: Window Explorer may not show the file name extensions. To make the extensions visible, run Explorer, choose View - Folder Options in the menu, select the View page, and clear the "Hide file extensions for known file types" option.

wildcard

the *star* (*) character used as a placeholder for zero, one or more of arbitrary characters. Note the question mark character (?) is NOT used as a wildcard in the filter specifications.

module name

the name of the module that is accessing a file. For more information about the modules see Trusted Modules.

See also:

Filters

Using the Filters

How Folder Guard applies the Filters



Reference: Filter properties: Apply to/Except for files

The *Apply to files* and *Except for files* areas may contain an arbitrary number (zero, one, or more) of the complete file names (wildcards are allowed), NOT including the folder part of the full paths of the files.

Examples:

***.txt**

All files that have the file name extension *txt*, such as Test.txt, ABC.TXT, foo123.tXt, match this specification. Test.txt1, ABC.doc, T.toc are some of the names that do NOT match this specification.

abc.*

All files that have the file name *abc*, such as abc.txt, ABC.doc, AbC.exe, match this specification. Abc1.txt, ABCDEF.doc, A.exe, abc (without any extension) are some of the names that do NOT match this specification.

abc*

All file names that begin with *abc*, such as abc.txt, ABC1.doc, AbCdEfG.exe, abc (without any extension) match this specification. Ab.txt, B.doc, CBA.exe, are some of the names that do NOT match this specification.

.t

All files that have the file name extension beginning with *t*, such as Test.txt, ABC.TOC, foo123.t, match this specification. Test.123, ABC.doc, T.exe are some of the names that do NOT match this specification.

.

All files match this specification, except the file names that don't have the dot in the name (and, therefore, don't have the file name extension).

All files match this specification.

abc.txt

(No wildcard is used). Only the files with the full file name **abc.txt** (case-insensitive) match this specification. All other names do NOT match this specification.

If a specification must include spaces, it should be enclosed in double quotes. For example, to specify all files that begin with *white paper*, use the specification "white paper*", including quotes.

Several specifications may be separated with spaces, semicolons (;), or commas (,). For example:

.txt;"white paper";*.EXE,*.doc

Any file that have the file name extension *txt*, or *exe*, or *doc*, or if its file name begins with *white paper*, would have matched such a composite specification.

See also:

[Filters](#)

[Using the Filters](#)

[Filter properties](#)

[How Folder Guard applies the Filters](#)



Reference: Filter properties: Apply to/Except for folders

The *Apply to folders* and *Except for folders* areas may contain any number (zero, one, or more) of the full paths to the folders (wildcards are allowed).

Examples:

C:\Docs

All files located in the C:\Docs folder, such as C:\Docs\Test.txt, C:\Docs\ABC.TXT, C:\Docs\foo123.toc, match this specification. If a file is located in any other folder (including any subfolders of C:\Docs), such as C:\Temp\Test.txt, C:\Docs\Personal\Test.txt, D:\Archive\ABC.TXT, do NOT match this specification.

C:\Docs*

All files located in any subfolder of the C:\Docs folder (but not those located in the C:\Docs folder itself), such as "C:\Docs\Business\white paper.txt", "C:\Docs\Personal\Letter to mom.doc", match this specification. If a file is located in any other folder (including the folder C:\Docs), such as C:\Temp\Test.txt, C:\Docs\ Test.txt, D:\Archive\ABC.TXT, do NOT match this specification.

C:\Docs*

All files located in any folder which path begins with "C:\Docs", such as "C:\Docs\Business\white paper.txt", "C:\Docs\Personal\Letter to mom.doc", C:\Docs\Test.txt, C:\DocsOld\1998.txt, match this specification. If the path of the folder does not begin with "C:\Docs", such as C:\Temp\Test.txt, C:\Doom\Game.exe, D:\Archive\ABC.TXT, do NOT match this specification.

*

Files in all folders match this specification.

If a specification must include spaces, it should be enclosed in double quotes. For example, to specify all files that reside in subfolders of C:\Program Files, use the specification "C:\Program Files*", including quotes.

Several specifications may be separated with line breaks, spaces, semicolons (;), or commas (,). For example:

"C:\Program Files*", "C:\Windows"

See also:

[Filters](#)

[Using the Filters](#)

[Filter properties](#)

[How Folder Guard applies the Filters](#)



Reference: Filter properties: [Apply to/Except for modules](#)

The *Apply to modules* and *Except for modules* areas may contain any number (zero, one, or more) of the module names (wildcards are allowed).

Examples:

notepad

The files accessed by Windows Notepad match this specification. Files accessed by any other module do not match this specification.

win*

Only module names that begin with *win*, such as *winfile* or *winword*, match this specification.

All module names match this specification.

Several specifications may be separated with spaces, semicolons (;), or commas (,). For example:

notepad winword winfile

See also:

[Filters](#)

[Using the Filters](#)

[Filter properties](#)

[How Folder Guard applies the Filters](#)



Reference: [Files](#)

FGuard.exe
FGKey.exe
FGuard.vxd
FGuard32.dll
FGuard.cfg
FGuard.fgp
FGuard.lic
FGuard.unm
FGuard.adm
Registry.bat



Reference: Files: FGuard.exe

FGuard.exe is the file name of the main application of Folder Guard. You use this application to assign desired access rights to the folders and control other Folder Guard settings. Windows runs FGuard.exe when you choose **Folder Guard** in Start Menu.

With FGuard.exe you can open and save the *.FGA files. FGuard.exe also generates the following files: *.FGD, FGuard.unm, FGuard.cfg, FGuard.lic.

FGuard.exe uses file FGuard32.dll during its operation; the latter must be present in the same folder in order for FGuard.exe to operate.

When you run FGuard.exe, it determines whether the protection is enabled. If this is the case, FGuard.exe disables the protection - thereby giving you full access to all folders on your computer while using FGuard.exe. When you exit FGuard.exe, it re-enables the protection according to the new settings, unless you have opted otherwise (by using the Settings command).



Reference: Files: FGKey.exe

FGKey.exe is a utility allowing you to dynamically enable/disable the protection of your computer.

When you run FGKey.exe without specifying any switches on its command line, it determines whether the protection is currently in effect and acts as follows:

- If the protection is not enabled, FGKey.exe prompts you to enable it. If you reply **Yes** to the prompt, FGKey.exe enables the protection.
- If the protection is enabled, FGKey.exe prompts you to enter the Master password. If you type in the valid password, FGKey.exe disables the protection. If the Master password has not been set up, FGKey.exe does nothing (that is, it leaves the protection in effect).

You can customize this behavior by using the following command line switches with FGKey.exe. You can specify several switches on the same command line, separating them with spaces.

Switch	Description
/S	Silent operation. If this option is used alone, FGKey.exe works in the same way as described above, except that it does not prompt you to enable it (the Yes reply is assumed), and does not show any messages if its operation was successful. FGKey.exe does show the password prompt and error messages, though. If you use this switch with other switches listed below, FGKey.exe will show only password prompts or error messages as needed. You don't have to specify this switch with the /D or /E switches, since they perform the operations <i>silently</i> by default.
/V	Verbose operation. Forces FGKey.exe to show all messages as needed. You may use this option with the /D and /E switches to override their default <i>silent</i> operation mode.
/P:path	Specifies the path of the file or folder to lock or unlock. If you specify this option, then FGKey.exe will attempt to lock or unlock the object specified by <i>path</i> . The path should be the long one, as displayed by Windows Explorer, NOT the MSDOS (8.3) alias. If the path contains spaces, it must be included in quotes, for example: /P:"C:\Program Files". If this option is not specified, then FGKey.exe will attempt to enable or disable all protection performed by Folder Guard.
/E	Enables the protection (if no /P switch is specified), or locks the object specified with the /P switch. If protection is already enabled (or the object is already locked), FGKey.exe does nothing, leaving the protection enabled. This switch assumes the /S switch, unless the /V switch is used in the command line as well.
/D:password	Disables the protection (if no /P switch is specified), or unlocks the object specified with the /P switch. If the "password" argument matches the appropriate <u>password</u> , this command "silently" disables the protection or unlocks the file or folder specified with the /P switch. If the password specified is invalid or missing, the command prompts for the password. If the protection is already disabled, the command does nothing, leaving the protection disabled. This switch assumes the /S, unless the /V switch is used in the command line as well.
/D	Disables the protection, prompting for the <u>Master password</u> (if no /P switch is specified), or unlocks the object specified with the /P switch, prompting for the appropriate <u>Item password</u> . If the protection is already disabled, FGKey.exe does nothing, leaving the protection disabled. This switch assumes the /S switch, unless the /V switch is used in the command line as well.

/C

Lets you clean up the registry settings used by Folder Guard while processing the permissions for the current user. Normally, you don't need to use this option, since Folder Guard handles all related registry settings automatically. In some rare cases, however, such as after a system crash while processing the permissions, you may need to use this option to reset all permissions for the current user. Note that you must disable the protection before using FGKey.exe with this switch.

Note: If you have enabled the protection with FGKey.exe, it will be in effect only until Windows reboots - unless you have also selected the *Enable protection at Windows startup* option in the Settings dialog box.

FGKey.exe uses FGuard32.dll during its operation; the latter must be present in the same folder in order for FGKey.exe to work.



Reference: Files: FGuard.vxd

FGuard.VxD is the core module of Folder Guard. This is the module which actually performs the protection of folders. FGuard.VxD can be loaded in two ways - statically or dynamically.

Windows loads FGuard.VxD *statically* during its boot process, if the following key exists in the Registry:

HKEY_LOCAL_MACHINE\ System\ CurrentControlSet\ Services\ VxD\ FGUARD

And also, if the string variable *StaticVxD* under this key contains a valid DOS path to FGuard.VxD. The path must not contain *long* file names; the 8.3 name aliases must be specified for the *long* components of the path. Folder Guard prepares and writes this variable into the Registry for you when you select the *Enable protection at Windows startup* option in the Settings dialog box, provided that the *Use compatibility mode* option is not checked. You can also add/remove this variable manually, or by using the FGuard.adm file with the Windows System Policy Editor.

FGuard.VxD can also be loaded/unloaded dynamically, by running FGKey.exe. When you select the *Compatibility Mode* option in the Settings dialog box, Folder Guard adds the following entry:

[MS-DOS path to the working folder of Folder Guard]\FGKey.exe /E

to the following key in the Windows Registry:

HKEY_LOCAL_MACHINE\ Software\ Microsoft\ Windows\ CurrentVersion\ Run

This entry causes FGuard.VxD to be loaded dynamically every time Windows starts.

Whenever FGuard.VxD is loaded (statically or dynamically) into Windows memory, and whenever a user logs on or off while FGuard.VxD is loaded into memory, the following occurs:

- FGuard.VxD searches for the appropriate FGD file. If such a file is found, FGuard.VxD starts to protect folders according to the data contained in the FGD file.
- FGuard.VxD searches for the licensing information. If no valid licensing information is found, FGuard.VxD starts to display the *Disable Folder Guard* prompt. The interval between the prompts is first set to 15 minutes, then increased to 30 and 60 minutes.



Reference: Files: FGuard32.dll

This file contains common routines used by FGuard.exe, FGKey.exe, and Setup.exe. None of these modules will work if the FGuard32.dll file is missing. FGuard32.dll is also indirectly used by FGuard.VxD during the logon monitoring.



Reference: Files: FGuard.cfg

This file is used by FGuard.exe to store its configuration settings between sessions. FGuard.cfg is created when you run FGuard.exe for the first time. The information stored in FGuard.cfg includes: position of the main window of Folder Guard on the screen, positions of its toolbars, options and settings of Folder Guard.

In order for FGuard.cfg to be used by FGuard.exe, it must be located in the same folder from which you run FGuard.exe. If FGuard.exe cannot find FGuard.cfg, it restores its settings and options to their default values. When you exit FGuard.exe, it overwrites file FGuard.cfg with the new settings.

Folder Guard does not store its settings in the Registry (as do many other Windows applications) because it is likely to be run by you (the Administrator) while logging onto Windows under different user names and, possibly, from different computers (that is, if you are using Folder Guard on a network).



Reference: Files: [FGuard.fgp](#)

This file is used by Folder Guard to store its passwords and is used while performing the protection. This file is recreated every time you rebuild the FGD files.

The passwords are stored in the encoded form, so they are not visible if someone opens this file.



Reference: Files: FGuard.lic

This file can be used to supply the licensing (registration) information for FGuard.VxD when you use Folder Guard on a large network.

Normally, when FGuard.VxD is loaded into Windows memory, it searches for the licensing information in the local Registry. On a large network, the Administrator can use FGuard.lic to avoid the time-consuming practice of manually entering the required licensing information into the Registry on each computer. How? Simply by placing this information into the FGuard.lic file.

The FGuard.lic file is created for you automatically when you enter the Registration Code using the Help - Registration Information command of Folder Guard. However, this file is not created if the number of computers in your license is less than 4.

You may also manually create this file. For example, if Folder Guard is registered to the name *FooSoft, Inc.*, for use on 10 computers, and the Registration Code is 12345, then you can create FGuard.lic as follows:

- Run Notepad.
- Enter the name, number of the computers and the Registration Code, separated with vertical lines (ASCII character 124), as a single line:

FooSoft, Inc.|10|12345

- Save the file in the working folder, using the name *FGuard.lic* in the Save As dialog box.
- Exit Notepad.

Note: In order for this file to be used by FGuard.VxD, it must be named FGuard.lic and placed in the working folder. It must also contain valid registration information, and the number of computers in your license must be 4 or more. If any of these conditions is not satisfied, FGuard.VxD ignores the information supplied by the FGuard.lic file.



Reference: Files: FGuard.unm

This is an auxiliary file, which Folder Guard may create in the working folder while building the *.FGD files. Folder Guard places information in FGuard.unm which helps FGuard.VxD determine which FGD file should be used for each user to perform the protection of folders. If you see this file in the working folder, do not modify or delete it.



Reference: Files: FGuard.adm

File FGuard.adm contains templates for the Windows System Policy Editor. You can use FGuard.adm to control some settings of Folder Guard with the System Policy Editor, and to automate setting up Folder Guard on multiple computers in a network.

To use this file, you must first install System Policies, and add it to the list of policy templates. If your version of Policy Editor does not support multiple policy templates, you need to merge the FGuard.adm file with the active template file. You can merge these two files using any plain text editor, such as Notepad:

- Run Notepad and open the active template file (usually C:\Windows\Inf\Admin.ADM - you can determine the active template file by running the System Policy Editor and choosing the Options - Template command in its menu).
- Run another instance of Notepad and open the FGuard.adm file. At this step, your screen should display two open Notepad windows.
- FGuard.adm contains two sections, CLASS MACHINE and CLASS USER. Merge these sections with the appropriate sections of the active template file (by copying them onto the Clipboard and pasting into the second Notepad window).
- Save the active template file and close both Notepad windows.

Note: If you have set up the logon password for Default user, you must enter the (encoded) password into the active template file before using its *Allow logon as Default user* option. The encoded password for the Default user is placed by Folder Guard into the local Registry, in the variable *DefUserData*, under the key HKEY_LOCAL_MACHINE\ System\ CurrentControlSet\ Services\ Folder Guard\ NetworkProvider. Refer to the comments in the FGuard.adm file for instructions on adding the encoded password to the template file.

Now run the System Policy Editor and choose File - Open Registry, or open the active policy file. Both the *Local User* and the *Local Computer* entries should now have additional sets of settings, in the *WinAbility - Folder Guard* branches.



Reference: Files: REGISTRY.BAT

REGISTRY.BAT is a simple MS-DOS batch command file, which you can use to automate the process of backing up and restoring the Windows Registry. It is no longer included with Folder Guard, but it is available for *free* download from our web site: <http://www.winability.com/>. (Follow the link to **Simple Registry Backup/Restore Utility**.)



Appendices

[How Folder Guard initializes system folders](#)
[How FGuard.VxD searches for the FGD file\(s\)](#)
[How FGuard.VxD searches for the licensing information](#)
[How Folder Guard applies the Filters](#)
[How Folder Guard validates user name at logon](#)
[How to create a new user account](#)
[How to delete a user account](#)
[How to backup the Registry](#)
[How to enable the logon prompt on a stand-alone computer](#)
[How to enable user profiles on a stand-alone computer](#)
[How to disable the Default user account](#)
[How to disable Ctrl+Esc during logon](#)
[How to disable Ctrl+C during Windows boot-up](#)
[How to restrict the *Restart in MS-DOS mode* command](#)
[A crash course in System Policies](#)
[MSDOS.SYS: Useful commands](#)



Appendices: How Folder Guard initializes system folders

Whenever you use Folder Guard to create a new FGA file, Folder Guard assigns the *default* attributes to all folders. If the Preset system folders option is turned on, Folder Guard also assigns the *Full access* and *Visible* attributes to the following folders:

- The folder in which Windows is installed (usually C:\Windows).
- The Windows system folder (usually C:\Windows\System).
- Any folder in the root folders which has the *system* attribute assigned by Windows (such as C:\Recycled).
- Any subfolder of the C:\Windows folder which has the *system* attribute assigned by Windows (such as C:\Windows\Fonts).

Folder Guard does this to prevent you from inadvertently restricting access to these folders, since Windows uses them during its operation. You may change these attributes, if you wish, although we do not recommend doing so. **Always backup the Registry** before experimenting with these folders!



Appendices: How FGuard.VxD searches for the FGD file(s)

FGuard.VxD first attempts to read the string variable *FGD* in the local Registry, under the key:

HKEY_CURRENT_USER\ Software\ WinAbility\ FGD.

If this variable contains the DOS path to an FGD file, FGuard.VxD uses this file to perform the protection.

Note: Folder Guard does not set up this variable, so it usually does not exist. You may, however, set up this variable (using the file FGuard.adm with the Windows System Policy Editor, for example), to force FGuard.VxD use a specific FGD file for a particular user.

If the previous step fails, FGuard.VxD determines the name of the user currently logged on to Windows and looks for the FGD file with the same name in the working folder.

If the previous step fails, FGuard.VxD uses the *Default.FGD* file (in the working folder) to perform the protection.



Appendices: How FGuard.VxD searches for the licensing information

FGuard.VxD first attempts to find the licensing information in the local Registry, under the key:

HKEY_LOCAL_MACHINE\ Software\ WinAbility\ Folder Guard\ Setup \ 1

If this key exists, FGuard.VxD reads the values of the following *string* variables: *Registered To*, *Number of Users*, and *Registration Code*. FGuard.VxD then verifies the validity of the Registration Code.

If the previous step fails, FGuard.VxD attempts to find the registration information in file FGuard.lic, which is assumed to be located in the working folder.



Appendices: How Folder Guard applies the Filters

Whenever a program attempts to access a file, Folder Guard takes a *virtual note* of the following information:

- The full file name of the file being accessed;
- The full path to the folder where the file in question is located;
- The name of the module that is accessing the file.

Folder Guard then walks through the list of filters, in the order they are listed in the Folder Guard window, and attempts to match the noted information against the specifications of each filter that has non-default access attribute for the user currently logged on to the computer. The match occurs if all the following conditions are met:

- The name of the file being accessed matches the specification of the *Apply to files* field of the filter, but does not match the *Except for files* field, AND
- The name of the folder where the file is located matches the specification of the *Apply to folders* field of the filter, but does not match the *Except for folders* field, AND
- The name of the module accessing the file matches the specification of the *Apply to modules* field of the filter, but does not match the *Except for modules* field.

If all three conditions above are met, Folder Guard stops walking through the filter list and uses the access attribute assigned to the filter to allow or deny access to the file. If at least one condition listed above is not met, Folder Guard skips the filter and continues to search for the matching filter until the end of the filter list is reached. If no matching filter is found, Folder Guard uses the access attribute of the file, as it was assigned with Folder Guard and displayed in the *folder view*. If the file was not added to the folder list, or has a default access attribute, the access attribute of the folder where the file is located is used.

Note: The Trusted Modules have a higher priority than those appearing in the filter specifications. That is, a trusted module can access all files unconditionally, even if you have set up filter(s) that restrict access to certain files for that module.

See also:

[Filters](#)

[Using the Filters](#)

[Filter properties](#)



Appendices: How Folder Guard validates user name at logon

If you have enabled the Validate user name option, Folder Guard checks the user name entered at the logon prompt against the list of users known to Windows (that is, the users who have already logged on to the computer at least once). This list is maintained by Windows in the **[Password Lists]** section of the file **System.ini**, located in the Windows folder. This section is used by Windows internally to determine which password list file (the PWL file) should be used to verify the logon password for each user. Windows maintains also the list of user profiles (only for users for whom separate profiles were created). This list is stored in the Registry, under the key:

HKEY_LOCAL_MACHINE\ Software\ Microsoft\ Windows\ CurrentVersion\ ProfileList

Each user is represented by a separate subkey under this key. Windows creates such a subkey automatically (if the profiles are enabled), when the user logs onto the computer for the first time.

When validating the user name entered at the logon prompt, Folder Guard checks the name against both of these lists, the [Password Lists] section in the System.ini file and the ProfileList key in the Registry. If none of these lists contains the name entered by the user at the logon prompt, the name is considered invalid.



Appendices: How to create a new user account

If you use Windows 98, you can manage the user accounts with Control Panel - Users command of Windows. If the computer is connected to a network, you should use the user managing tools provided by the network to create or delete the user accounts. On a stand-alone computer, if you use Folder Guard to validate user's name at logon, and want to allow a new user to use the computer, please follow these steps:

1. Temporarily disable the *Validate user name* option. That is, run Folder Guard, choose File - Settings in the menu, and press the Options button on the Startup page. In the dialog box, clear the *Validate user name* check box.
2. Exit Folder Guard and logoff. When the logon prompt appears on the screen, enter the new user name and password (it will be accepted, since the *Validate user name* option of Folder Guard is OFF now). Continue the logon process until the Desktop for the new user is shown.
3. Now re-enable the *Validate user name* option (see step 1 above).



Appendices: **How to delete a user account**

If you use Windows 98, you can manage the user accounts with Control Panel - Users command of Windows. Alternatively, you can delete user accounts manually, following these steps:

1. Suppose you want to delete resources associated with the user name **John**. Logon to the computer as some other user, who has full access to all folders and other resources.

2. Run RegEdit.exe and find the following key:

HKEY_LOCAL_MACHINE\ Software\ Microsoft\ Windows\ CurrentVersion\ ProfileList\ **John**

If this key does not exist, go to step 4. Otherwise, make a note of the value of the variable *ProfileImagePath*, if any. It contains the DOS path to the folder in which the profile for this user is stored (it is *C:\Windows\Profiles\John* by default).

3. With Windows Explorer, delete the user profile folder, as determined in step 2, if the folder exists.

4. Delete the **John** subkey of the ProfileList key in the Registry and exit the Registry Editor.

5. Run Notepad (or any other text editor, but not a word processor!) and open the file System.ini, located in the Windows folder.

6. Find the [Password Lists] section in this file and make a note of the value of the variable **John** in this section. It contains the path to the password list file associated with the user John. (*C:\WINDOWS\JOHN.PWL* by default). Delete the *JOHN=C:\WINDOWS\JOHN.PWL* line from the [Password Lists] section and save the System.ini file. Exit Notepad.

7. With Windows Explorer, find and delete the **JOHN.PWL** file determined in step 6.

8. Delete all other files and/or folders you might have previously allocated for use by the user John.



Appendices: How to backup the Windows Registry

The Registry is a very important part of Windows. It is a place where Windows stores information about hardware and software installed on your computer. Whenever you add or remove a device, install a new software product, change a device settings, modify options for a program - all these changes (and others, too) are written by Windows into the Registry.

Physically, the Registry consists of a number of files. To backup the Registry, you must backup its key files. The following two files are the core components of the Registry; they are always present in the Windows folder (usually, C:\Windows):

System.dat

contains mostly information about the hardware configuration of the computer.

User.dat

contains mostly information about the software installed on the computer.

In addition, if user profiles are enabled, the user-specific parts of the Registry are stored in separate

User.dat files, one per user. (These files are usually located in folders C:

\Windows\Profiles\<user_name>.) Whenever a user logs on the system, Windows restores the specific settings for this user by merging the user-specific User.dat file with the *generic* User.dat file.

It is important to backup the Registry before making any significant changes to your system. You can backup the Registry by making copies of the files mentioned above. If you need to restore the Registry, replace its existing files with the copies you have saved during backup. You can manually perform these operations, after rebooting Windows in the command prompt mode, or you may wish to use our *free*

Simple Registry Backup/Restore Utility, available for *free* download from our web site:

<http://www.winability.com/>

For more information about the Registry, please consult your Windows documentation.



Appendices: How to enable the logon prompt on a stand-alone computer

*Please note that features described here are built-in into Windows and are **NOT provided by Folder Guard**. The information below is provided only for reference purposes for your convenience. If you have any questions regarding the features described below, you should contact the technical support department of Microsoft, NOT WinAbility.Com.*

If you are going to enable the user profiles, you don't need to do anything else to force Windows show the logon prompt at startup: the prompt will be enabled automatically as soon as you enable the profiles.

If, however, you are not going to employ the user profiles, you can enable (or disable) the logon prompt by resetting the logon password. To reset the logon password, simply delete the password list file (of the type PWL), located in the Windows folder. If there are several PWL files in this folder, you can determine the name of the user who is currently logged onto the computer by running RegEdit.exe and examining the variable *Current User*, under the following key:

HKEY_LOCAL_MACHINE\ System\ CurrentControlSet\ control

After you have deleted the PWL file, restart Windows. When the logon prompt appears on the screen, enter a non-empty password, to keep the logon prompt appearing again whenever you restart Windows.

If no logon prompt is shown at this point, make sure you have installed at least one network-related component of Windows, such as Dial-Up Networking.

To disable the logon prompt, leave the password field in the logon prompt empty, when Windows prompts for it for the first time. If the user profiles are also disabled, Windows will not show the logon prompt next time you boot it up.



Appendices: How to enable user profiles on a stand-alone computer

*Please note that features described here are built-in into Windows and are **NOT provided by Folder Guard**. The information below is provided only for reference purposes for your convenience. If you have any questions regarding the features described below, you should contact the technical support department of Microsoft, NOT WinAbility.Com.*

This section describes how to enable user profiles on a stand-alone computer, not connected to a network. For complete information please refer to the Windows Resource Kit.

- Step 1. Backup the registry, in case of emergency.
- Step 2. Prepare the Desktop: arrange folders and shortcuts on the Desktop as you want them to appear for each user when the user first logs on to Windows under his or her own name. Move those items which you don't want to be used by other users into a separate folder somewhere on your hard disk; later, you will be able to return them to your personal Desktop, when you log on under your own name. Do the same with the Start Menu; its contents is maintained by Windows (usually in the C:\Windows\Start Menu folder).
- Step 3. Enable user profiles: Open the Control Panel and double-click on *Passwords*. In the dialog box, select the *User Profiles* page and check the *Users can customize their preferences and desktop settings* option. Also check both options in the *User Profile settings* group, on the same page. Press OK and restart Windows.
- Step 4. Create user profiles: When Windows reboots, enter your name and password at the logon prompt and let Windows save your personalized settings for future use. Log off and repeat this procedure for all other users of your computer. You may also wish to create a profile for a *Guest* user, just in case.
- Step 5. Restore your Desktop and Start Menu: log on under your own name and move all items you've saved while performing Step 2 back to your Desktop and Start Menu.

Now you can run Folder Guard and set up folder attributes and permissions as desired for each user.

See also:

[How do I protect user profiles?](#)



Appendices: How to disable the Default user account

*Please note that features described here are built-in into Windows and are **NOT provided by Folder Guard**. The information below is provided only for reference purposes for your convenience. If you have any questions regarding the features described below, you should contact the technical support department of Microsoft, NOT WinAbility.Com.*

Although Folder Guard offers an option to disable the Cancel button on the logon prompt and thus lets you prevent the use of the Default user account, sometimes it's desirable to use the following *quick-and-dirty* method of preventing the use of the Default account:

- Enable and create the user profiles, if you have not done so yet. If you try this method without enabling the user profiles, you will effectively **lock out yourself of your computer!** (If this happens, remember that you can always restore access to your computer by booting it up in the *safe* mode and fixing the error). **Make sure you know how to reboot the computer in the safe mode before attempting to implement this method!**
- Run Registry Editor (RegEdit.exe). Please be **very careful** when using this tool, because if you do something wrong with it, you may end up reinstalling Windows from scratch!
- Find the following key:

```
HKEY_USERS
  .Default
    Software
      Microsoft
        Windows
          CurrentVersion
            Run
```

- Create a new *string* value under this key (in the *right* pane of the Registry Editor window). Rename it to *DisableAccount* (or use some other name, if you like), and specify the following command as its Value Data:

```
rundll.exe user.exe,EXITWINDOWS
```

From now on, whenever someone logs on as the default user, the Windows session will be immediately terminated. The other user accounts may be used as usual.

If you ever need to logon as the default user, you can do so by booting the computer up in the *safe* mode.



Appendices: How to disable Ctrl+Esc during logon

*Please note that features described here are built-in into Windows and are **NOT provided by Folder Guard**. The information below is provided only for reference purposes for your convenience. If you have any questions regarding the features described below, you should contact the technical support department of Microsoft, NOT WinAbility.Com.*

There is a bug in Windows 95 that lets the user run Task Manager before logging on to Windows, by pressing Ctrl+Esc while the logon prompt of Windows is displayed on the screen. This can be a problem since Task Manager can further be used to run programs (including Explorer) before logging on to Windows.

To prevent this from happening, you may wish to make use of the Disable system keys during logon option (choose **File - Settings - Startup - Options** to display this dialog.)

Or, this problem can be solved in one of the following ways:

- Method 1. The executable file for Task Manager is TaskMan.exe, it is installed by default in the C:\Windows folder. Rename this file (to *TM.exe*, for example), or move it into some other folder, or simply delete it if you are not going to use it.
- Method 2. Add the following line to the [boot] section of the System.ini file:

```
taskman.exe=*
```

Tip You can assign an arbitrary program to be run when the user presses Ctrl+Esc during Windows logon, by specifying the program's file name after the "=" character in the line above. For example, to let Windows Notepad be accessible in this fashion, specify:

```
taskman.exe=Notepad.exe
```



Appendices: How to disable Ctrl+C during Windows boot-up

*Please note that features described here are built-in into Windows and are **NOT** provided by Folder Guard. The information below is provided only for reference purposes for your convenience. If you have any questions regarding the features described below, you should contact the technical support department of Microsoft, NOT WinAbility.Com.*

By default, Windows lets anyone press the Ctrl+C keys during its initial booting phase and stop the booting. If the user is knowledgeable enough about the MSDOS mode, s/he can then examine the contents of all your drives and folders, since Folder Guard does not protect them in the MSDOS mode. To prevent this from happening, you can reconfigure your computer to disable the Ctrl+C keys in the MSDOS mode.

First, make a backup copy of the C:\CONFIG.SYS file (just in case something goes wrong) by copying this file onto your emergency startup disk. Also, make sure that you can actually use the startup disk to boot your computer into the MSDOS mode.

Open C:\CONFIG.SYS with Notepad and add the following line at the very beginning of the file:

BREAK=OFF

Now save the file and try to reboot the computer and see how it works. For more information please refer to the file Config.txt, installed by Windows in your C:\Windows folder.

Note that this setting also disables Ctrl+C for all programs running in the MSDOS mode.



Appendices: How to restrict the *Restart in MS-DOS mode* command

*Please note that features described here are built-in into Windows and are **NOT provided by Folder Guard**. The information below is provided only for reference purposes for your convenience. If you have any questions regarding the features described below, you should contact the technical support department of Microsoft, NOT WinAbility.Com.*

If you would like to prevent users from using the *Restart in MS-DOS mode* command (one of the shut down options offered by Windows), here is the procedure:

1. Run Windows Explorer and open the folder in which Windows is installed (we'll assume that it is C:\Windows)
2. Find the following item: *Exit To Dos* (Shortcut to MS-DOS Program). Highlight it.
3. Make a backup copy of this file (just in case). That is, while it is highlighted, press Ctrl+C, then press Ctrl+V. This should create a new file named *Copy of Exit To Dos*. If anything goes wrong, you can use it to restore the original file.
4. Now, while *Exit To Dos* is selected, press Alt+Enter to open its Properties dialog. Select the *Program* tab.
5. Change the *Cmd line* field to read as follows:

C:\Windows\Win.com
6. Press OK to close the dialog.

Now, try to restart the computer in the MS-DOS mode (by choosing *Shut down* on the Start menu and selecting the *Restart in MS-DOS mode* option). The screen should go black for awhile, but eventually Windows should appear again, not MS-DOS prompt.

Note: This change affects all users of the computer.



Appendices: A Crash Course in System Policies

*Please note that features described here are built-in into Windows and are **NOT provided by Folder Guard**. The information below is provided only for reference purposes for your convenience. If you have any questions regarding the features described below, you should contact the technical support department of Microsoft, NOT WinAbility.Com.*

System Policies is an optional component of Windows which you can use to enforce some Windows settings on the per-user basis. For complete information on installing and using System Policies, consult the Windows Resource Kit.

To make System Policies work on your computer, you must first install them on your computer:

- Insert your Windows CD into the CD-ROM drive.
- Open Control Panel, double click on *Add/Remove Programs*, select the *Windows Setup* page, and click on *Have disk* button.
- Enter the following path into the dialog box: D:\ADMIN\APPTOOLS\POLEDIT\POLEDIT.INF (replace D: with the drive letter that designates your CD-ROM) and click on OK.

The System Policy Editor uses files of two kinds: template files (extension ADM) and policy files (extension POL). Template files contain information that guides the System Policy Editor in modifying the Registry in response to your commands. Policy files contain the restrictions you are setting up for each user and computer.

After you have installed System Policies, run the System Policy Editor, choose the Options - Template command in its menu, and select the template file you want to be active (usually it is ADMIN.ADM; this file is installed in the C:\Windows\INF folder).

Now create a policy file:

- Run the System Policy Editor and choose File - New in its menu.
- Use commands of the System Policy Editor to create entries for users of your computer and set up their policies.
- Choose File - Save and save the file. You may wish to name the file CONFIG.POL and save it in the Windows folder (usually, C:\Windows), although you are free to select other name and location for this file.

Finally, you must activate the policy file you have just created. On a stand-alone computer, do the following:

- Run the System Policy Editor and choose File - Open Registry in its menu.
- Open the *Local Computer* item and find the following entry: Network - Update - Remote Update. Check this checkbox.
- In the *Settings for Remote Update* area (at the bottom of the same dialog box), specify the following information:

Update Mode: *Manual*

Path for manual update: (enter here the path to the Policy file you wish to be active; for example: C:\WINDOWS\CONFIG.POL).

- Press OK to close the dialog and choose the File - Save command in the menu to save the changes to the Registry.

Note: The path to the active policy file is stored in the Registry in the variable *NetworkPath*, under the key:

HKEY_LOCAL_MACHINE\ System\ CurrentControlSet\ Control\ Update

From now on, whenever a user logs on to Windows, the restrictions you have specified in the policy file will be applied to the user's settings.



Appendices: MSDOS.SYS: Useful commands

*Please note that features described here are built-in into Windows and are **NOT provided by Folder Guard**. The information below is provided only for reference purposes for your convenience. If you have any questions regarding the features described below, you should contact the technical support department of Microsoft, NOT WinAbility.Com.*

In Windows, MSDOS.SYS is a text file which may be used to control the boot process. It contains a [Paths] section that lists the locations for other Windows files (such as the Registry) and an [Options] section that you can use to control the boot process.

If you want to change any of the values in the MSDOS.SYS file, you can use any plain text editor (like Notepad).

IMPORTANT: Before you edit the MSDOS.SYS file, you should first make a backup copy of it. The original file is located in the root folder of your boot drive. If you delete the MSDOS.SYS file, your computer will not start. Also, make sure you can boot your computer with a floppy disk, and that the disk contains a plain text editor - one you can use to modify the MSDOS.SYS file, if anything goes wrong.

The [Options] section can contain the following settings:

BootDelay=<Seconds> Default: 2

Sets the amount of time the *Starting Windows* message remains on the screen before Windows continues to boot. If this setting is 0, then you will NOT be able to press the F8 key when *Starting Windows* appears to invoke the Startup menu.

BootSafe=<Boolean> Default: 0

A setting of 1 forces your computer to boot in safe mode.

BootGUI=<Boolean> Default: 1

A setting of 1 forces the loading of the GUI interface. A setting of 0 disables the loading of the GUI interface.

BootKeys=<Boolean> Default: 1

A setting of 1 enables the use of the function key boot options (that is, F4, F5, F6, and F8). A setting of 0 disables the use of these function keys during the boot process.

Note: A setting of BootKeys=0 overrides the use of BootDelay=n.

BootMenu=<Boolean> Default: 0

A setting of 1 enables the Startup menu. If this setting is 0, then you must press the F8 key when *Starting Windows* appears to invoke the Startup menu.

BootMenuDefault=<Number>

Default: 1 if the system is running correctly, 3 if the system hung in the previous instance.

Use this setting to set the default menu item for startup.

BootMenuDelay=<Number> Default: 30

This setting is used to set the number of seconds your system will pause on the Startup menu. If the number of seconds counts down to 0 without intervention, the BootMenuDefault is activated.

NOTE: This option will not function unless BootMenu=1 has been specified.

BootMulti=<Boolean> Default: 0

A setting of 0 disables the multi-boot option. (For example, with a setting of 0 you cannot boot your previous operating system.) A setting of 1 enables the F4 and F8 keys to boot your previous operating system.

Note: This setting is set to 0 by default to prevent you from inadvertently starting MS-DOS and damaging data by running a disk utility that does not recognize long file names.

BootWarn=<Boolean> Default: 1

A setting of 0 disables the safe mode boot warning message and the Startup menu.

BootWin=<Boolean> Default: 1

A setting of 1 forces Windows to load at startup. A setting of 0 disables Windows as your default operating system (this is useful only if you have MS-DOS version 5.x or 6.x on the computer).

Note: Pressing F4 inverts the default only if BootMulti=1. (For example, pressing the F4 key with a setting of 0 forces Windows to load.)

DBLSpace=<Boolean> Default: 1

A setting of 1 allows the automatic loading of the DBLSPACE.BIN file. A setting of 0 prevents the automatic loading of this file.

DRVSpace=<Boolean> Default: 1

A setting of 1 allows the automatic loading of the DRVSPACE.BIN file. A setting of 0 prevents the automatic loading of this file.

Note: Windows uses either Dblspace.bin or Drvspace.bin if either is present in the root folder of the boot drive at startup. To prevent a compression driver from being loaded at startup, use both settings in the MSDOS.SYS file. For example:

```
DBLSpace=0
DRVSpace=0
```

Logo=<Boolean> Default: 1

A setting of 1 forces the default Windows logo to appear. A setting of 0 prevents the animated logo from being displayed.

Network=<Boolean> Default: 0

A setting of 1 means the network was installed and adds *Safe mode with network support* as an option on the Windows Startup menu.

The MSDOS.SYS file also contains a section with seemingly useless information. These entries are required for compatibility with programs that expect MSDOS.SYS to be at least 1024 bytes in length. For example, if an anti-virus scanner detects that MSDOS.SYS is smaller than 1024 bytes, it may assume that a virus has infected this file.



FAQ (Frequently Asked Questions)

[How do I enter the Registration Code?](#)
[Will Folder Guard slow down my computer?](#)
[Will Folder Guard encrypt my files?](#)
[My password is not accepted...](#)
[How do I logon as the *default* user ?](#)
[How do I determine the status of the protection?](#)
[Which modules should or should not be made "trusted"?](#)
[How do I rename a folder in the Folder Guard window?](#)
[How do I hide drive icons?](#)
[How do I prevent formatting of the drives?](#)
[How do I protect folders on the Desktop?](#)
[How do I protect Start Menu?](#)
[How do I protect Control Panel?](#)
[How do I protect the Windows folder?](#)
[How do I protect user profiles?](#)
[How do I protect folders on removable drives?](#)
[Can I hide the *My Computer* folder?](#)
[How can I get printed documentation for Folder Guard?](#)
[Troubleshooting hints](#)



FAQ: How do I enter the Registration Code ?

You are prompted to enter your name and Registration Code during the installation procedure.

Alternatively, choose the Help - Registration Information command of Folder Guard, and click on the *Register* button in the dialog box.

When entering the registration information, be sure to spell your name in exactly the same way as it appears on your Registration Acknowledgment. If the latter does not contain your name, you should enter your name using the same spelling as when you placed the order (that is, if you ordered with a credit card, spell it as it appears on the card).

Related topics:

[This is *Try Before You Buy* software](#)

[What do you get when you order a license for Folder Guard](#)

[How to order a license for continued use of Folder Guard](#)



FAQ: Will Folder Guard slow down my computer?

Folder Guard is designed to perform the protection with minimum overhead. You will not notice any decrease of performance of your computer, unless you assign separate attributes to thousands of files and folders. If you are concerned about the performance, try to reduce the number of items which have non-default attributes. For example, instead of assigning the *hidden* attribute to a group of files or subfolders of the same parent folder, make the parent folder *hidden* instead.



FAQ: Will Folder Guard encrypt my files?

No. Folder Guard does NOT encrypt or otherwise modify your files in ANY WAY. Folder Guard protects your files *dynamically*, that is, it intercepts requests from other programs to open files or list the contents of folders, and then allows or rejects such requests according to the settings set by the administrator. The files and folders themselves remain undisturbed during this process, in their original condition.

This means, for example, that if your system crashes while Folder Guard is performing the protection, there is no risk of losing your important data because of Folder Guard. If necessary, you can always deactivate the protection (or even uninstall Folder Guard, for that matter), and you will get full access to all your files and folders back.



FAQ: My password is not accepted...

First, keep in mind that the passwords used by Folder Guard are case-sensitive, so you should enter them in the same letter case each time. If a password is not accepted, it might be because the CapsLock key is accidentally turned ON, or, if you use an international version of Windows, a keyboard layout for a different language is selected. Also, the password to turn off the protection (the *Master* password) is NOT the same as the *Administrator's* password; you cannot interchange them, unless you have specifically chosen the same word for both of these passwords.

If you are still experiencing this problem, you need to set up the password(s) again.

To set up the Master password , or a password for any particular file or folder, or the logon password for the Default User, run Folder Guard and use its appropriate commands.

If you cannot run Folder Guard because your Administrator's password is not accepted, you must delete the file FGuard.FGP, located in the folder from which you run FGuard.exe (usually it is the same folder where you installed Folder Guard).

If you cannot delete the FGuard.FGP file (for example, because it is protected by Folder Guard), you must reboot Windows in the *safe* or *command prompt only* mode. The protection is not enabled in either of these modes, so you will be able to delete FGuard.FGP.



FAQ: How do I logon as the *default* user ?

You can logon as the *default* user if you press the Cancel button on the Windows or network logon prompt (provided that you have not restricted this method of using the computer with Folder Guard).



FAQ: How do I determine the status of the protection?

If you are running Folder Guard, the status of the protection is indicated by the state of the *Toggle*



Protection button in the toolbar: . If this button is pressed, the protection is currently enabled. If the button is not pressed, the protection is currently disabled.

If you are not running Folder Guard, you can determine the status of the protection by running FGKey.exe (represented by the *Toggle Protection* command in the Windows Start Menu): If you are prompted to enable the protection - it is currently not enabled. If, however, you are prompted to enter a password to disable the protection, the protection is currently in effect.



FAQ: Which modules should or should not be made "trusted"?

You may wish to add to the Trusted Modules list the names of the system tools such as anti-virus utility, disk defragmenter, disk scanner, backup utility, etc. If you do so, you won't have to manually disable the protection before running such tools, since they will have full access to all your folder and files anyway, as if Folder Guard was not present in your system at all.

If you plan on making the Windows folder *read-only*, you will need to add the **REGSVR32** module to the Trusted Modules list. This module is used by Windows to access the Registry, which files are stored in the Windows folder and must be fully accessible in order for Windows to operate properly.

The following modules should **NOT** be made trusted:

Explorer : If you add this module to the trusted modules list, Windows Explorer will be allowed full access to all files and folders, even to those you have marked as hidden or restricted with Folder Guard!

KERNEL32 : If your computer is connected to a network and you *share* some of your drives, this module is used by Windows to provide information about your files and folders on the shared drives over the network. If you make it trusted, all your files and folders will be accessible to other network users.

MPREXE : This module is used to access network resources. If you make it trusted, all network drives will be accessible to the user.



FAQ: How do I rename a folder in the Folder Guard window?

You cannot rename or otherwise manipulate (copy, move, delete) folders or files with Folder Guard. If you want to rename/copy/move/delete a folder, you must do it with Explorer. To force Folder Guard to update its listing of folders in the main window, use its View - Refresh command (or press F5).



FAQ: How do I hide drive icons?

Windows treats the root folders of the drives and drives themselves as separate items. When you use Folder Guard to assign the *Hidden* attribute to a drive, you are hiding the root folder of the drive, but not the drive itself.

To hide the drive icons, use the Edit - Permissions command of Folder Guard.



FAQ: How do I prevent formatting of the drives?

Folder Guard allows you to prevent formatting of the local drives. Even more, you can allow the formatting for some users and prevent it for others.

To set up the desired options, use the Edit - Permissions command of Folder Guard and select the *Drives* page of the Permissions dialog box. Then mark the drive letters in the *Formatting* area according to your preferences.



FAQ: How do I protect items on the Desktop?

You can restrict access to any *real* folder (that is, any folder in which you can store arbitrary files, shortcuts, etc., in contrast to the *virtual* folders, such as *My Computer*, *Dial-Up Networking*, etc.), as well as to *real* shortcuts and files on your Desktop in the same way as you do it for any other files or folder: by running Folder Guard and assigning appropriate attributes to the items. (To protect files and shortcuts you may need to add them to the list of folders shown in the Folder Guard window, using the *Edit - Add File* command).

The only trick when protecting the Desktop items is to determine the correct locations of these items in the file system of your computer.

By default, Windows stores the Desktop items in the *C:\Windows\Desktop* folder on your disk. If the user profiles are not enabled, this folder is used for all users of the computer. If the profiles are enabled, however, then for those users for whom you have chosen to create separate desktops, their desktops are stored in the user-specific folders. For example, for user *John* the desktop items are stored in the folder *C:\Windows\Profiles\John\Desktop*.

Keep in mind, however, that Windows can be configured so that some other desktop folders are used for a particular user. To determine these locations, you must logon as that user, run RegEdit.exe, and examine the values of the following key in the Registry:

HKEY_CURRENT_USER\ Software\ Microsoft\ CurrentVersion\ Explorer\ User Shell Folders

Note also that you may find out in the same way the locations of other user-specific folders, like **Start Menu**, **Favorites**, etc. [Such folders and their items can be restricted with Folder Guard, too!](#)

See also:

[How do I protect Start Menu?](#)

[How do I protect Control Panel?](#)

[How to enable user profiles on a stand-alone computer](#)

[How do I protect user profiles?](#)

[How do I protect the Windows folder?](#)



FAQ: How do I protect Start Menu?

By default, Windows stores the Start Menu items in the *C:\Windows\Start Menu* folder on your disk. If the user profiles are not enabled, this folder is used for all users of the computer. If the profiles are enabled, however, then for those users for whom you have chosen to create separate desktops, their Start Menu items are stored in the user-specific folders. For example, for user *John* the desktop items are stored in the folder *C:\Windows\Profiles\John\Start Menu*.

So, to restrict access to Start Menu, use Folder Guard to restrict access to the appropriate folder(s).

Note: Windows can be configured so that some other folders are used for a particular user. To determine these locations, you must logon as that user, run RegEdit.exe, and examine the values of the following key in the Registry:

HKEY_CURRENT_USER\ Software\ Microsoft\ CurrentVersion\ Explorer\ User Shell Folders

See also:

[How do I protect folders on the Desktop?](#)

[How do I protect Control Panel?](#)



FAQ: How do I protect Control Panel?

One way is to use the permissions offered by Folder Guard (see the [Edit - Permissions](#) command).

An alternative method is to restrict access to the CPL files, located usually in the C:\Windows\System folder. Each of the CPL files is a module responsible for one or several groups of settings of Control Panel:

Module	Settings
ACCESS.CPL	Accessibility Options
APPWIZ.CPL	Add/Remove Programs
DESK.CPL	Display
INETCPL.CPL	Internet
INFRARED.CPL	Infrared
INTL.CPL	Regional settings
JOY.CPL	Game Controllers
MAIN.CPL	Fonts, Keyboard, Mouse, PC Card (PCMCIA), Printers
MMSYS.CPL	Sounds
MODEM.CPL	Modems
NETCPL.CPL	Network
PASSWORD.CPL	Passwords
POWERCFG.CPL	Power Management
SYSDM.CPL	System
TELEPHON.CPL	Telephony
THEMES.CPL	Desktop Themes
TIMEDATE.CPL	Date/Time

(You may have other CPL files, or not all of the files listed above, depending on the software installed on your computer).

So, to restrict access to Control Panel, use Folder Guard to restrict access to the appropriate CPL files, by assigning the *no access* attribute to them.

See also:

[How do I protect folders on the Desktop?](#)

[How do I protect Start Menu?](#)



FAQ: How do I protect the Windows folder?

Special care must be exercised when protecting the Windows folder (that is, the folder in which Windows is installed, usually C:\Windows). Do **not** apply the *no access* or *hidden* attributes to this folder, because this will prevent Windows from working! (Windows is just designed so that this folder **must** be accessible and visible, at least partially).

First of all, **backup the Registry before trying to restrict the Windows folder!** It takes only a couple of minutes, but it will save you hours of your time if anything goes wrong (and believe me, there *are* things that may go wrong when you are trying to protect this folder).

You may try to make the Windows folder *read-only*, however you should be aware that Windows and some other programs need to be able to write information into some files kept in this folder in order to operate properly. For example, the System.dat and User.dat files (the files used to store the contents of the Registry), are kept in this folder and are constantly updated by Windows while it is operating. As a result, if you mark this folder *read-only* with Folder Guard, a registry corruption error may be reported, and Windows may fail to work properly. **To remedy this problem, make sure that the REGSVR32 name is added to the trusted modules list.** (This module is used by Windows to write information into the registry files).

Other programs may also need to write information into the Windows folder in order to work correctly. Also, most of the old 16-bit applications store their configuration data in the win.ini or other *.ini files. For example, the old-style File Manager, that is still available in Windows 95/98 as *winfile.exe*, uses the file *winfile.ini*, in the Windows folder, to keep its configuration data between sessions. To allow such programs access their configuration files, you may wish to set up special filters. In case of File Manager, create the following filter:

Apply to files: winfile.ini	Except for files:
Apply to folders: C:\Windows	Except for folders:
Apply to modules: winfile	Except for modules:

and assign the *full access* attribute to it. This would make the C:\Windows\winfile.ini file fully accessible to File Manager itself (since its module name is **winfile**). If some other module attempts to access this file, the filter would not apply, and the *read-only* attribute of the C:\Windows folder itself would prevent any modifications to this file.

You may need to set up similar filters to allow other programs full access to their respective configuration files in the Windows folder.

In addition, Windows uses some of the subfolders of the Windows folder to store its data, so you will need to mark such subfolders with the *full access* attribute. Examples of such subfolders are: Application Data, Cookies, Downloaded Program Files, History, msdownld.tmp, TASKS, TEMP, Temporary Internet Files, and others, depending on your configuration of Windows.

You may also try to restrict the visibility of the contents of the Windows folder by marking it *restricted* with Folder Guard. This may or may not work well for you, depending on Windows components and other software installed on your machine, so you will need to test your protection configuration well.

When restricting the visibility of the Windows folder, keep in mind the following:

- Some subfolders of the Windows folder which are used by Windows itself (*System*, *Fonts*, *Profiles*, *Temp*, etc.) must be marked *visible*. You may try to mark some of them as *read only*, though, but whether it works depends on other settings of Windows.
- If you mark the Windows folder *restricted*, you may not be able to access the programs kept in this folder (including Explorer.exe, Notepad.exe, etc.). You should review the contents of this folder with Explorer before restricting it, and move the files which you want to be used into some other folder. If you do so, you may need to update the shortcuts pointing to those files, too.
- If you restrict the Windows folder for the *default* user, and Windows fails to work, you may try to restrict this folder for the *non-default* users instead.

See also:

[How do I protect folders on the Desktop?](#)

[How do I protect Start Menu?](#)

[How do I protect Control Panel?](#)

[How to enable user profiles on a stand-alone computer](#)

[How do I protect user profiles?](#)



FAQ: How do I protect user profiles?

Care must be exercised when restricting access to the folders in which user's profiles are stored. For example, for the user *John* the profile is usually stored in the folder *C:\Windows\Profiles\John*. The exact location of such a folder can be determined by examining the value of the variable *ProfileImagePath*, stored in the Registry under the key:

HKEY_LOCAL_MACHINE\ Software\ Microsoft\ Windows\ CurrentVersion\ ProfileList\ John

A problem may occur if you restrict access to such folders for the *default* user and you do not employ at the same time the logon monitoring feature of Folder Guard. As a matter of fact, before a user logs onto the computer, Folder Guard enables the restrictions set up for the default user. This means that if you have restricted access to the user profile folders for the default user, these folders may not be accessible while the logon prompt is displayed and processed on the screen. This in turn means that the users for whom the profiles are restricted may not be able to logon to the computer.

This problem does not occur if you use the Monitor user logon feature: Folder Guard is designed so that it allows full access to the profiles of all users while the logon process is taking place. This does not compromise the security, since as soon as the user logs onto the machine, Folder Guard enables the restrictions set up for this user.

Summary: do not restrict the *default* user's access to the folders in which other user's profiles are stored, unless you have enabled the logon monitoring feature of Folder Guard.

See also:

[How do I protect folders on the Desktop?](#)

[How do I protect the Windows folder?](#)



FAQ: How do I protect folders on removable drives?

Normally, Folder Guard does not protect folders on the removable drives. Folder Guard lets you protect only the root folders on such drives, and thus specify the access rights to the drive as a whole.

Beginning with version 4.08, Folder Guard offers you an option that lets you protect folders on the removable drives (such as SCSI or ZIP drives, but **not** floppy or CD-ROM ones), as well.

To use this option, first make sure the removable disk you would like to protect is inserted into the drive. (Below we refer to this particular disk as the *original* one, that is the disk you use when you are setting up the attributes of its folders.) Run Folder Guard, choose the File - Options command, go to the *Misc* page, and select the *Allow protection on removable drives* option. Now set up the attributes of folders on the removable disk as desired, in the same way as you would do it for a regular, *fixed*, drive.

From that time on, whenever the protection is enabled, and the same (original) disk is inserted into the drive, its folders are protected by Folder Guard, as usual. If you insert some other disk into the same drive, that has a different structure of folders than the original disk, the folders on such disk will **not** be protected, unless they happen to have the same paths as the folders on the original disk.

A problem may occur if you run Folder Guard and some other disk (not the original one) is inserted into the drive. In such a situation, while reading the active FGA file and not finding the protected folders on the disk, Folder Guard assumes that you might have renamed or moved the folders and prompts you to specify their new locations. To deal with this problem, when the first such prompt appears on the screen, remove the *wrong* disk from the drive, and insert the original disk into the drive instead. Then press the OK button on the prompt, to let Folder Guard continue reading the FGA file. At the end of the initializing, use the View - Refresh command (or simply press F5) to force Folder Guard to re-initialize its information, this time using the *correct*, original disk.



FAQ: Can I hide the My Computer folder?

Unfortunately, Windows does not provide a way to hide this folder alone. Instead, you may wish to hide drive icons shown in this folder, by using the Edit - Permissions command of Folder Guard.

If you assign the *Hidden* attribute to *My Computer* using Folder Guard, this attribute will be applied to the root folders of the drives, but not to *My Computer* itself. This is a limitation of the current implementation of Windows.



FAQ: [How can I get printed documentation for Folder Guard?](#)

The documentation for Folder Guard is available only in the on-line form - as the Help file you are reading now.

You can print out the Help, though: just press the *Print...* button in the Help Topics dialog box, (displayed after you click the Contents button while browsing Folder Guard Help).



FAQ: Troubleshooting information

This section contains assorted information you may find useful when solving problems with Folder Guard. **Be very careful when editing the Registry with Registry Editor (RegEdit)!**

1. If you encounter a problem with Folder Guard which **vanishes after you use the *Toggle Protection* command** to turn the protection off and then back on, try to use the *Compatibility Mode* option available on the *Startup* page of the *Settings* dialog box. The *logon monitoring* feature will not work in this case, but if all you need is the protection of folders, this procedure should do the job.
2. If you use **Norton CrashGuard**, and your computer hangs when a user logs off, try to turn OFF the *16-bit Crash Protection* option of Norton CrashGuard.
3. If you use **McAfee VirusScan**, and your computer hangs when Folder Guard performs the protection, try to change the VirusScan setting *Scan all files* to *Scan executables only*.
4. If the **resolution of your monitor** can be adjusted **dynamically**, and the appropriate *taskbar icon* is running, an error may occur when you log off and the *logon monitoring* feature of Folder Guard is in effect. This is a known problem, we've been working on a solution. Meanwhile, use the Display properties applet of Control Panel to hide the taskbar icon, and to change the resolution of the display.
5. You attempt to run the main application of Folder Guard, FGuard.exe, but its window does not appear on the screen. This problem might be caused by an incompatibility problem with the taskbar application called **Grip Control Center**, which is used to control the function of Gravis GamePad Pro. If you have this program, you need to disable its icon in order to be able to use Folder Guard. After you have set up the restrictions and closed the Folder Guard window, you may wish to re-enable the taskbar icon of the Grip Control Center.
6. If you have enabled the **logon monitoring** feature of Folder Guard, but your computer **locks up and does not accept any input when the logon prompt is displayed** on the screen, then try the following:
 - a) Reboot the computer in the *safe* mode.
 - b) Run Registry Editor and find the following key:

HKEY_LOCAL_MACHINE\ System\ Services\ VxD\ FGWARD
 - c) Create the following DWORD value under this key:

Name: MiscOption1
Value: 1
 - d) Now try to reboot Windows as usual and see if it makes a difference.
7. If the problem persists, please visit our web site, <http://www.winability.com/>, and make sure that you have the latest version of Folder Guard. Also, check with the Folder Guard FAQ section on the web site, it contains the latest troubleshooting information.
8. If the problem persists, it means that you have some other software or hardware that is incompatible with Folder Guard. Please check with the following list:

- a) Any additional storage devices, like tape or zip drives;
- b) Any other devices which appear as separate drives in the "My Computer" folder;
- c) Any anti-virus software;
- d) Any other software that runs on background (like ZipMagic, etc.);
- e) Is your computer connected to a network?

If you have anything from this list, please try to temporarily disable it and see if it makes the difference. If you've discovered what caused the error, please let us know, by sending email to:

support@winability.com

Error: Cannot open WinAbility.Com web site. It appears that you don't have a web browser on your computer. If you do have a browser, it is not properly configured. Please visit our web site by connecting to the Internet, opening your web browser, and specifying the following address: **<http://www.winability.com/>**

Error: Cannot open this web site. It appears that you don't have a web browser on your computer. If you do have a browser, it is not properly configured.

Error: Cannot send e-mail. It appears that you don't have an e-mail client application on your computer. If you do have an e-mail client, it is not properly configured.

Error: Cannot open this file.

