UltimateGuard™

(Version 3.0 Beta)

Quick Guide

Notices

UltimateGuard™ 3.0 Beta is Pretec's next generation storage security & utility solution for USB flash drives that provides real-time antivirus, AES-256 encryption, data recovery & online back-up for PCs and mobile devices. Combining security protection and functional utilities, the new UltimateGuard™ 3.0 Beta ensures a satisfying storage experience. Your comments and efforts on trying it will help our further improvement.

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 temporarily be 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 flash drive. When you see a pop-up message requesting to activate “DATA RECOVERY Main Application” and “licman.exe” of DATA RECOVERY, 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™ 3.0 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™ 3.0 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.
- ✓ **Immediate online back-up**
  keep your data secure by storing off-site and your files and folders are regularly backed up on a remote storage. They are protected even if your computer gets stolen or your house burns down.
- ✓ **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 Close

Quit UltimateGuard™.

5. Software Quick Instruction

UltimateGuard™ includes the topmost advanced technology of GoAnywhere and DATA RECOVERY. 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.

5.1 Anti-virus & AES-256 Encryption with *GoAnywhere*

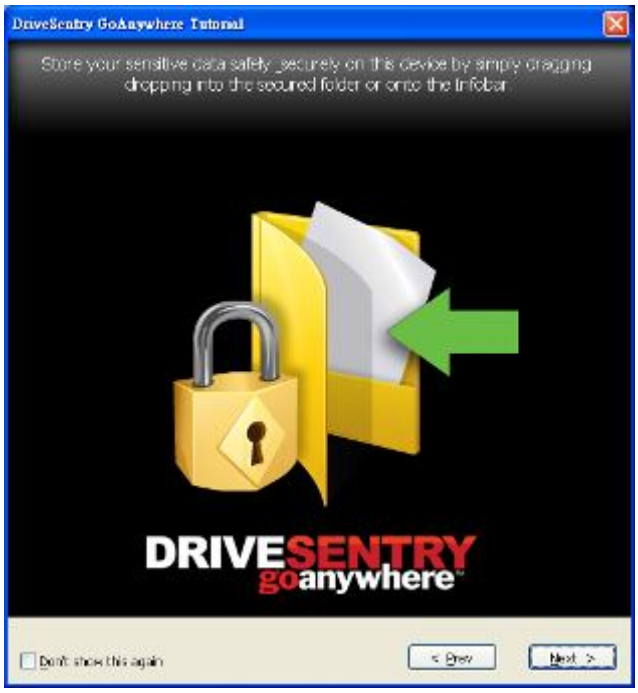
GoAnywhere provides **standalone antivirus protection** and high level **encryption**, so you no longer have to rely on the host system to provide these security methods. GoAnywhere allows you to transfer, transport and work on your data on foreign, third party systems, with confidence and control.

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.

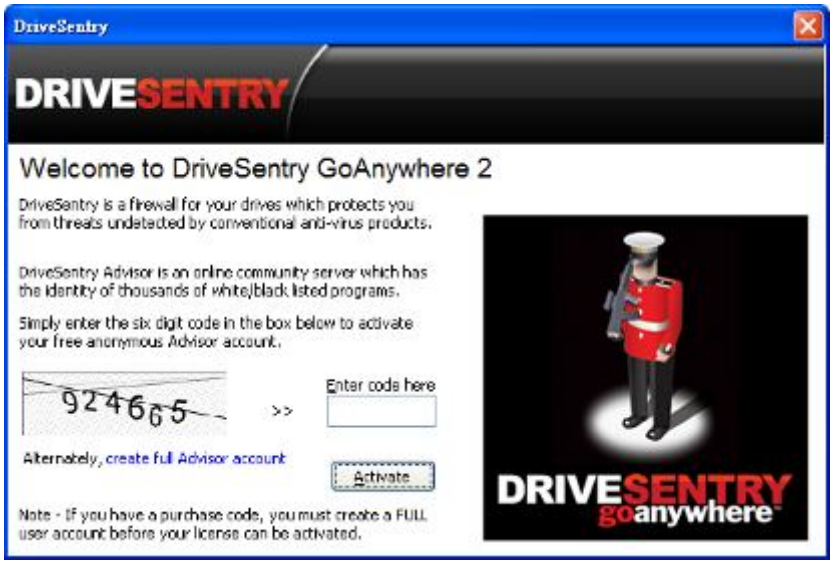
The first time use GoAnywhere

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

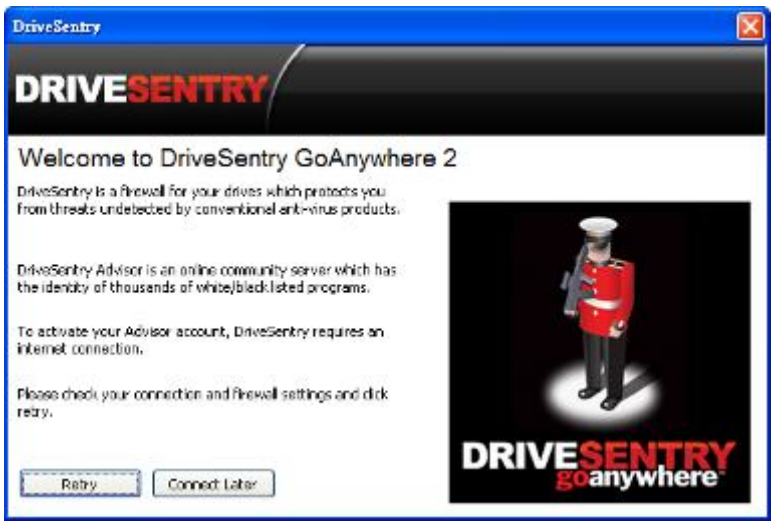
To activate a guest Advisor account, simply enter the six digit security code into the box provided and click the "Activate" Button.

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 a secure encryption password, all data stored on your removable device will now be protected from malicious attack and you have maximized 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.**

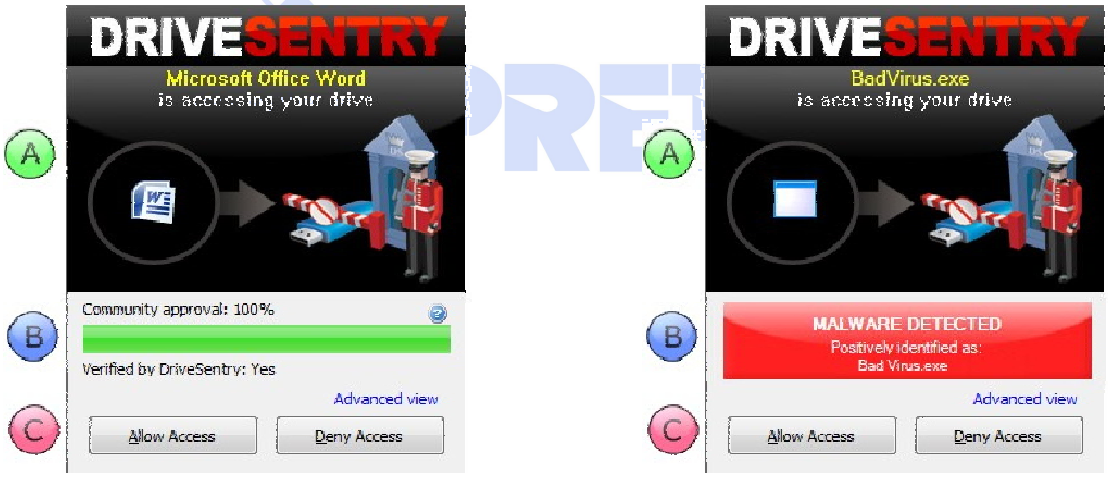
2) **Standard Write Access Popups**

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.

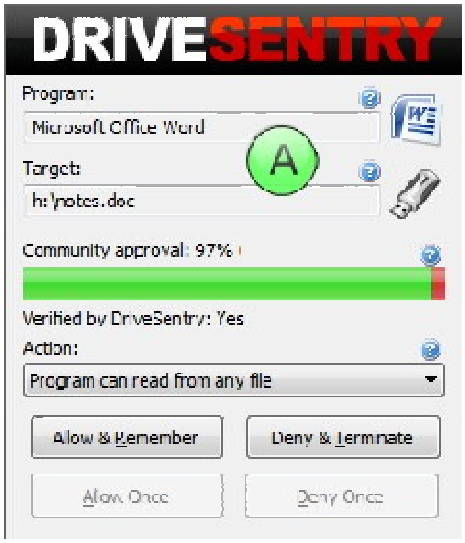


3) **Standard Read Access Popups**

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.



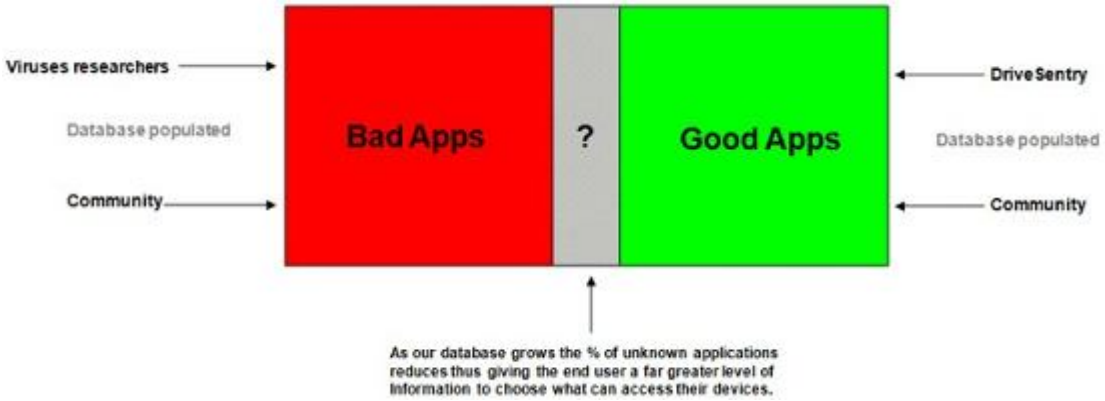
4) **Malicious File Popups**

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.

5.2 DATA RECOVERY with *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:

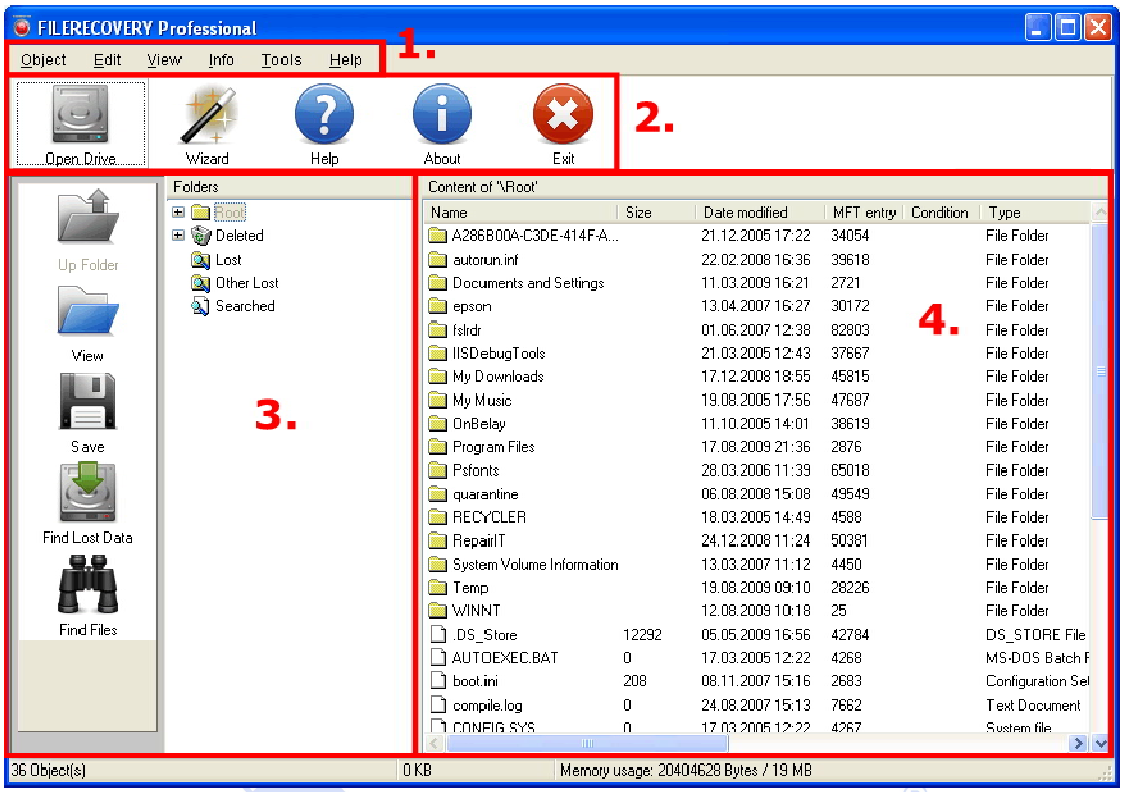
Notice!
DO NOT CONTINUE WORK ON A HARDDRIVE CONTAINING LOST DATA.

- 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 DATA RECOVERY on the system.

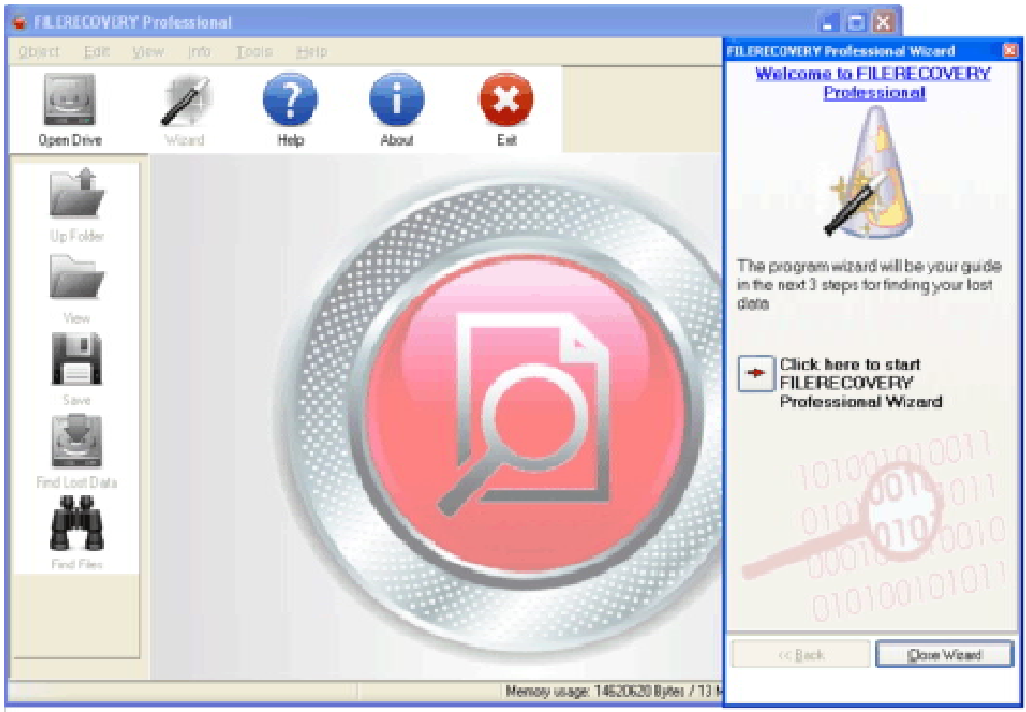
NOTE: For using *FILERECOVERY* under Windows 2000/XP/VISTA/Win7 your user account must have administrator privilege.

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.

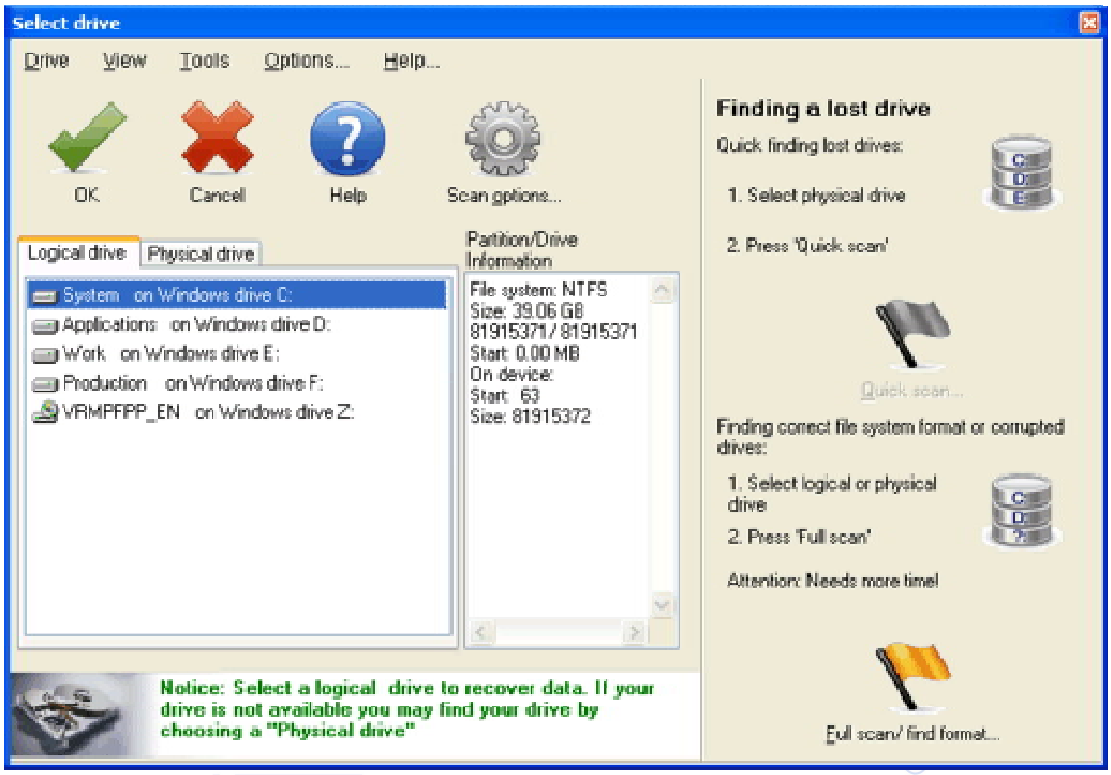


In four steps you recover your deleted files!

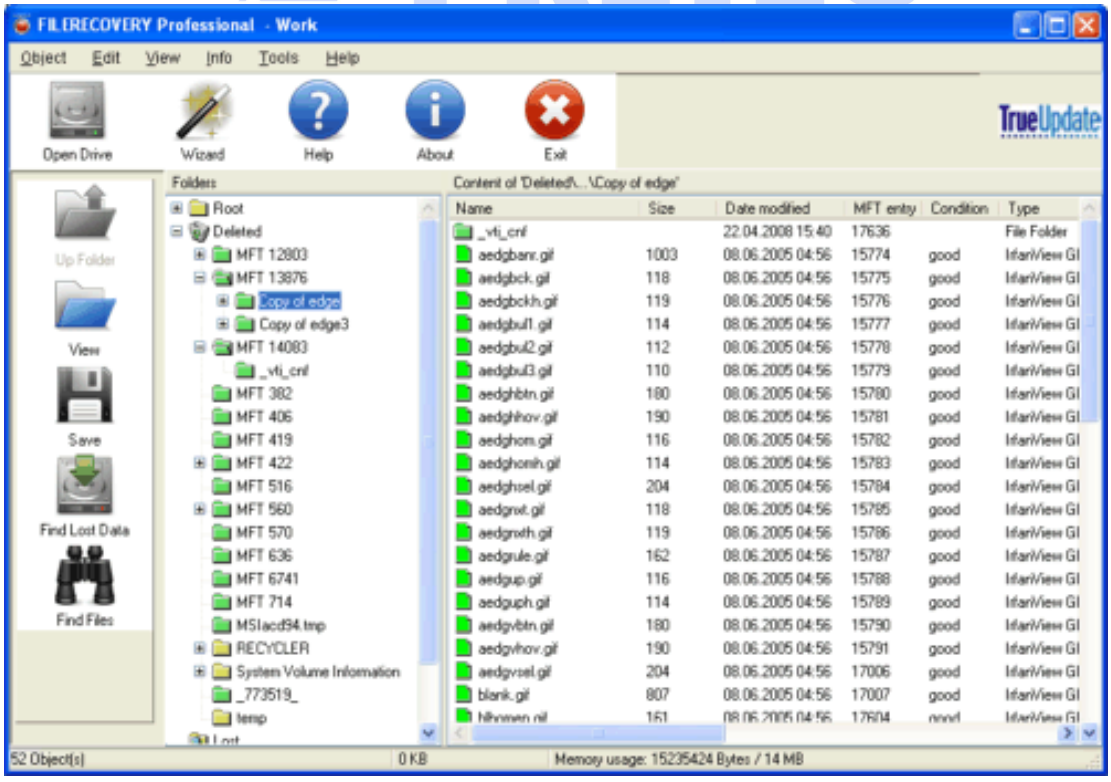
Step 1: Run *FILERECOVERY*



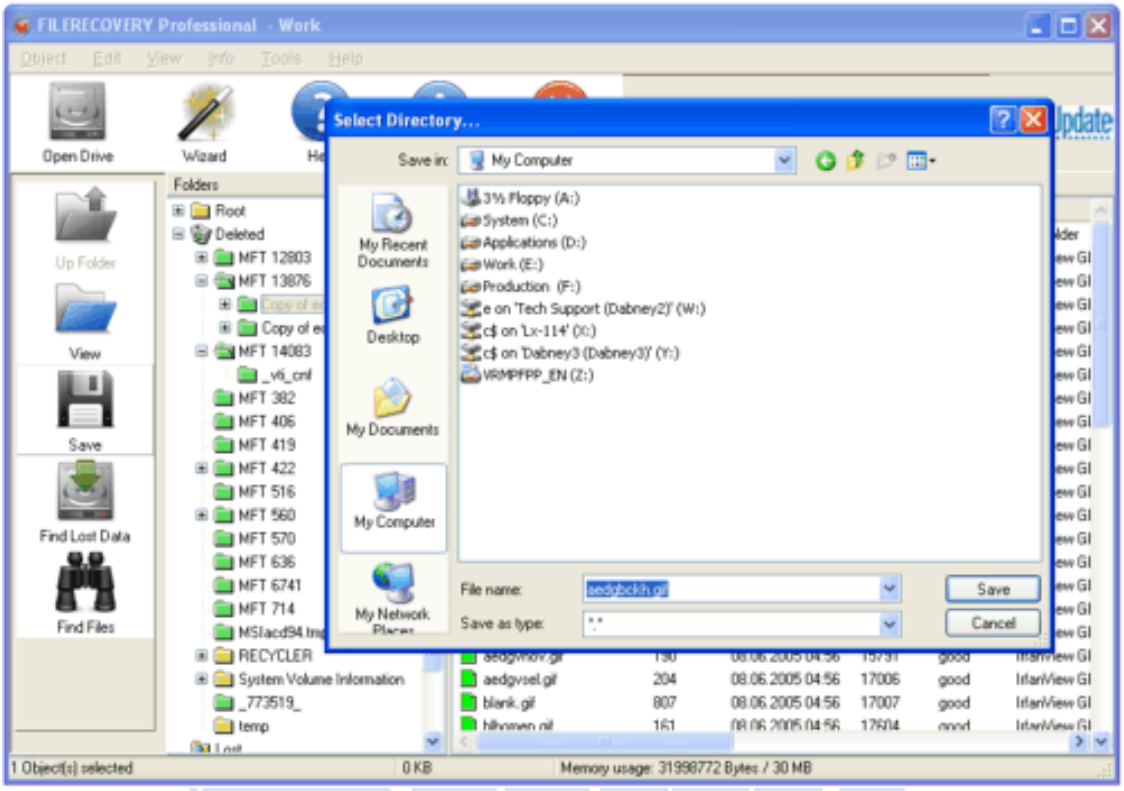
Step 2: Choose your drive



Step 3: Select your deleted files/directories



Step 4: Simply save them to another hard disk!



5.3 Online Data Backup with *Acronis Online Backup*

Acronis Online Backup makes it possible to keep your data secure by storing off-site. Because your files are stored elsewhere, they are protected even if your computer gets stolen or your house burns down. So the risk of data loss as a result of theft, fire, or other natural disasters is practically eliminated. Online backup is basically a method of off-site data storage whereby files and folders are regularly backed up on a remote storage. As a result, you can safely recover any corrupted, lost or deleted files on your computer.

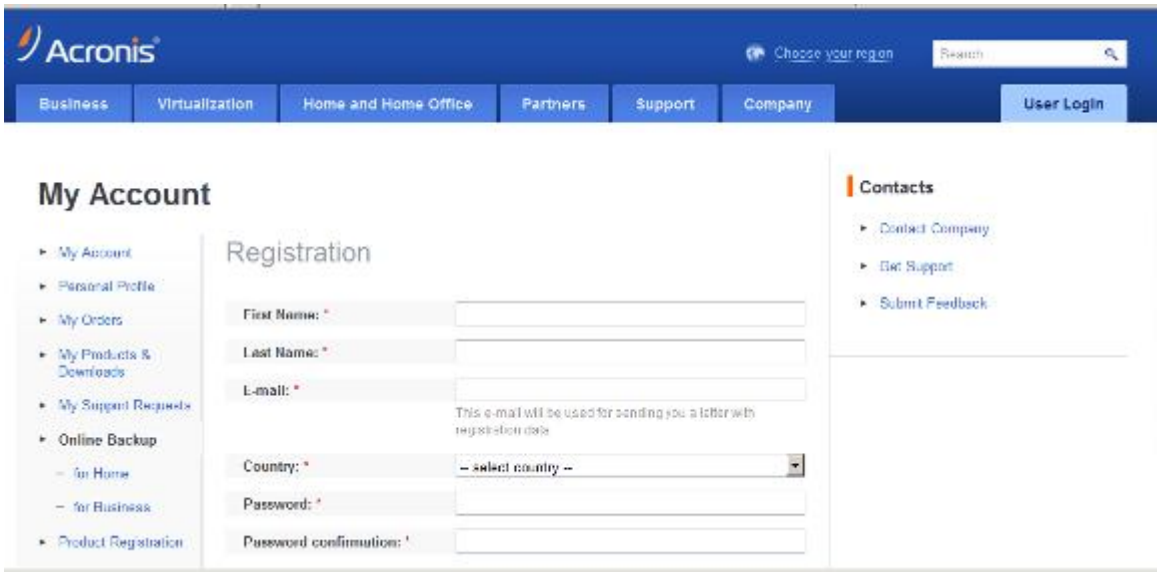
Of course, online backup is not without its shortcomings. If there is a problem with your Internet connection, you could be left without access to your data for some time. And you won't be able to boot up your computer from an online backup, so it is advisable to supplement online backup with image backups to local hard disks.

The biggest drawback of online backup is speed. Even through a fast broadband connection, backing up your data online will be much slower than backing up to a

local hard drive. Depending on the amount of data you want to store off-site, your first full online backup could last several hours, though subsequent backups will take much less time, as you'll be backing up only new or changed files.

If you decide to use encryption, the files will be encrypted before transmission over the Internet and data will be stored on the Acronis Online Storage in encrypted form, so you can rest assured that your private information is secure.

■ Creating an online backup account



Performing backups to Acronis Online Storage requires subscription to the Online Backup service. Clicking on **Online Data Back Up** icon in the main dash board, which will direct you to Acronis' subscription page to continue registration. Please make sure your PC is connected to the Internet to activate the subscription process.

If you already have an Acronis account, type the e-mail address and password for that account under "Log in to Your Account" to the right. If you do not have an Acronis account, fill in the appropriate fields, and the account will be created for you. Provide your first and last names and e-mail address. You will be offered a country selected on the basis of the IP address of your computer, though you can select another country, if you wish. Then provide a password for your new account and confirm the password by retyping it once more in the appropriate field. When you perform all actions necessary for account registration, please, wait for an e-mail message that will

confirm opening of the account.

To keep your personal data secure, choose a strong password for your online backups, guard it from getting into the wrong hands, and change it from time to time.

After opening an Acronis Online Backup account, log in to your account page, and then wait for an e-mail message describing the details of your subscription plan and expiration date. Now you can perform your first online backup.

■ Backing up to Acronis Online Storage

To perform an online backup, log on to your Online Backup service account by clicking **Backup Online Backup** on the sidebar and entering your e-mail address used for opening the account and the password. In order to not enter the password during subsequent logons, you may want to select the **Remember the password** check box. Make these settings and click **Log In**.

After the program connects to Acronis Online Backup Server, select a computer for connection to the Online Storage. When logged on to the online backup service for the first time, register a computer for work with Online Backup. To do this, click **New computer**, then type in the computer name.

If you want to use encryption for the data to be stored on the Online Storage, enter an encryption key to be used for encrypting your data. Entering the encryption key automatically enables encryption of all data stored on the Online Storage. The encryption key is similar to a password, but it is used for unlocking access to your encrypted data. Acronis Online Backup uses the industry standard AES-256 encryption algorithm. The data will be encrypted before transferring through the Internet to the Online Storage and will be stored in encrypted form. You need to enter the encryption key for the computer only once during its registration, though it will be required if you try to recover files backed up from this computer when connected to the Online Storage from another computer.

Having made all the necessary settings, click **Continue**. Until you log off, subsequent connections to the Online Storage from this computer will occur automatically - you just need to select **Online Backup**. If you already registered the computer, select it from the list of registered computers, then click **Continue**. By default your current

computer is selected for registration.

When the computer connects to the online storage, the **Online storage** screen with your storage space quota appears. If you have performed backup on this computer before, you will see how much Online storage space is occupied by the backed up files and folders. The screen also shows the space occupied by the data backed up from other computers (if any) and the remaining free space on the Online storage in accordance with your quota.

When you are going to back up from the current computer for the first time (or need to change the files and folders selected for online backup), click **What to Back Up**. This will open the What to Back Up window with two tabs: **Include** and **Exclude**. The **Include** tab displays your computer's file and folder tree. The area to the right of the tree shows
the contents of a selected folder. This tab allows you to select individual files and folders for backing up, as well as data categories. For more information on categories see Selecting what data to back up (p. 50).

Furthermore, you can create a custom category by clicking **Add new category**.
The **Exclude** tab enables hidden and system files and folders to be excluded from online backup, as well as files meeting the criteria you specify. Excluding unnecessary files may be useful for backups to the Online storage as the data transfer rate and available space is limited.

*You can also exclude/include files and folders by selecting them in Windows Explorer and choosing **Storages Exclude from Online Backup** (or **Include in Online Backup**) in the shortcut menu that opens by right-clicking on the selected file or folder. This shortcut is only available when you are logged on to the Online Backup service.*

Having finished selecting files and folders for backing up to the Online storage and for excluding from backup click **OK**. If you do not unselect the **Run the updated online backup task now** check box that is selected by default, the online backup task will start immediately. Otherwise it will run according to the schedule you set.

To schedule online backups, click the **Edit schedule...** link. For instance, you may want the backups to be performed at night in order to not interfere with your web

surfing. For more information see Scheduling tasks (p. 76). When you finish scheduling and click **OK**, the schedule information will be shown above the **Edit schedule...** link.

By default Acronis True Image Personal schedules daily backups to the Online Storage with randomly selected backup start time.

You can quickly start updating the files and folders backed up on the Online storage without creating a backup schedule. To do so, click **Update Backup Now**. This may be useful when you want to back up immediately some important changes to the files backed up on the Online Storage. Incidentally, if the last scheduled online backup has failed, this link changes to **Update Backup Now (Last backup failed)**, allowing you to repeat the failed backup task right away. If you have suspended the previous online backup for any reason, the link text will be as follows: **Update Backup Now (Last backup suspended)**.

■ Recovering data from Online Storage

Log on to your online backup account by clicking **Backup** **Online Backup** on the sidebar and entering your e-mail address used for opening the account and the password. After the program connects to Acronis Online Backup Server, select a computer for registration on the Online Storage. By default your current computer is selected for registration. Click the **Continue** button. The Online storage screen opens with this computer selected. If you have data backed up from more than one computer, you can select on this screen the computer from which to recover required files. Naturally, you can only browse and recover the data backed up from other computers. If you encrypted data on another computer, you will be asked to enter the encryption key for the computer to get access to its data on the Online Storage.

1. Click **Browse** on the **Online storage** screen.
Acronis Time Explorer will be opened with the **Online Storage** tab selected.

2. This window also allows choosing the computer from which you backed up the files and folders you need to recover. Select the computer by its name on the directory tree under Online Storage in the left pane.

3. By default the state of the Online Storage after the latest backup is displayed, so

the latest versions of the files and folders will be recovered. If you need to recover earlier versions, select the date and time on which you want to recover the state of the files and folders.

4. Select the folder containing the files you want to recover in the left pane. The right pane lists the files in that folder. Select the files to recover. When selecting multiple files you can use the **Ctrl** and **Shift** keys like in Windows Explorer. Having finished selection, click the **Recover** icon on the toolbar.

5. Acronis True Image Personal opens the **Browse for folder** dialog. By default the original location from which the files were backed up will be selected. If necessary, you can select another folder or create a new folder for the files to be recovered to by clicking the **Make New Folder** button. After selecting the folder click **OK**.

If you recover the files to the original folder and Acronis True Image Personal finds a file with the same name there, it will open a dialog window where you can choose what to do with the file: **Recover and replace** the file on the disk, **Do not recover** (to keep the file on the disk), and **Recover, but keep both files** (the recovered file will be renamed). If you want to use the choice for all files with identical names, select the **Apply to all files** check box.

*It is impossible to **Recover and replace** files on the disk which are being used or locked by the operating system at the moment of recovery.*

If you need to recover a specific version of a file, select the file, right click and choose **View Versions** in the shortcut menu. This opens the **File Versions** window. Select the required version by its backup time and click **Recover** on the toolbar. You can also recover the version by dragging it into a selected folder.

To choose the correct version, you can open the version in the associated application and view the file contents. Select the file in the right pane and the bottom line of Time Explorer will show the times of backing up all its versions kept on the Online Storage. Choose a version by its backup time, then right-click on the file in the right pane and choose **Open** in the shortcut menu. Acronis True Image Personal will recover the file version to a temporary folder and then will open the file using the associated application.

■ Managing Online Storage

As the available space on Acronis Online Storage is limited depending on the chosen backup plan, you need to manage your Online Storage space by cleaning up the obsolete data. Cleanup can be done in a variety of ways. The most "drastic" one is removing a computer registered on the Online Storage, if you have registered more than one. Removing a computer results in deleting all data that was backed up from that computer, so such an operation must be carried out with caution. To remove a computer, select it on the **Online storage** screen by its name and click **Remove <Computer_name>**, then click **Yes** in the confirmation window. After the deletion finishes, click **Refresh** on the toolbar to refresh the storage state shown.

The Online backup options provide for automatic cleanup of the Online Storage. You can specify deletion of files that have been kept on the storage longer than the specified number of months or days. In addition, you can set the maximum number of file versions to be kept on the Online Storage. You can accept the default settings for those options shown above the **Change cleanup options...**link or set the values you need. To change the above options, click the link and set the desired values.

You can also manage Acronis Online Storage by deleting individual files or even some of their versions.
1. Click **Browse** on the **Online storage** screen. Acronis Time Explorer will be opened with the **Online Storage** tab selected.

2. Select the computer from which you backed up the files you need to manage by its name on the directory tree under Online Storage in the left pane.

3. Select the folder containing the files you want to manage in the left pane. The right pane lists the files in that folder.

4. If you want to delete some versions of a specific file, select the file and click **View Versions** on the toolbar. This opens the **File Versions** window. Select the version you want to delete and click **Remove** on the toolbar. When you want to delete several versions, use the **Ctrl** and **Shift** keys like in Windows Explorer to select the versions for deletion and then click **Remove** on the toolbar. Having finished removing the versions, click **OK**. To delete all versions of the file click **Remove All** on the toolbar.

5. If you want to delete a file, select it in the right pane. When selecting multiple files for deletion you can use the **Ctrl** and **Shift** keys like in Windows Explorer. Having finished selection, right-click on the selection and choose **Delete** in the shortcut menu.

6. After you finish managing the Online Storage, close the Acronis Time Explorer window.

7. To see how much space you have freed up, click **Refresh** on the toolbar of the Storage state screen and check the new value of free space.

■ Setting online backup options

You can set these options after logging on Acronis Online Backup and selecting a computer for use
with Online backup service. To do so, click **Settings** on the **Storage state** screen.

■ Connection attempts

This page allows you to optimize the settings Acronis True Image Personal uses when establishing connection to the Online Storage. Here you can specify how many connection attempts will be made if the first attempt fails (the default number is 10). In addition you can specify a time interval between connection attempts (30 seconds by default).

■ Storage connection speed

One more option gives you the ability to "throttle" the bandwidth allocated for data transfer to the Online Storage. Set the connection speed that will allow you to send e-mail or surf the Web without annoying slowdowns while online backup is running. To do this, select the **Limit transfer rate to:** check box and set the connection speed (8 Mbps by default).

To back up your data to the Online storage at the maximum speed your Internet connection can provide, unselect the **Limit transfer rate to:** check box.

■ Storage cleanup

The **Storage cleanup** page is intended for setting the options that enable automatic cleanup of obsolete file versions from the online storage to keep the storage from

overfilling.

You can:
- Delete versions that are older than the specified time period - 6 months by default.
- Specify how many versions of your files must be kept on the Online Storage. This will allow you to return to a previous file version if your changes in a file turn out to be erroneous. By default

Acronis True Image Personal will keep 10 versions of your files, though you can specify any othernumber.

■ Proxy settings

If your computer is connected to the Internet using a proxy server, enable use of the proxy server and enter its settings.
Acronis Online Backup supports only http and https proxy servers.

In the **Host name** box, type the name or IP address of the proxy server, such as proxy.example.com or 192.168.0.1. In the **Port** box, type the proxy server's port, such as 8080.In the **User name** and **Password** boxes, type the credentials you use for connecting to the proxy server, if necessary.

To test the proxy server connection, click the **Test** button.

If you do not know your proxy server settings, contact your network administrator or Internet service provider for assistance. Alternatively, you can take these settings from your browser's configuration.

■ Recommendations on selecting data for storing online

Because online backups are relatively slow, you should think over what data to back up. First of all consider backing up your personal data that cannot be recovered if lost as a result of fire, computer theft, etc. Before proceeding with a backup, estimate how long it will take to back up your data. For instance, if your folders take up 10GB and your upload speed is 1000 Kbps (somewhat less than half a gigabyte per hour), it should take more than 20 hours to perform your first full backup. So depending on the speed of your Internet connection, you may want to back up just the most critical files.