UltimateGuard™

(Version 2.0 Beta)

Quick Guide

Notices

UltimateGuard™ 2.0 Beta is Pretec's latest security solution for USB flash storage providing real-time antivirus monitoring, military-grade (AES 256-bit) encryption and powerful data recovery function. Since UltimateGuard™ 2.0 Beta comes with the robust protection for mobility data storage; it might take a moment to run the pop-up warning messages due to different system configuration and internet quality. Please be advised the current UltimateGuard™ 2.0 remains a beta version at this stage. Your comments and efforts on trying it will help further improvement for releasing formal version.

ATTENTION:

1. The immediate access control of GoAnywhere may cause system to slow down or temporary non-response.

2. The files and folders encryption of GoAnywhere may temporary non-complete, we strongly suggest that you regularly back up the data to a computer, or other storage media.

3. The immediate virus protection of GoAnywhere detects all access to your USB. When you see a pop-up message requesting grant to activate “FILERECOVERY Main Application” and “licman.exe” of FILERECOVERY, please allow its access for optimized performance.

Table of Contents

Disclaimer of Liability

The software embedded in the product is copyrighted work of several third party providers respectively. C-ONE Technology Corporation ("C-ONE") provides no guarantee or assurance as to the quality or performance of such software. The use of such software is governed by the terms and conditions of End User License Agreement, or the like, which will be provided by correspondent third party provider in digital form that is included in the software. Please do not install the software before you read and agree to the terms and conditions of the End User License Agreement.

C-ONE IS NOT LIABLE FOR ANY DAMAGES SUFFERRED AS A RESULT OF USING, MODIFYING, CONTRIBUTING, OR COPYING THE SOFTWARE. C-ONE IS NOT LIABLE FOR ANY INDIRECT, INCIDENTAL, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGE (INCLUDING LOSS OF BUSINESS, REVENUE, PROFITS, USE, DATA OR OTHER ECONOMIC ADVANTAGE). In no event will C-ONE be liable for damages hereunder in excess of the amount you provided to C-ONE for this product. This indemnity is in lieu of any other indemnity or warranty, express or implied, with respect to patents and copyrights.

The remedies set forth herein are exclusive and the liability of C-ONE for a breach of C-ONE obligations with respect to the Products (including warranty obligations) shall be limited to the actual damages incurred by you, provided that such liability for damages shall not exceed the total amount of the relevant Products to which such breach relates. In addition to the foregoing limitations, in no event shall C-ONE's aggregate liabilities for all claims made by you exceed the aggregate annual amount in respect of all the Products (or any portion thereof) delivered up to the date of any claim.

1. Introduction

UltimateGuard™ 2.0 Beta is Pretec's next-generation complete security solution for USB flash storage that provides comprehensive data protections, including real-time antivirus monitoring, military-grade (AES 256-bit) files and folders encryption, along with professional data recovery function, which not only protects but also ensures your lost data can be retrieved. UltimateGuard™ powerful security solution assures users a worry-free environment where there is no virus attack and data loss possibility, whenever and wherever you use your storage device.

UltimateGuard™ 2.0 Beta provides benefits:

- ✓ **Mobile protection**
  automatically launching protection to safeguard your data no matter what PC it is connected to.
- ✓ **Smart access identification**
  use Whitelisting and Blacklisting and Auto Advisor Tri-Security to allow or block unknown threatening access.
- ✓ **Secure data from malware**
  intelligently protects all your data without configuration.
- ✓ **Highest standard for data encryption**
  simply drag and drop AES 256-bit top secret encryption to ensure seamless protection of your sensitive data.
- ✓ **Easy & professional data recovery**
  recover lost/deleted data, prevent accidental/malicious formats and easily recovery operates even novice users.
- ✓ **Friendly customer experience**
  extremely convenient and intuition use interface design.

2. System Requirements

- 486 or Pentium-class Processor
- 512MB RAM (1GB recommended)
- 50MB free hard disk drive space
- Operating Systems: Windows 7, Windows Vista Service Pack 1 (32-bit only) or later, Windows XP Service Pack 2 or later, Windows 2000 Service Pack 4
- Available USB 2.0 port
- Turn on **use visual styles on windows and buttons** option of system performance

  To modify the system performance options, follow these steps:
  1. Right-click **My Computer**, and then click **Properties**.
  2. Click the **Advanced** tab.
  3. Under **Performance**, click **Settings**.
  4. In the **Performance Options** dialog box, click the **Visual Effects** tab.
  5. Select **Processor scheduling** option, click **OK**.
  6. Click **OK** to close the **System Properties** dialog box.
- UltimateGuard™ drive

3. Getting Started

To launch UltimateGuard™, please plug-in your Pretec USB flash drive and execute “UltimateGuard.exe” in “Pretec_UG” folder in this drive.

Notice!

Reboot Request: If your operating system shown a pop-up message “Find a new device,” followed by a reboot request, please click the “No” button to cancel it.

4. UltimateGuard™ Start

4.1 Start

If UltimateGuard™ is installed, click on "**Start**" button to launch it.

If UltimateGuard™ isn't installed before, click on "**Start**" button to open software installation panel.

4.2 Information

If UltimateGuard™ is installed, click on "**Information**" button to open software installation panel.

If UltimateGuard™ isn't installed before, click on "**Information**" button to open the "UG_QuickGuide.pdf" which will guide you through the process of installation of your drive.

4.3 Minimize

Click on "**Minimize**" button will minimizing the UltimateGuard™ to the task tray. You can click on the UltimateGuard™ icon in the system task tray to active it

again.

4.4 Close

Quit UltimateGuard™.

5. UltimateGuard™ Install Panel

5.1 Install Now

Start to install UltimateGuard™ valued software GoAnywhere into Pretec USB flash drive and FILERECOVERY to your local hard disk drive. Once the installation is finished, the program will be executing itself. Otherwise check if your security software blocks the programs and change its setting to allow it.

After UltimateGuard™ is installed; the "**Install Now**" button will change to "**Start**." Click on it to activate UltimateGuard™. Software instruction please refers to "Software Quick Instruction" cheater, user manual for detail tutor information.

5.2 How to Install

Click on "How to Install" button for a quick install instruction, or find the "UG_QuickGuide.pdf" in "Pretec_UG" folder in your Pretec USB flash drive.

5.3 User Manual

Open the UltimateGuard™ software user manual.

5.4 Description

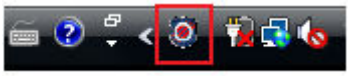
Short descriptions of each buttons on the UltimateGuard™ software installation panel.

5.5 Information

Link to www.ultimateguard.net for product updated information, or find more information on Pretec website www.pretec.com .

5.6 Minimize

Minimize the UltimateGuard™ to the system task tray. Click on the UltimateGuard™ icon in the system task tray to activate it again.



5.7 Close

Quit UltimateGuard™.

6. Software Quick Instruction

UltimateGuard™ includes the topmost advanced technology of GoAnywhere and FILERECOVERY. Simplify software instruction description as follows. For detailed software instructions please refer to user manual in “Pretec_UG” folder in your Pretec USB flash drive.

6.1 GoAnywhere

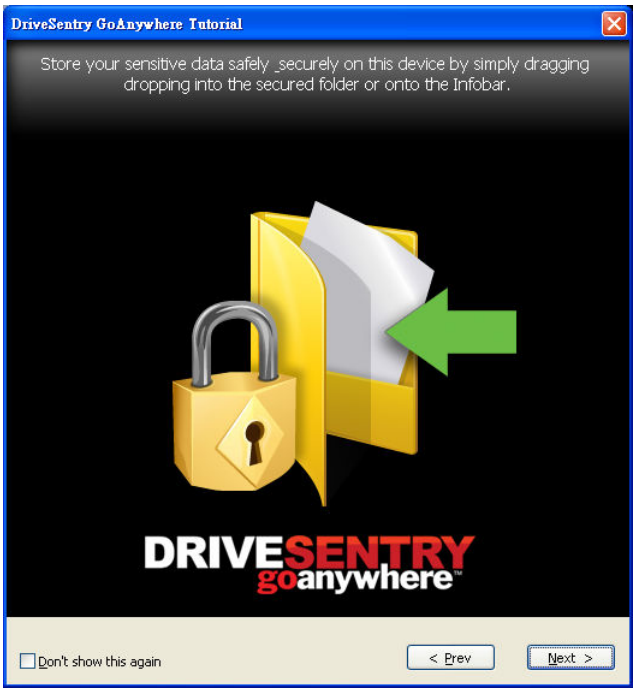
GoAnywhere provides **standalone antivirus protection** and high level **encryption**, so you no longer have to rely on the host system to provide these security methods. GoAnywhere allows you to transfer, transport and work on your data on foreign, third party systems, with confidence and control.

GoAnywhere provides next generation antivirus protection, securing all data upon your device from the very latest threats. It’s new approach to protection combines a **blacklist** of over 1.3 million virus signatures, with a **whitelist** of known trusted programs and program statistics from it’s **Advisor Community**. This Tri-Security program information is stored within its online Advisor database and is used to **automate protection**. GoAnywhere protects your data by monitoring all reads and writes to your device, only allowing access to good programs.

GoAnywhere also provides an easy to use, **secure encryption facility** which enables you to encrypt data **on your device** and **upon the host system** of which your GoAnywhere device is inserted. This will lock your files from prying eyes, even if your system or your device is lost or stolen.

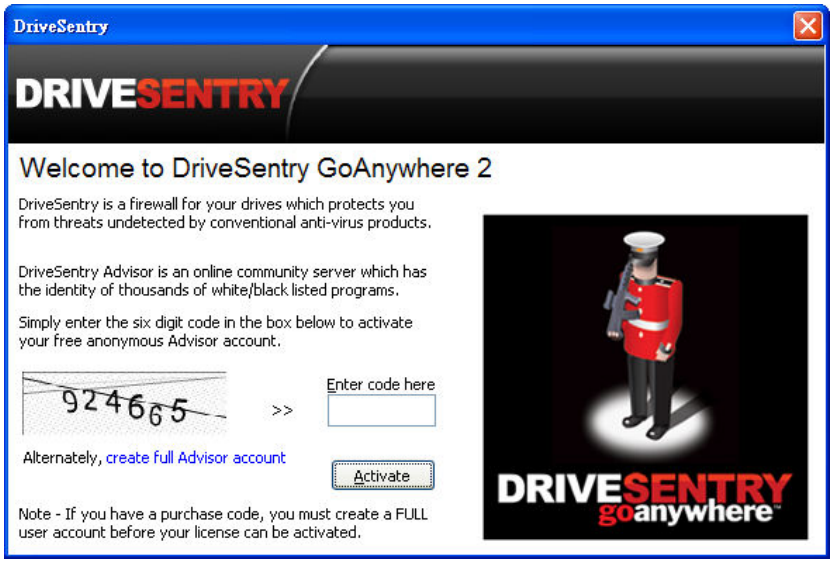
The first time use GoAnywhere

The first time that you insert your device into a system, GoAnywhere will auto launch, presenting you with the following 3 slide tutorial. (Tick the 'don’t show this again' if you do not wish to see the tutorial every time you insert your device).



Welcome Screen - Create an Advisor Account

You need to create an Advisor account in order to access the online Advisor database which holds key program information. This will enable automated protection and access to community advice.



Activate a guest Advisor account

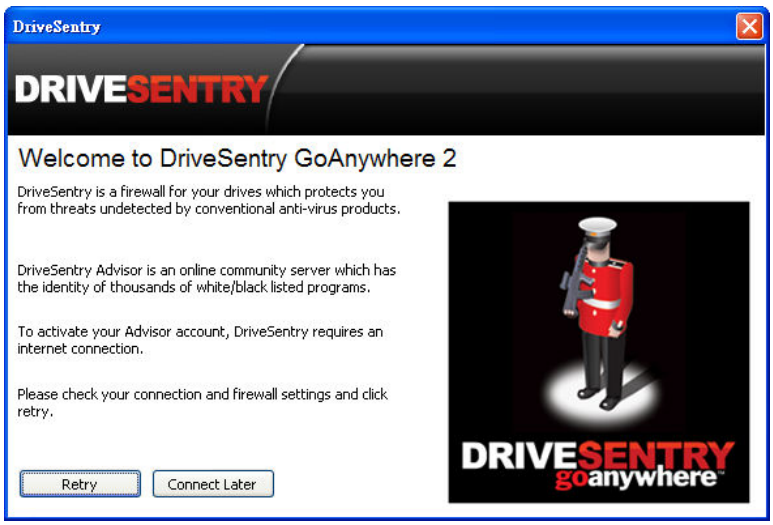
To activate a guest Advisor account, simply enter the six digit security code into the box provided and click the "Activate" Button.

Create Full Advisor account

Select "Create full Advisor account" highlighted in blue and enters your details in the following window and selects "Create".

No Internet Connection Welcome Screen

Important: If you can not connect to the Internet you will not be able to activate your anonymous account or login to your personal user account. In this case you will encounter the screen displayed below which gives you the choice of two options.



Select "Retry" - if a connection can be established this will take you to the normal welcome screen with the option to login.

Select "Connect Later" - this will allow you to login later. When GoAnywhere is

attempting to access Advisor information whilst you are connected to the Internet, you will be prompted to login.

Encryption - Create a secure encryption password

After the creating an Advisor account you will be asked to setup a password in order to make use of the high level encryption facility. This password will be required once per session when encrypting or decrypting files.

Enter your chosen password in the top window, confirm in the bottom window and select 'OK' to continue.

Important: Ensure that you enter a memorable password as there is no way to decrypt encrypted data if you forget this password as GoAnywhere does not store a record of this.

Selecting 'cancel' on the above screen will allow you to create a password later upon encrypting your first file! Please see the next section for information on 'Upgrading'.

Run GoAnywhere

After creating an secure encryption password, all data stored on your removable device will now be protected from malicious attack and you have maximize 5MB free encryption space to use. See the GoAnywhere user

manual section on ugrading to unlimited encryption.

After initial setup the GoAnywhere icon will appear in the task tray and the following information bubble will fade on and off your screen. The GoAnywhere **InfoBar** will also appear on the desktop of the host system.

GoAnywhere - InfoBar

The GoAnywhere InfoBar appears on the host system when you executing the program. The InfoBar provides key information regarding access to your removable drive, including total encrypted files and quick access to key settings and your **'DriveSentry Secured'** folder.

InfoBar Icons


'Purchase GoAnywhere' - Click this icon to upgrade your version of GoAnywhere to enable unlimited encryption.


'Open Secured folder' - Click this icon to open the DriveSentry Secured folder on your GoAnywhere device.


'Turn Compression On/Off' - Click this icon to turn encrypted file compression on or off.

This means that every file that you encrypt will be automatically compressed, enabling you to store more data on your device.


'Display Help file' - Click this icon to access this GoAnywhere help file.

Drag and drop to encrypt files

Simply drag and drop files onto the GoAnywhere InfoBar for **quick and easy encryption**. These files will be automatically encrypted and added to your 'DriveSentry Secured' folder.

GoAnywhere Data Encryption

GoAnywhere boasts an advanced encryption standard known as an AES 256 encryption algorithm. AES stands for Advanced Encryption standard and is used by many Government bodies around the world to keep data safe from prying eyes.

Although GoAnywhere adopts such a high level of encryption, it is easy to use and can be used to encrypt data on both the host system and the standalone device from which GoAnywhere runs. GoAnywhere's encryption facility has been designed for anyone to use. It does not require any configuration other than the creation of a secure password during the initial insertion of your GoAnywhere device. The secure password is only required once per session of use when encrypting or decrypting files.

File encryption process

GoAnywhere - AntiVirus Protection

GoAnywhere provides portable Antivirus protection to ensure that no matter what system you insert your device into, your data will always be protected from the very latest threats.

GoAnywhere protects your data by automatically launching from your device, monitoring all program access. GoAnywhere automates protection by connecting to the Online Advisor server and cross referencing all attempted access against a blacklist of known malware and a whitelist of trusted applications. By doing this GoAnywhere will only allow whitelisted programs to

access your device, automatically blocking and deleting known malware and querying the unknown.

Online Advisor

The online Advisor is an online resource that stores program information and collects Advisor Community data. The online Advisor database stores the following Tri-Security information:

- Advisor Community statistics (access decisions from community of users)
- Whitelist (good programs)
- Blacklist (of over 1.2 million virus identities)

GoAnywhere uses this Tri-Security information to facilitate **Auto Advisor**, through automating read and write access decisions to your device. When a program is not contained within the white or blacklist, Advisor Community information is helpful in assisting you to make independent access decisions based on the responses submitted by fellow users.

Popup Information

The popup window informs you in real-time when a non-trusted program is attempting to write to a protected area.

There are five categories of popups which you may encounter whilst using GoAnywhere.

1) **Auto Advisor Popups**

Blacklisted programs (known malware) are blocked, encrypted, and deleted immediately.

Whitelisted programs and those which have been trusted by the Advisor Community are automatically allowed access.

Unknown programs trigger a popup which requires your authorization before access will be granted.

The DriveSentry tray icon will appear as shown below when access is automatically allowed or denied.

 The DriveSentry guard will glow green when **access is automatically granted**.

 The DriveSentry guard will glow black with a red background when access is automatically **blocked.**

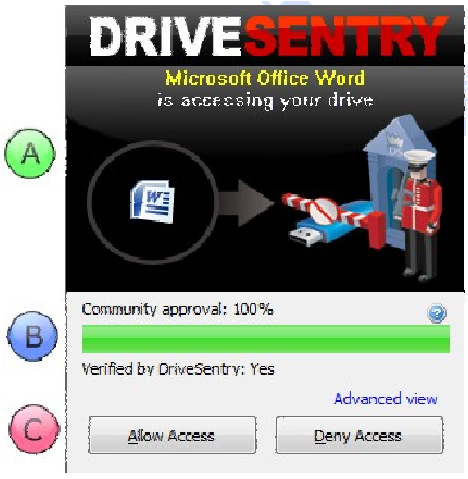
2) **Standard Write Access Popups**

If Auto Advisor has been turned off (through the task tray menu) or there is no Internet connection available, DriveSentry will request authorization for access to your removable device.

Rules can be created and remembered through the popup. Upon removal of your storage device the session rules will NOT be remembered. The next time you insert your removable drive, you will receive popups for programs where rules were previously created.

The standard write access popup can be displayed in both simple and advanced views. Please refer to GoAnywhere user manual for detail descriptions.

The simple write access popup (shown below) will appear when a write is attempted to your removable device. This popup is limited in comparison to the advanced view (explained below) but is deemed suitable for most users. The image to the right appears when the program attempting to access your device is known to online Advisor as malware.

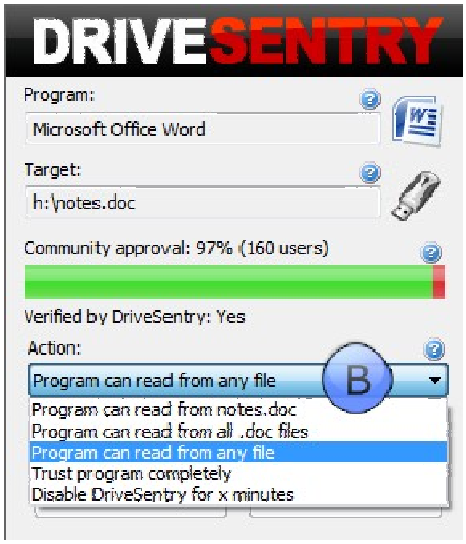


3) **Standard Read Access Popups**

As with the previous section regarding write access popups, If Auto Advisor has been turned off or there is no internet connection available GoAnywhere will request authorization for programs trying to read from your removable device. This is designed to stop malicious programs accessing the data on your removable device. Please refer to GoAnywhere user manual for detail descriptions.

The popups that appear when a program is attempting to read from your

device are similar to standard write access popups (explained in the previous section) with the exception of the file rule options, which are relevant to ***"reads"*** rather than ***"writes"***. Please refer to GoAnywhere user manual for detail descriptions.



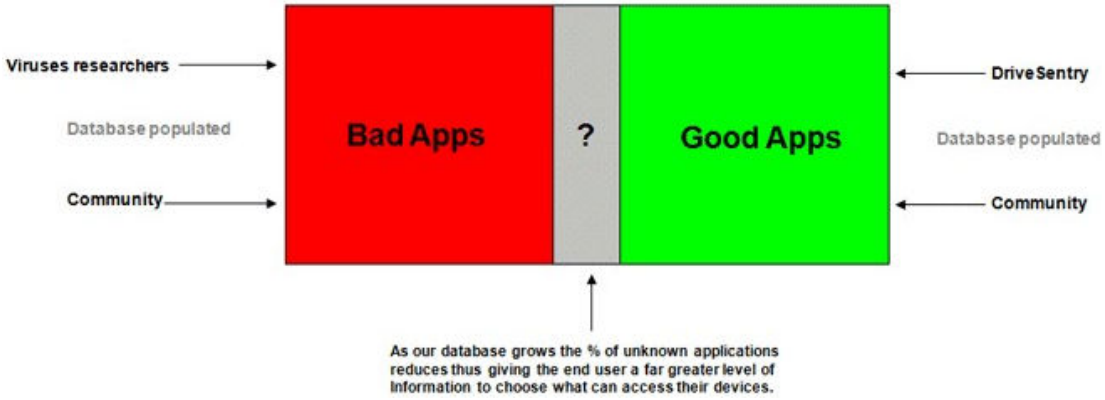
4) **Malicious File Popups**

Similar to the **malicious program popup**, the quarantine popup is triggered if a program is attempting to write a malicious **file** to your device. The Real-time scanner facility is designed to detect malicious files. Please refer to GoAnywhere user manual for detail descriptions.

In the example below GoAnywhere detected a ".com" file as being malicious.

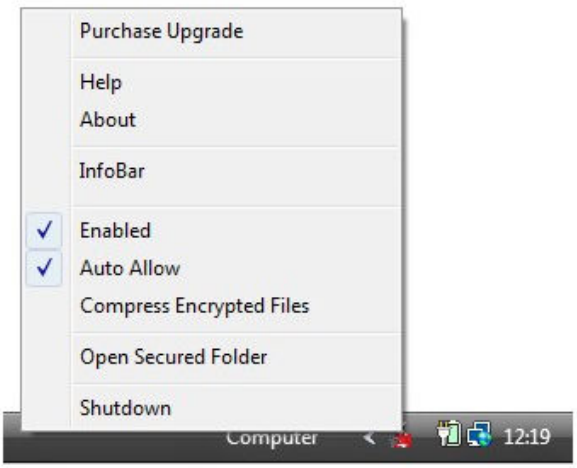
5) **Threat Scoring**

Conventional security software relies on a database of "bad", blacklisted programs (Viruses). GoAnywhere is unique in building an Advisor Community database of both "good" (whitelisted) and "bad" (blacklisted) programs. However new threats are appearing every day which is why GoAnywhere has introduced a threat scoring initiative for the grey area of unknown programs. Please refer to GoAnywhere user manual for detail descriptions.



Shutdown GoAnywhere

When GoAnywhere is in operation the icon below will be displayed in the task tray. Right click on the GoAnywhere icon to access the menu options (below).



Selecting '**Shutdown**' brings up the following dialog.

Select '**Shutdown**' on the dialog to shutdown GoAnyhere's Antivirus protection.

Click the '**do not show again**' checkbox so that GoAnywhere will shutdown directly from the task tray options in the future.

6.2 FILERECOVERY

FILERECOVERY is a safe and affordable do-it-yourself data recovery solution that is designed to recover lost and deleted files from all types of media such as hard drives, floppy drives, SmartMedia, CompactFlash, Memory Sticks, and other types of removable media. It recovers files whether they have been deleted from the command line, from within an application, Windows Explorer, or removed from the Recycle Bin. In addition FILERECOVERY recovers formatted or lost drives and drives with a severe logical file system damage. FILERECOVERY will scan the drive and bring up list of files which can be saved from the scanned drive. Especially for forensic application the list of recovered and reconstructed files and folders can be saved to disk as well as printed out. To preserve the drive with the lost or deleted files, all recovered files must be saved to another storage device or another drive letter in the system. FILERECOVERY is a non-destructive read-only application and will not write or make changes to the drive it is recovering from.

Getting Started

Before getting started your success in recovering files depends a great deal on how the disk is handled and the amount of information written to the disk after the deletion occurred:

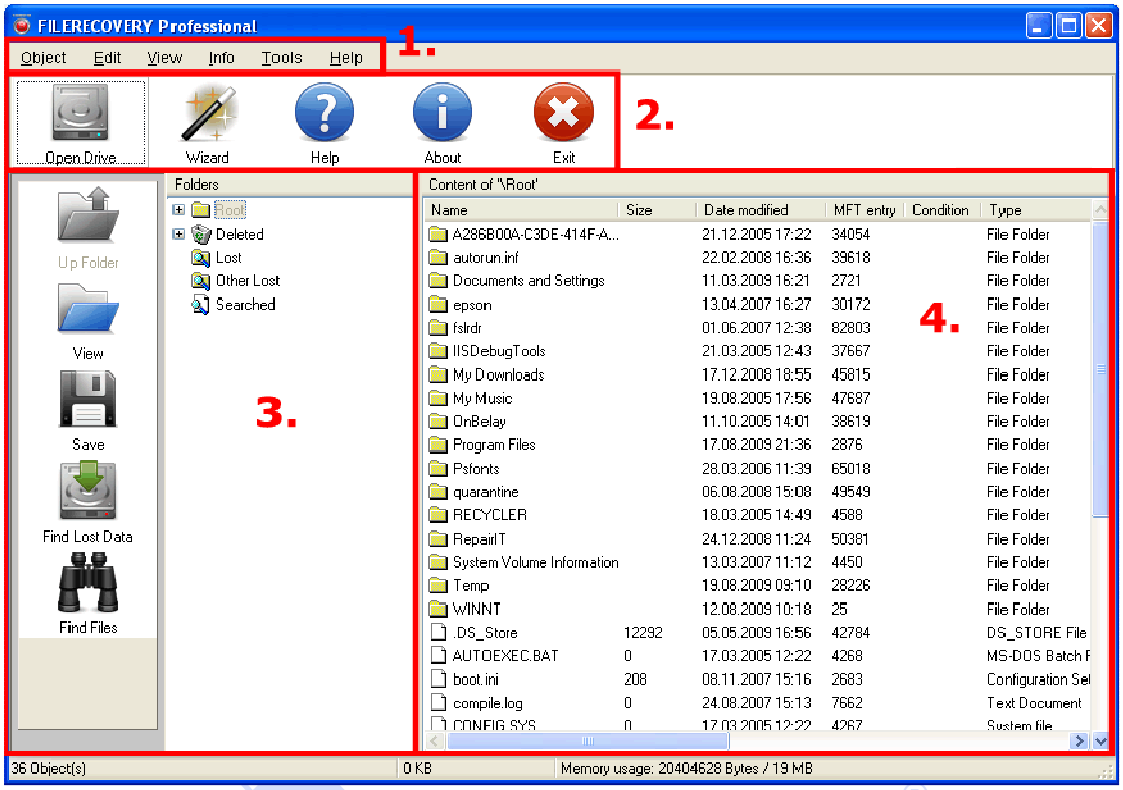
Notice!
DO NOT CONTINUE WORK ON A HARDDRIVE CONTAINING LOST DATA.

- You should not use the system with the deleted files to surf the Internet, check mail or create documents.
- Do NOT reboot or shut down the system.
- Never install software to a system containing deleted files you wish to recover.
- The more activity the less of a chance of recovery.
- DO NOT defragment your hard drive or execute SCANDISK in a deleted recovery situation. Doing so will likely remove all remnants of the file you are trying to recover.

FILERECOVERY was designed to run from the CD-ROM or from a directory on another partition or network drive. It is **not** recommended that you install the software on the work system; temporary files may be written to the disk. Simply run the software from the **AutoRun** menu (right click your CD-ROM symbol) or Click the **RECOVERY.EXE** file in Windows explorer. Once the desired files are recovered you can install FILERECOVERY on the system.

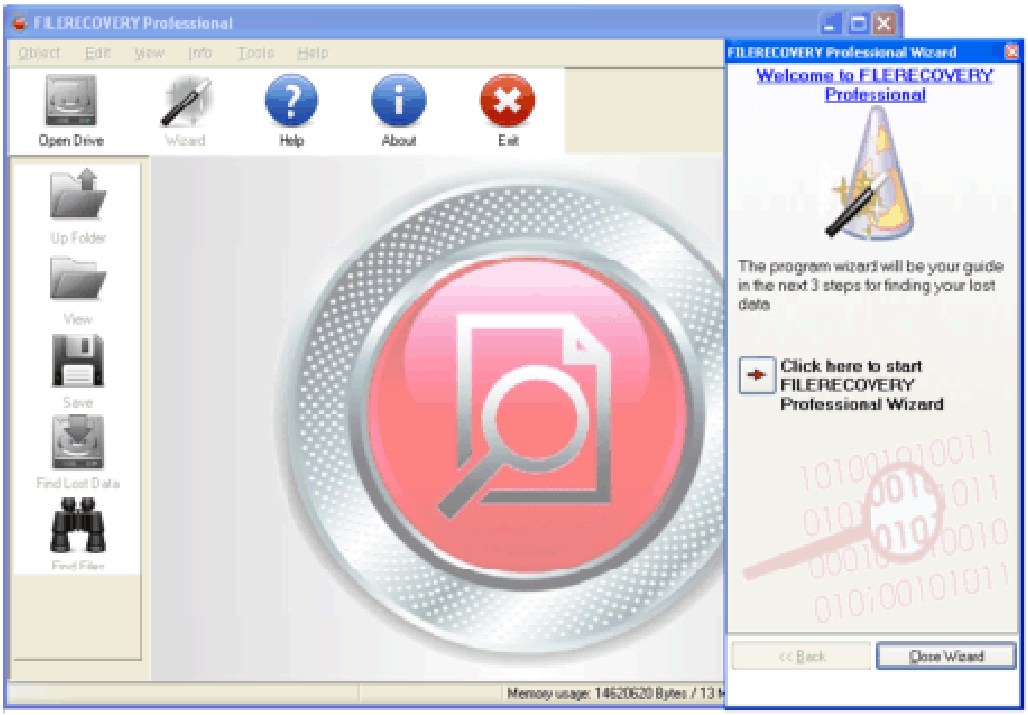
NOTE: For using FILERECOVERY under Windows 2000/XP/VISTA/Win7 your user account must have administrator privilege.

The user interface
Below the program title there is the menu bar (1). Further below there is the button toolbar (2) from which the most important points of the program can be accessed. The directory tree (3) and the file list view (4) are used to navigate through your drive.

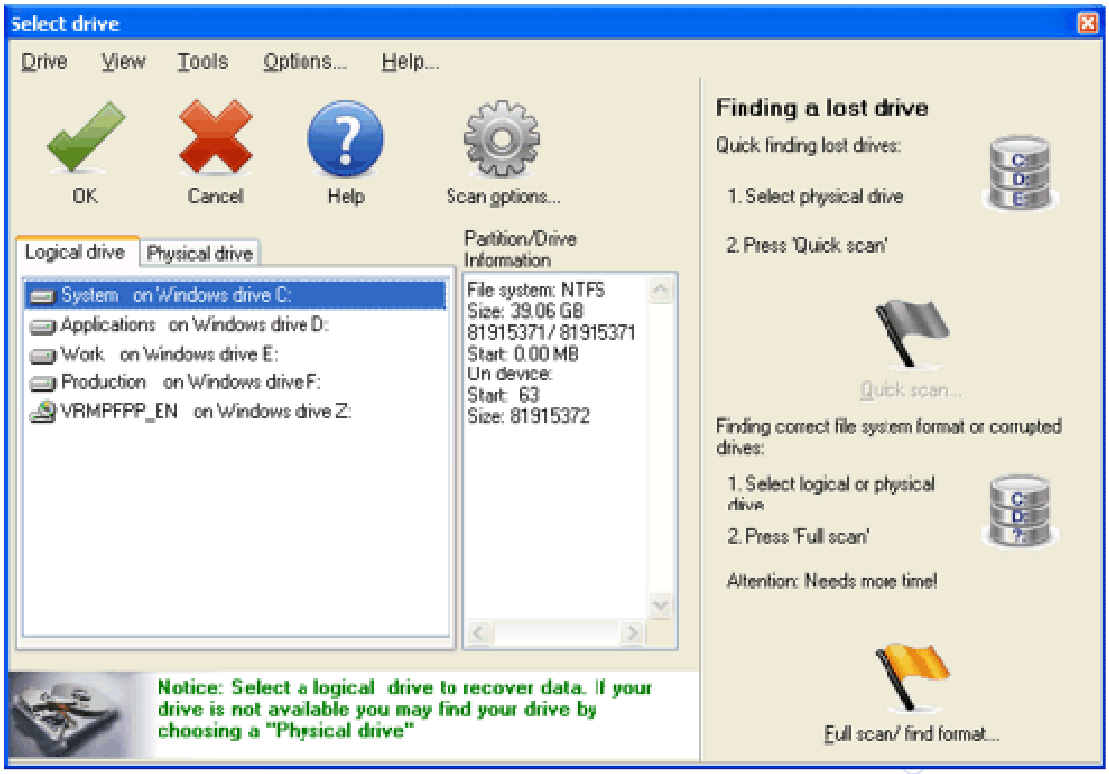


In four steps you recover your deleted files!

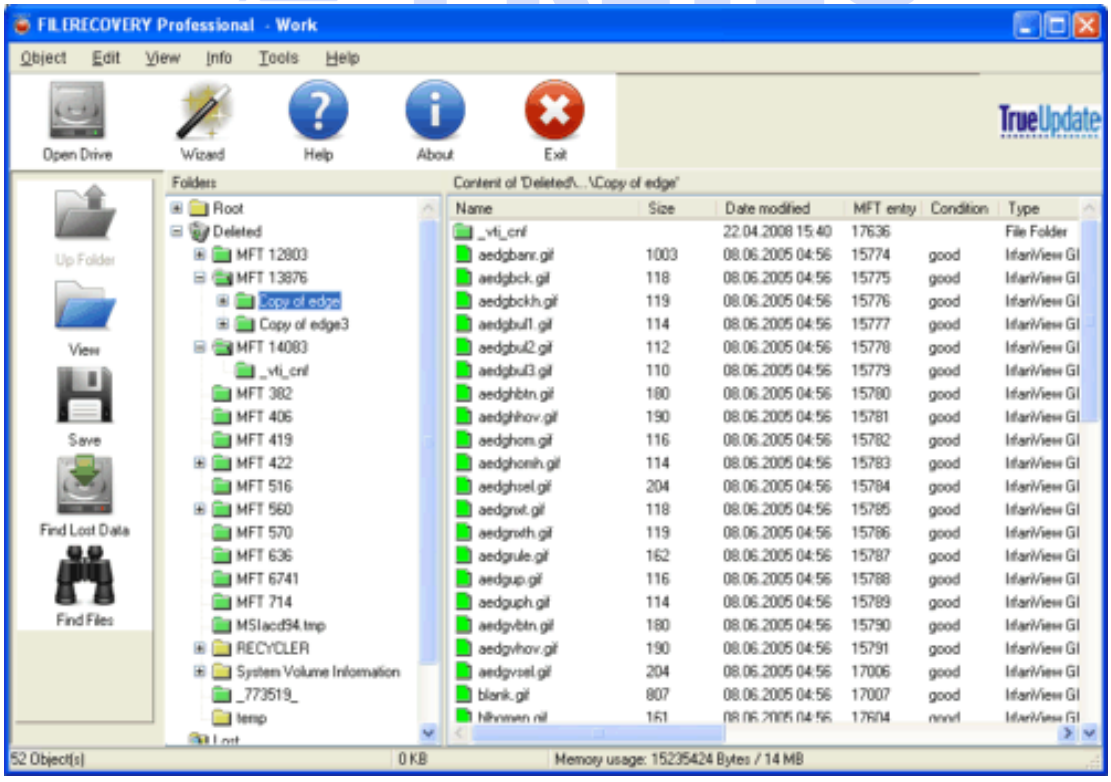
Step 1: Run FILERECOVERY



Step 2: Choose your drive



Step 3: Select your deleted files/directories



Step 4: Simply save them to another hard disk!