



Acronis® TrueImage WD Edition

User's Guide

Copyright © Acronis, Inc., 2000-2010. All rights reserved.

“Acronis” and “Acronis Secure Zone” are registered trademarks of Acronis, Inc.

"Acronis Compute with Confidence", "Acronis Startup Recovery Manager", "Acronis Active Restore" and the Acronis logo are trademarks of Acronis, Inc.

Linux is a registered trademark of Linus Torvalds.

VMware and VMware Ready are trademarks and/or registered trademarks of VMware, Inc. in the United States and/or other jurisdictions.

Windows and MS-DOS are registered trademarks of Microsoft Corporation.

All other trademarks and copyrights referred to are the property of their respective owners.

Distribution of substantively modified versions of this document is prohibited without the explicit permission of the copyright holder.

Distribution of this work or derivative work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Third party code may be provided with the Software and/or Service. The license terms for such third-parties are detailed in the license.txt file located in the root installation directory. You can always find the latest up-to-date list of the third party code and the associated license terms used with the Software and/or Service at <http://kb.acronis.com/content/7696>

Table of contents

1	Introduction	6
1.1	What is Acronis® True Image WD Edition?.....	6
1.2	Acronis True Image WD Edition basic concepts	6
1.3	System requirements and supported media	8
1.3.1	Minimum system requirements	8
1.3.2	Supported operating systems	8
1.3.3	Supported file systems.....	9
1.3.4	Supported storage media	9
2	Acronis True Image WD Edition installation and startup.....	10
2.1	Installing Acronis True Image WD Edition	10
2.2	Running Acronis True Image WD Edition.....	10
2.3	Removing Acronis True Image WD Edition.....	11
3	General information and proprietary Acronis technologies	12
3.1	Disk/partition images.....	12
3.2	Full backup	12
3.3	Backup file naming conventions.....	12
3.4	Viewing disk and partition information.....	13
3.5	Acronis DriveCleanser	13
3.6	Booting from system image tib files	14
4	Preparing for disaster recovery	15
4.1	How to best prepare for a disaster.....	15
4.1.1	Recommendations for testing that your backups can be used for recovery.....	15
4.1.2	Additional recommendations.....	16
4.2	Testing bootable rescue media	16
4.3	Creating a custom rescue CD	18
5	Getting to know Acronis True Image WD Edition.....	20
5.1	Program workspace	20
5.2	Main screens.....	21
5.3	Options screen	24
6	Creating backup archives	26
6.1	Preparing for your first backup.....	26
6.2	Deciding what data to back up	26
6.3	Some typical backup scenarios.....	27
6.3.1	Backing up a system partition	27
6.3.2	Backing up an entire system disk	27
6.3.3	Backing up a data partition or disk	29
6.3.4	Backing up to a network share	29
7	Additional backup features	31
7.1	Backup Wizard – detailed information	31

7.1.1	Selecting what data to back up	31
7.1.2	Selecting archive location	31
7.1.3	Backup method	32
7.1.4	Selecting the backup options	33
7.1.5	Providing a comment.....	33
7.1.6	The backup process.....	34
7.2	Fine-tuning your backups	34
7.2.1	Backup options.....	34
7.2.2	Local storage settings.....	36
8	Data recovery with Acronis True Image WD Edition	38
8.1	Recovering your system partition.....	38
8.2	Recovering a disk backup to a different capacity hard disk	39
8.2.1	Recovering a disk without a hidden partition	40
8.2.2	Recovering a disk with a hidden partition	41
8.3	Recovering a data partition or disk.....	43
8.4	Recovering files and folders.....	44
8.4.1	Recovering files and folders from image archives	44
9	Additional recovery information	46
9.1	Recovery Wizard - detailed information.....	46
9.1.1	Starting the Recovery Wizard.....	46
9.1.2	Archive selection	46
9.1.3	Recovery method selection	47
9.1.4	Selecting a disk/partition to recover.....	47
9.1.5	Selecting a target disk/partition.....	49
9.1.6	Changing the recovered partition type	49
9.1.7	Changing the recovered partition size and location	50
9.1.8	Assigning a letter to the recovered partition	50
9.1.9	Setting recovery options.....	51
9.1.10	Executing recovery	51
9.2	Setting default recovery options	51
9.2.1	File recovery options.....	51
9.2.2	Overwrite file options	51
9.2.3	Recovery priority	52
10	Creating bootable media.....	53
10.1	Creating Linux-based rescue media.....	53
11	Exploring archives and mounting images	56
11.1	Mounting an image.....	56
11.2	Unmounting an image	58
12	Searching backup archives and their content	60
12.1	Searching	60
12.2	Windows Search and Google Desktop integration.....	61
12.2.1	Using Google Desktop with Acronis True Image WD Edition	62
12.2.2	Using Windows Search with Acronis True Image WD Edition	64
13	Other operations	68
13.1	Validating backup archives	68
13.2	Viewing Tasks and Logs.....	68

13.3	Managing backup archives	70
13.4	Removing backup archives	71
13.5	Moving backup archives	71
14	Transferring the system to a new disk	72
14.1	General information	72
14.2	Security	72
14.3	Executing transfers	73
14.3.1	Selecting Clone mode	73
14.3.2	Selecting source disk	74
14.3.3	Selecting destination disk	74
14.3.4	Partitioned destination disk	75
14.3.5	Selecting partition transfer method	75
14.3.6	Cloning with manual partitioning.....	76
14.3.7	Cloning summary	78
15	Adding a new hard disk.....	79
15.1	Selecting a hard disk	79
15.2	Creating new partitions	79
15.3	Disk add summary	80
16	Security and Privacy Tools.....	82
16.1	Acronis DriveCleanser.....	82
16.2	Creating custom algorithms of data destruction.....	85
17	Troubleshooting	87
17.1	General	87
17.2	Installation issues.....	87
17.3	Backup and validation issues	88
17.4	Recovery issues.....	89
17.5	Bootability after recovery issues	90
17.6	Other issues	90
18	Hard Disks and Boot Sequence	93
18.1	Arranging boot sequence in BIOS.....	93
18.2	Installing hard disk drives in computers	93
18.2.1	Installing an IDE hard disk drive, general scheme.....	93
18.2.2	Motherboard sockets, IDE cable, power cable	94
18.2.3	Configuring hard disk drives, jumpers	95
18.2.4	Installing a SATA hard drive	96
18.2.5	Steps for installing a new internal SATA drive.....	96
18.3	Hard Disk Wiping methods	97
18.3.1	Functioning principles of Information wiping methods.....	97
18.3.2	Information wiping methods used by Acronis	98
19	Startup Parameters.....	99
19.1	Description.....	99

1 Introduction

1.1 What is Acronis® True Image WD Edition?

Acronis True Image WD Edition is an integrated software suite that ensures security of all information on your PC. It can backup the entire disk drive or selected partitions, including your operating system, applications, settings and all of your data. You can also use the software to securely delete any confidential data you no longer need.

Acronis True Image WD Edition is designed to create optimally aligned partitions on WD Advanced Format Drives. The drive image archive backup and restore, drive cloning, and "add new disk" features all operate in this manner by transferring or creating partitions that are aligned on 4K sector boundaries. This process ensures optimal performance for the product.

Should your disk drive become damaged or your system attacked by a virus or malware, you can restore the back-up data quickly and easily, eliminating hours or days of work trying to rebuild your disk drive's data and applications from scratch.

Acronis True Image WD Edition provides you with all the essential tools you need to recover your computer system should a disaster occur, such as losing data, accidentally deleting critical files or folders, or a complete hard disk crash. If failures occur that block access to information or affect system operation, you will be able to restore the system and the lost data easily.

The unique technology developed by Acronis and implemented in Acronis True Image WD Edition allows you to perform exact, sector-by-sector disk backups, including all operating systems, applications and configuration files, software updates, personal settings, and data.

You can store backups on almost any PC storage device: internal or external hard drives, network drives or a variety of IDE, SCSI, FireWire (IEEE-1394), USB (1.0, 1.1 and 2.0) and PC Card (formerly called PCMCIA) removable media drives, as well as CD-R/RW, DVD-R/RW, DVD+R/RW, magneto-optical, Iomega Zip and Jaz drives.

If you are going to install a new hard disk drive, Acronis True Image WD Edition will help you to transfer information from the old one in minutes, including operating systems, applications, documents, and personal settings. After migrating to the new hard disk you can destroy all confidential information on the old one securely. This is the recommended procedure if you intend to donate, throw away, or sell the old hard disk drive.

Wizards and a Windows Vista-style interface will make your work easier. Just perform a few simple steps and let Acronis True Image WD Edition take care of everything else! When a system problem occurs, the software will get you up and running in no time.

1.2 Acronis True Image WD Edition basic concepts

This section provides general information about basic concepts which could be useful for understanding how the program works.

Backup

According to Wikipedia, "**backup** refers to making copies of data so that these additional copies may be used to **restore** the original after a data loss event. Backups are useful primarily for two purposes.

The first is to restore a state following a disaster (called disaster recovery). The second is to restore small numbers of files after they have been accidentally deleted or corrupted."

Acronis True Image WD Edition provides for these purposes by creating disk (or partition) images. By default, Acronis True Image WD Edition stores in an image only those hard disk parts that contain data (for supported file systems). However, you may use an option that lets you include in an image all of the sectors of a hard disk (so called sector-by-sector backup).

Disk cloning

This operation migrates/copies the entire contents of one disk drive to another (e.g., when installing a larger disk) to get two identical drives with the same file structure. The "Disk Clone" tool effectively copies all of the contents of one hard disk drive onto another hard disk drive. The operation allows you to transfer all the information (including the operating system and installed programs) from one hard disk drive to another without having to reinstall and reconfigure all of your software. If you decide to use cloning, the best chance of success is to remove the existing drive from the computer and install the new drive in its place. It should be connected in exactly the same way as the old drive.

Acronis True Image WD Edition does not provide for cloning a single partition. You can clone only an entire drive.

By the way, you can also transfer all the information from your hard disk drive to another one by backing up the entire old hard disk and then recovering the backup to the new disk.

Backup archive components

Archive - Known as archive chain or archive group, it is the whole set of backup files managed by a single backup task. The archive can consist of one or several slices.

Slice - It is a set of files created during each cycle of the task execution. The amount of slices created is always equal to the amount of times the task is executed. A slice represents a point in time, to which the system or data can be recovered.

Volume - It is a tib file associated with the slice. Usually there is only one volume per slice however, each slice may consist of several volumes. If you have set archive splitting in the task options, the resulting slice will be split into several files. In addition, Acronis True Image WD Edition automatically splits a slice into several files of 4GB each (except the last file) when you make a large backup to a FAT32 formatted hard disk. These files are the slice's volumes.

Snapshots

While creating disk images, Acronis True Image WD Edition uses "snapshot" technology that allows creating even system partition backups while running Windows with files open for reading and writing without the necessity to reboot the computer. Once the program starts the partition backup process, it temporarily freezes all the operations on the partition and creates its "snapshot". Snapshot creation usually takes just several seconds. After that the operating system continues working as the imaging process is under way and you will not notice anything unusual in the operating system functionality.

In its turn, the Acronis driver continues working to keep the point-in-time view of the partition. Whenever the driver sees a write operation directed at the partition, it checks whether these sectors are already backed up and if they are not, the driver saves the data on the sectors to be overwritten to a special buffer, then allows overwriting. The program backs up the sectors from the buffer, so that all the partition sectors of the point-in-time when the snapshot was taken will be backed up intact and an exact "image" of the partition will be created.

Backup file format

Acronis True Image WD Edition saves backup data in the proprietary tib format using compression. This provides for reducing the storage space requirements, as well as for backward compatibility with the previous Acronis True Image WD Edition version. While creating a tib file, the program calculates checksum values for data blocks and adds these values to the data being backed up. These checksum values allow verifying the backup data integrity. However, using the proprietary format means that the data from such backups can be recovered only with the help of Acronis True Image WD Edition itself – either in Windows or in the recovery environment.

Backup archive validation

How can you be sure that you'll be able to recover your system if the need arises? The feature called backup validation provides a high degree of such assurance. As was already said, the program adds checksum values to the data blocks being backed up. During backup validation Acronis True Image WD Edition opens the backup file, re-calculates the checksum values and compares those values with the stored ones. If all compared values match, the backup file is not corrupted and there is a high probability that the backup can be successfully used for data recovery. It is highly recommended to validate system partition backups after booting from the rescue media.

Disaster recovery

Recovering from a disaster usually requires a rescue media, because such disaster often means that your operating system does not boot either due to system data corruption (e.g. caused by a virus or malware) or a hard disk failure. When the operating system fails to boot, you need some other means of booting and using Acronis True Image WD Edition to recover the system partition. So to be better prepared for a disaster, you absolutely must have a rescue media. Legal owners of the program can create a rescue media using the tool called Media Builder.

To enable booting to the recovery environment, it is necessary to ensure that the BIOS boot sequence includes the rescue media. See Arranging boot sequence in BIOS (p. 93).

1.3 System requirements and supported media

1.3.1 Minimum system requirements

The hardware requirements of Acronis True Image WD Edition correspond to the minimum requirements for the operating system installed on the computer to be used for running Acronis True Image WD Edition. In addition Acronis True Image WD Edition requires the following hardware:

- Attached Western Digital device
- CD-RW/DVD-RW drive for bootable media creation
- Mouse or other pointing device (recommended).

Acronis True Image WD Edition rescue media has the following hardware requirements:

- 256 MB RAM
- Processor Pentium 1 GHz or faster

The recommended minimum screen resolution is 1152 x 864.

1.3.2 Supported operating systems

Acronis True Image WD Edition has been tested on the following operating systems:

- Windows XP SP3
- Windows XP Professional x64 Edition SP2
- Windows Vista SP2 (all editions)
- Windows 7 (all editions)

Acronis True Image WD Edition also enables creation of a bootable CD-R/DVD-R that can back up and recover a disk/partition on a computer running any Intel- or AMD- based PC operating system, including Linux®. The only exception is the Intel-based Apple Macintosh, which is currently not supported in native mode.

1.3.3 Supported file systems

- FAT16/32
- NTFS
- Ext2/Ext3 *
- ReiserFS *

If a file system is not supported or is corrupted, Acronis True Image WD Edition can copy data using a sector-by-sector approach.

** The Ext2/Ext3, and ReiserFS file systems are supported only for disk or partition backup/recovery operations. You cannot use Acronis True Image WD Edition for file-level operations with these file systems (file backup, recovery, search, as well as image mounting and file recovering from images), as well as for backups to disks or partitions with these file systems.*

1.3.4 Supported storage media

- Hard disk drives*
- Networked storage devices
- CD-R/RW, DVD-R/RW, DVD+R (including double-layer DVD+R), DVD+RW, DVD-RAM, BD-R, BD-RE**
- USB 1.0 / 2.0 / 3.0, FireWire (IEEE-1394) and PC card storage devices
- REV®, Jaz® and other removable media

* Acronis True Image WD Edition does not support dynamic and GPT disks.

** Burned rewritable discs cannot be read in Linux without a kernel patch.

2 Acronis True Image WD Edition installation and startup

2.1 Installing Acronis True Image WD Edition

To be able to install the program you need at least one Western Digital hard drive to be attached.

To install Acronis True Image WD Edition:

- Run the Acronis True Image WD Edition setup file.
- In the Install Menu, select the program to install: Acronis True Image WD Edition.
- Follow the install wizard instructions on the screen.



Typical, **Custom** and **Complete** installation is available. Having pressed **Custom**, you can choose not to install **Rescue Media Builder**.

With **Rescue Media Builder** you can create bootable rescue disks (see details in Creating bootable media (p. 53)). Installing the **Bootable Rescue Media Builder** will allow you to create bootable media or its ISO image at any time from the main program window or by running **Bootable Rescue Media Builder** on its own.

When installed, Acronis True Image WD Edition creates a new device in the Device Manager list (Control Panel → System → Hardware → Device Manager → Acronis Devices → Acronis True Image Backup Archive Explorer). Do not disable or uninstall this device, as it is necessary for connecting image archives as virtual disks (see Exploring archives and mounting images).

2.2 Running Acronis True Image WD Edition

You can run Acronis True Image WD Edition in Windows by selecting **Start** → **Programs** → **Acronis** → **Acronis True Image WD Edition** → **Acronis True Image WD Edition** or by clicking on the appropriate shortcut on the desktop.

2.3 Removing Acronis True Image WD Edition

Select **Start** → **Settings** → **Control panel** → **Add or remove programs** → **<Acronis True Image WD Edition>** → **Remove**. Then follow the instructions on the screen. You may have to reboot your computer afterwards to complete the task.

If you use Windows Vista, select **Start** → **Control panel** → **Programs and Features** → **<Acronis True Image WD Edition>** → **Remove**. Then follow the instructions on the screen. You may have to reboot your computer afterwards to complete the task.

3 General information and proprietary Acronis technologies

3.1 Disk/partition images

A backup archive is a file or a group of files (also called "backups" in this guide), that contains a copy of all information stored on selected disks/partitions.

Backing up disks and partitions is performed in the following way: Acronis True Image WD Edition stores a sector-by-sector snapshot of the disk, which includes the operating system, registry, drivers, software applications and data files, as well as system areas hidden from the user. This procedure is called "creating a disk image," and the resulting backup archive is often called a disk/partition image.

*By default, Acronis True Image WD Edition stores only those hard disk parts that contain data (for supported file systems). Furthermore, it does not back up swap file information (pagefile.sys under Windows XP and later) and hiberfil.sys (a file that keeps RAM contents when the computer goes into hibernation). This reduces image size and speeds up image creation and recovery. However, you might use the **Create an image using the sector-by-sector approach** option that lets you include all of the sectors of a hard disk in an image.*

A partition image includes all files and folders. This includes all attributes (including hidden and system files), boot record, and FAT (file allocation table); as well as files in the root directory and the zero track of the hard disk with the master boot record (MBR).

A disk image includes images of all disk partitions as well as the zero track with the master boot record (MBR).

By default, files in all Acronis True Image WD Edition archives have a ".tib" extension. Do not change this file extension.

It is important to note that you can recover files and folders from disk/partition images. To do so, mount the image as a virtual disk (see Exploring archives and mounting images) or start the image recovery and select **Recover chosen files and folders**.

3.2 Full backup

Acronis True Image WD Edition can create full backups.

A **full backup** contains all data at the moment of backup creation. It forms a base for further incremental backup or is used as a standalone archive (incremental backups are not available in the current version of the product).

A standalone full backup might be an optimal solution if you often roll back the system to its initial state or if you do not like to manage multiple files.

3.3 Backup file naming conventions

Let's remember that Acronis True Image WD Edition may split a full archive into volumes either when a user sets the splitting option or when a large backup having a size bigger than 4GB is saved to a FAT32 disk. See "Backup archive components" in Acronis True Image WD Edition basic concepts.

Though users may assign any name to backups, many would still prefer using automatic naming and the below information may come in handy when viewing the contents of a backup archive storage in Windows Explorer.

1) When saved to a FAT32 disk, such backup may be split into volumes with the names SystemBackup_mm_dd_yyyy1.tib, SystemBackup_mm_dd_yyyy2.tib, SystemBackup_mm_dd_yyyy3.tib, etc.

As in this case the subsequent automatically scheduled backups will replace the previous one (once every seven days by default) only after the next backup finishes (to keep the old backup in the event of the current backup's failure), the backup filename(s) will be alternately named SystemBackup_mm_dd_yyyy.tib and SystemBackup_mm_dd_yyyy(1).tib.

2) In some cases when you create a new full backup task at a new destination, the backup gets the name "MyBackup_mm_dd_yyyy.tib".

If a backup is split (either automatically, e.g. due to the 4GB file size limit on FAT32 disks or when configuring a backup task), the constituent backup files (volumes) are named as follows:

MyBackup_mm_dd_yyyy1.tib...MyBackup_mm_dd_yyyyN.tib, where N is the number of volumes

3) When you back up, for example, partitions C and D, the backup gets the name "System_C_D_mm_dd_yyyy.tib".

4) When you rename backups on the Data recovery and backup management screen, a backup is renamed only in the program's metadata database; however, backup file names on the disk remain unchanged.

3.4 Viewing disk and partition information

You can change the way data is represented in all schemes you see in various wizards.

The header may have up to three icons: **Columns**, **Arrange Icons by** and **Disk properties**, the latter duplicated in the context menu opened by right-clicking objects.

To sort messages by a particular column, click the header (another click will switch the messages to the opposite order) or the **Arrange Icons by** button and select the column.

To select which columns to view, right-click the headers line or left-click the **Columns** button. Then flag the columns you want to display. When left-clicking the **Columns** button, you can also change the display order of columns using the **Move Up** and **Move Down** buttons.

If you click the **Disk properties** button, you will see the selected partition or disk properties window.

This window contains two panels. The left panel contains the properties tree and the right describes the selected property in detail. The disk information includes its physical parameters (connection type, device type, size, etc.); partition information includes both physical (sectors, location, etc.), and logical (file system, free space, assigned letter, etc.) parameters.

You can change the width of a column by dragging its borders with the mouse.

3.5 Acronis DriveCleanser

Acronis True Image WD Edition contains utilities for secure destruction of data on an entire hard disk drive, individual partitions. When replacing your old hard drive with a new, higher-capacity one, you may unwittingly leave on the old disk lots of personal and confidential information that can be recovered, even if you have reformatted it.

The Acronis DriveCleanser provides for the destruction of confidential information on hard disk drives and/or partitions with the help of techniques that meet or exceed most national and state standards. You can select an appropriate data destruction method depending on the importance of your confidential information.

3.6 Booting from system image tib files

Users of the Enterprise and Ultimate editions of Windows 7 can now test whether they will be able to boot from the recovered system partition. Acronis True Image WD Edition allows booting from a tib file containing a system partition image. So if you are able to boot from such backup, you almost certainly will be able to boot after an actual system recovery from that backup. When you choose a tib file to boot from, Acronis True Image WD Edition creates a temporary vhd file by converting this tib file, so your hard disk must have enough free space for storing it. Then the program adds a new item to the Windows boot loader list. When you select the tib file in the boot loader list, your computer will actually boot from that temporary vhd file. After testing the bootability of the tib file, you can remove the file from the boot loader list and delete the temporary vhd file, though you can keep it.

4 Preparing for disaster recovery

4.1 How to best prepare for a disaster

Let us remind you of Murphy's Law: "Whatever can go wrong will go wrong" (and at the worst possible time, in the worst possible way). And some people say that Murphy was an incurable optimist. So be warned – your computer may crash and will eventually crash (and maybe just at the worst possible moment). We may interpret Murphy's Law the other way around – it is vitally important to consider all the possible things that can go wrong and act so as to prevent them. The best way to counteract a possible disaster is by taking the necessary precautionary measures:

- 1) To be better prepared for a disaster, you need to make a full backup of your system disk (or at the very least the partition containing Windows and your applications).
- 2) Whenever possible, you should store your system drive image on a hard drive other than your primary hard disk C:, preferably on an external one. This gives an additional guarantee that you will be able to recover your system if your primary hard disk drive fails. Furthermore, it is usually better to keep your personal data separate from your operating system and applications, for example, on disk D:. Such an arrangement speeds up the creation of your system and data disks (or partitions) images and reduces the amount of information you will need to recover. This makes the backup file of your system disk much smaller and recovery can be easier. In its turn, the smaller the backup file size, the less chance of its corruption and the less time required for your system recovery.
- 3) If you store your data (documents, videos, photos, etc.) on a non-system disk, e.g. using the arrangement described in item 2), it needs to be backed up too. You can either back up the folders containing your data or create a data disk image. Remember that the imaging procedure is much faster than copying files and could speed up the backup process significantly when it comes to backing up large volumes of data. Incidentally, if the image file becomes corrupted for some reason, it is sometimes possible to mount the image and save most files and folders by copying them from the mounted image using Windows Explorer.
- 4) As recovery of your system from a disaster in most cases will be done after booting from the rescue media, you **must** test the rescue media as described in the next section - Testing bootable rescue media.

4.1.1 Recommendations for testing that your backups can be used for recovery

- 1) Even if you start recovery of the active partition in Windows, the program will reboot into the Linux environment after the recovery process starts because Windows cannot be left running while the recovery of its own partition is being carried out. So you will recover your active partition under the recovery environment in all cases. If you have a spare hard drive, we strongly recommend you to try a test recovery to this hard drive booting from the rescue media which uses Linux. If you do not have a spare drive, please, at least validate the image in the recovery environment. A backup that can be read during validation in Windows, **may not always be readable under Linux environment**.

When you use the Acronis True Image WD Edition rescue media, the product creates disk drive letters that might differ from the way Windows identifies drives. For example, the D: drive identified in the standalone Acronis True Image WD Edition might correspond to the E: drive in Windows. To be on the safe side, it is advisable to assign unique names to all partitions on your hard drives. This will make finding the disk containing your backups easier.

2) It may also be useful to complete all the steps in the Recovery Wizard right up to the Summary screen, but not click the Proceed button. This will allow you to simulate the recovery process and to make sure that Acronis True Image WD Edition recognizes both the drive containing your backups and the target drive. After completing all the Recovery Wizard's steps click **Cancel** on the Summary screen. You may repeat this until you feel sure of your settings and choices.

4.1.2 Additional recommendations

1) Many IT professionals recommend that you have at least two copies of your system backup (three are even better). To be on the safe side, it is further recommended to keep one copy of a backup in a different location from the other (preferably on other premises – for example, at work or at a friend's home, if you use the backed up computer at home). One more argument in favor of several backups: when starting recovery, Acronis True Image WD Edition deletes the target partition (or disk), so when you have just a single backup, the moment the system partition is deleted on the computer being recovered you are at great risk - the only thing you have is the image being recovered and if it is corrupted you are in big trouble.

2) It is better to format the hard drive used for storing your backups to the NTFS file system rather than FAT32. This is due to the 4GB file size limit on FAT32 disks. So if your backup has a size of about 100GB, Acronis True Image WD Edition will split it into 25 files. When there are several such full backups on the hard disk, the number of files will multiply accordingly. This may be inconvenient if, for example, you would like to move the backup to another location using Windows Explorer.

3) If you have only one computer at home, it is advisable to print some information that may be helpful in recovering from a disaster, because you may not be able to use the Internet. Keep the printed material in a safe place along with the rescue CD/DVD or another rescue media.

4.2 Testing bootable rescue media

To maximize the chances of your computer's recovery if need arises, you must test that your computer can boot from the rescue media. In addition, you must make sure that the recovery media contains all drivers required for operation of your mass storage devices and network adapter.

1) If you purchased the program after downloading it, you absolutely must create a bootable rescue CD (or other rescue media, for example, a USB stick) following the recommendations given in the User's Guide or program's Help and then make sure this rescue media is bootable on your computer.

You must configure your computer so as to enable booting from the rescue media and make your rescue media device (CD-ROM/DVD-ROM drive or USB stick) the first boot device. See Arranging boot sequence in BIOS (p. 93);

In case you have a rescue CD, press a key to start booting from the CD, as soon as you see the prompt "Press any key to boot from CD". If you fail to press a key within five seconds, you will need to restart the computer. When using other rescue media, the procedure will be similar.

2) After the computer boots into the recovery environment, check that it detects all the hard drives you have in your system, including external ones, if you use them for storing backups. Incidentally, you must attach the external drive(s) before booting from the rescue media, otherwise the recovery environment might not detect the drive(s).

3) If you store your backups on the network, you should also check that you can access the network in the recovery environment. When booted from the rescue media, Acronis True Image WD Edition might not detect the network. If no computers are visible on the network, but the Computers near me icon is found under My Computer, ensure that a DHCP server is running on your network. If you

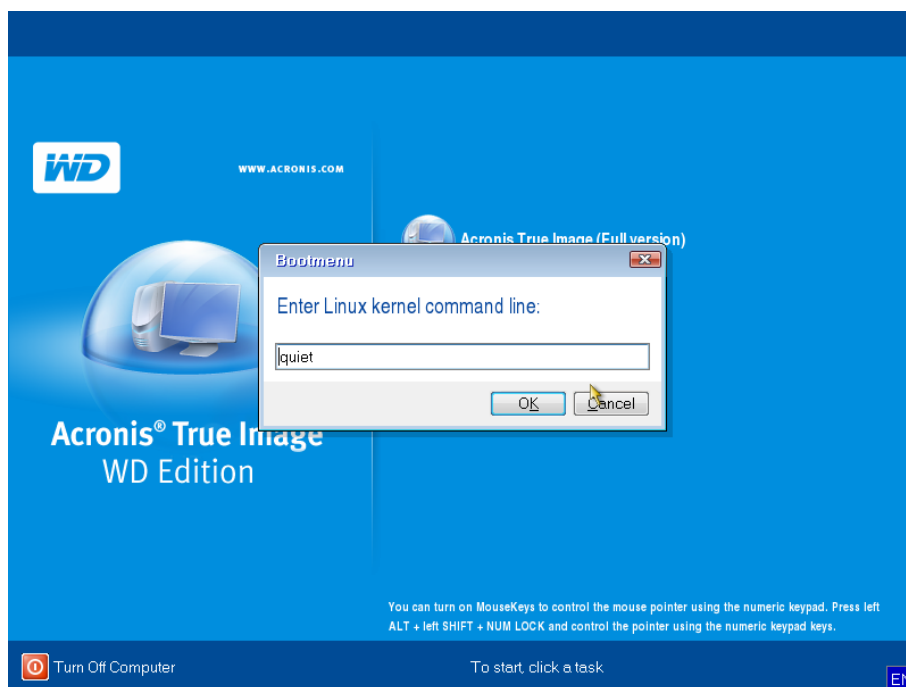
don't use a DHCP server, specify network settings manually in the window available at Tools & Utilities ® Options ® Network adapters.

If the **Computers near me** icon is not available under **My Computer**, there may be problems either with your network card or with the card driver shipped with Acronis True Image.

Selecting video mode when booting from the rescue media

When booting from the rescue media the optimal video mode is selected automatically depending on the specifications of your video card and monitor. However, sometimes the program can select the wrong video mode, which is unsuitable for your hardware. In such case you can select a suitable video mode as follows:

1. Start booting from the rescue media. When the boot menu appears, hover the mouse over Acronis True Image WD Edition (Full version) item and press the F11 key.
2. When the command line appears, type "vga=ask" (without quotes) and click **OK**.



3. Select Acronis True Image WD Edition (Full version) in the boot menu to continue booting from the rescue media. To see the available video modes, press the Enter key when the appropriate message appears.

4. Choose a video mode you think best suitable for your monitor and type its number in the command line. For instance, typing 338 selects video mode 1600x1200x16 (see the below figure).

```
Press <ENTER> to see video modes available, <SPACE> to continue, or wait 30 sec
Mode: Resolution: Type: Mode: Resolution: Type: Mode: Resolution: Type:
0 F00 80x25 UGA 1 F01 80x50 UGA 2 F02 80x43 UGA
3 F03 80x28 UGA 4 F05 80x30 UGA 5 F06 80x34 UGA
6 F07 80x60 UGA 7 320 320x200x8 VESA 8 321 320x400x8 VESA
9 322 640x400x8 VESA a 323 640x480x8 VESA b 324 800x600x8 VESA
c 325 1024x768x8 VESA d 326 1152x864x8 VESA e 327 1280x960x8 VESA
f 328 1280x1024x8 VESA g 329 1400x1050x8 VESA h 32a 1600x1200x8 VESA
i 32b 1792x1344x8 VESA j 32c 1856x1392x8 VESA k 32d 1920x1440x8 VESA
l 32e 320x200x16 VESA m 32f 320x400x16 VESA n 330 640x400x16 VESA
o 331 640x400x16 VESA p 332 800x600x16 VESA q 333 1024x768x16 VESA
r 334 1152x864x16 VESA s 335 1280x960x16 VESA t 336 1280x1024x16 VESA
u 337 1400x1050x16 VESA v 338 1600x1200x16 VESA w 339 1792x1344x16 VESA
x 33a 1856x1392x16 VESA y 33b 1920x1440x16 VESA z 33c 320x200x32 VESA
33d 320x400x32 VESA 33e 640x400x32 VESA 33f 640x400x32 VESA
340 800x600x32 VESA 341 1024x768x32 VESA 342 1152x864x32 VESA
343 1280x960x32 VESA 344 1280x1024x32 VESA 345 1400x1050x32 VESA
346 1600x1200x32 VESA 347 1792x1344x32 VESA 348 1856x1392x32 VESA
349 1920x1440x32 VESA 300 640x400x8 VESA 301 640x400x8 VESA
303 800x600x8 VESA 305 1024x768x8 VESA 307 1280x1024x8 VESA
30e 320x200x16 VESA 311 640x400x16 VESA 314 800x600x16 VESA
317 1024x768x16 VESA 31a 1280x1024x16 VESA
Enter a video mode or "scan" to scan for additional modes: _
```

Incidentally, when there is a digit or letter before a three-digit number, you can also select such video mode by typing the corresponding single digit or letter ("v" in our instance).

5. Wait until Acronis True Image WD Edition (Full version) starts and make sure that the quality of the Welcome screen display on your monitor suits you.

To test another video mode, close Acronis True Image WD Edition and repeat the above procedure.

After you find the optimal video mode for your hardware, you can create a new bootable rescue media that will automatically select that video mode.

To do this, start Acronis Media Builder, select the required media components, and type the mode number with the "0x" prefix (0x338 in our instance) in the command line at the "Bootable media startup parameters" step, then create the media as usual.

4.3 Creating a custom rescue CD

If the recovery environment cannot detect some of the hard disk drives or the network adapter, usually there is a problem with the drivers. Acronis rescue CD cannot contain drivers for all hardware on the market. So when the standard rescue CD lacks some of your hardware drivers, you need to create a custom one.

The Linux-based recovery environment used by Acronis does not provide the ability for users to add new drivers. Because of this, you should request Acronis Customer Service Department to create a custom rescue CD that will have all the drivers you need.

Before making a request, collect the information about your system. Select **Generate System Report** in the Help menu. Acronis True Image WD Edition will automatically collect the required information and display a list of what is collected in the report. In the process of creating the report the program may install some components required for collecting the necessary information. When the report is complete, click **Save As** and select the desired folder or leave the default **My Documents** folder. The program will archive the report into a zip file. Send the file to the Acronis Customer Service Department. They will build an iso image of a custom rescue media compatible with your computer hardware and send you an iso file. Burn this file to a CD/DVD using a program that can handle iso

files such as Nero. Incidentally, this report may also be useful when you request the Acronis Customer Service Department to help you with a problem.

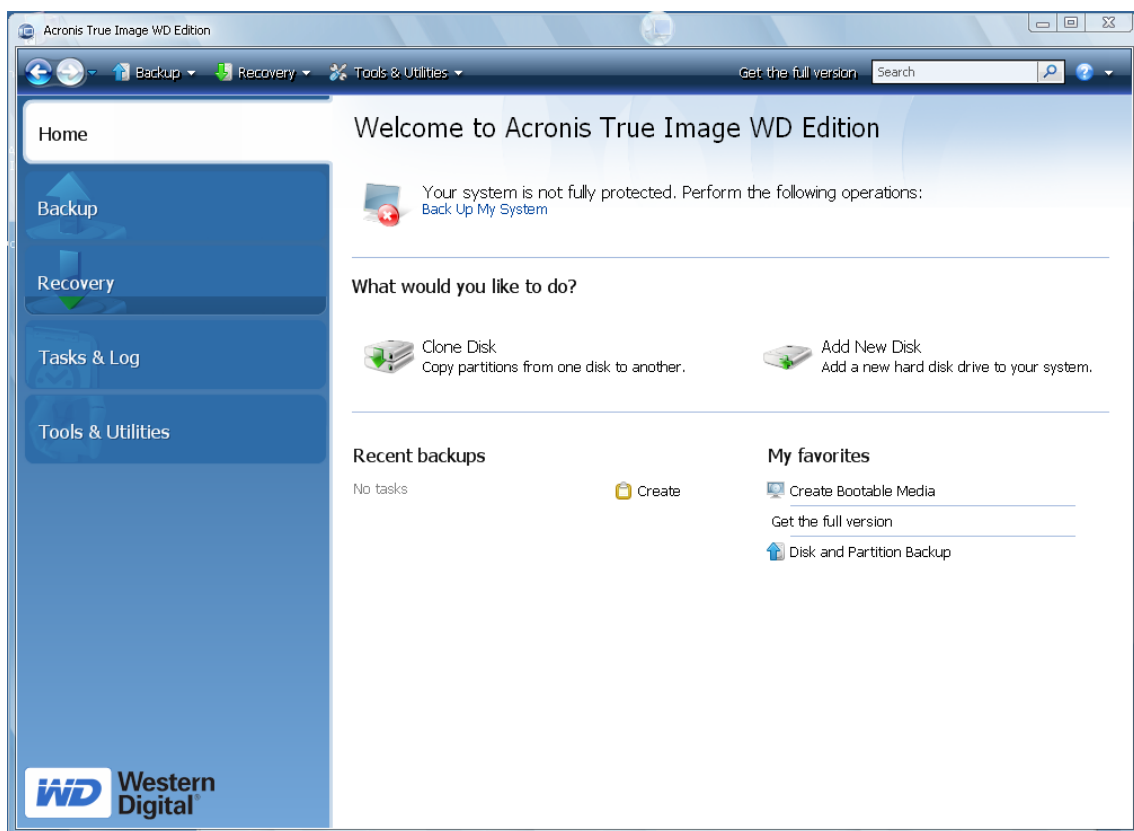
After burning your custom rescue CD, test it to make sure that your hard disk drives and network adapter are now detected in the recovery environment.

5 Getting to know Acronis True Image WD Edition

5.1 Program workspace

Starting Acronis True Image WD Edition takes you to the Welcome screen. This screen provides quick access to backup and recovery features, as well as highlights any issues with your system's protection.

Your system is considered fully protected when it is backed up and a bootable rescue media is created. If some of the aforementioned have not been done, Acronis True Image WD Edition shows the following links allowing to solve the protection issues: Back Up My System, Create Bootable Rescue Media. After an issue is solved, the corresponding link disappears.

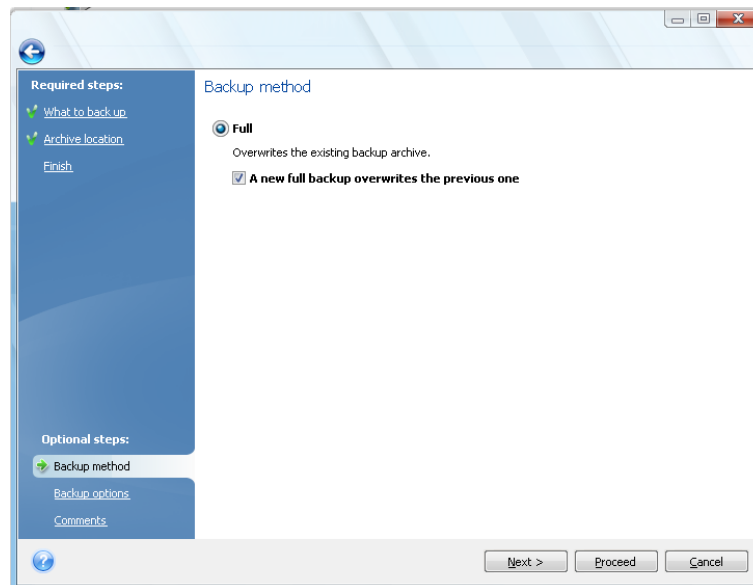


Clicking the items in the right pane takes you to the corresponding screen where you can either start the backup or recovery task immediately or make further selections.

The **My favorites** area in the right pane lists the features you have used most often and provides shortcuts to them in case you would like to use the features again. The **Recent backups** area lists the backups you have recently run and allows you to update the backup archives with just one click.

You can easily access the Acronis True Image WD Edition features through the so called *sidebar* occupying the left side of the screen. Choosing an item on the sidebar takes you to a screen, where you can access the corresponding features.

Acronis True Image WD Edition uses wizards, which guide you through many operations. Like the main program window, wizards also have the sidebar listing all the steps (both required and optional) needed for completing the operation. For example, see the Backup Wizard screen shot below.



The completed steps are marked with green checkmarks. The green arrow shows the current step. After you complete all the required steps and come to the **Finish** step, the program displays the Summary screen. If you wish to omit the optional steps, read the summary of the operation to be performed (to make sure that the default settings satisfy you) and then click **Proceed** to start the task. Otherwise, click **Options** to go to the optional steps where you can change the default settings for the current task.

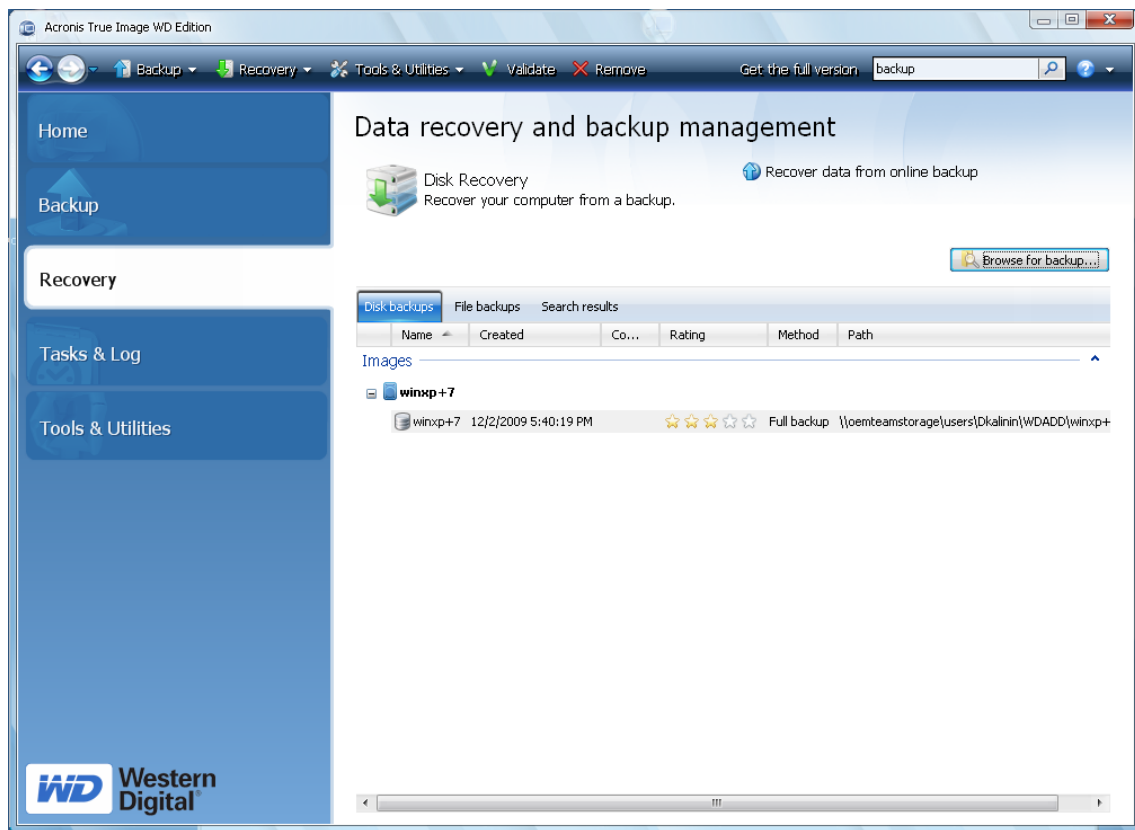
Taskbar notification area icons

During most of the operations, special indicator icons appear in the Windows taskbar notification area (the right portion of the status bar with the clock). If you mouse over the icon, you will see a tool tip indicating the operation's progress or state. Right-clicking on the icon opens a shortcut menu where you can change operation's status or cancel the operation if necessary. This icon doesn't depend on the main program window being open.

5.2 Main screens

And now let's get acquainted with some of the other screens you will use while working with Acronis True Image WD Edition.

To go to one more screen of interest, click **Recovery** on the sidebar.

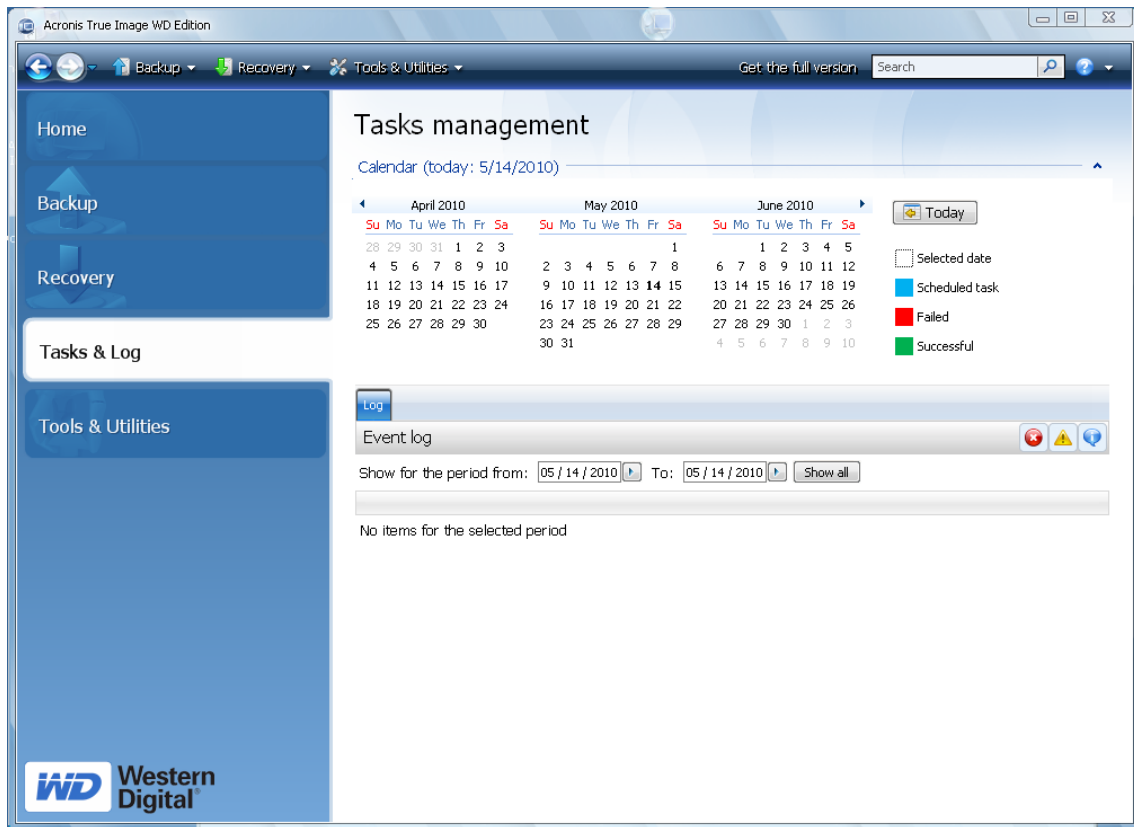


The **Data recovery and backup management** screen gives detailed information on your backup archives and provides for quickly performing operations on these archives – Recover, Validate, Move, Remove, Explore backup archives, as well as Mount image backups by right-clicking on an archive and choosing the required operation. This starts the appropriate wizard or performs the appropriate action.

Here you can also edit comments for backups, see detailed information on the backups, and assign ratings to your backups. For instance, you may want to assign a high rating to an important backup. A backup rating is indicated by the number of "stars" in the **Rating** column (more stars means a higher rating). The default rating is three stars, but you can raise or lower it by clicking on the stars in the column. Ratings might save you a lot of time you will otherwise spend on exploring multiple files in your backup archives, trying to guess which of the outdated backups can be deleted without losing important data.

Furthermore, this screen shows the results of searches for backup archives and their content. To perform a search, enter a search string into the Search field at the top right of the Acronis True Image WD Edition window and then click the magnifying glass icon. For more information see Searching.

Another useful screen shows the log of program operations. A calendar provides quick access to the logs (for past dates). You just click on a desired date. For more information see Viewing Tasks and Logs.

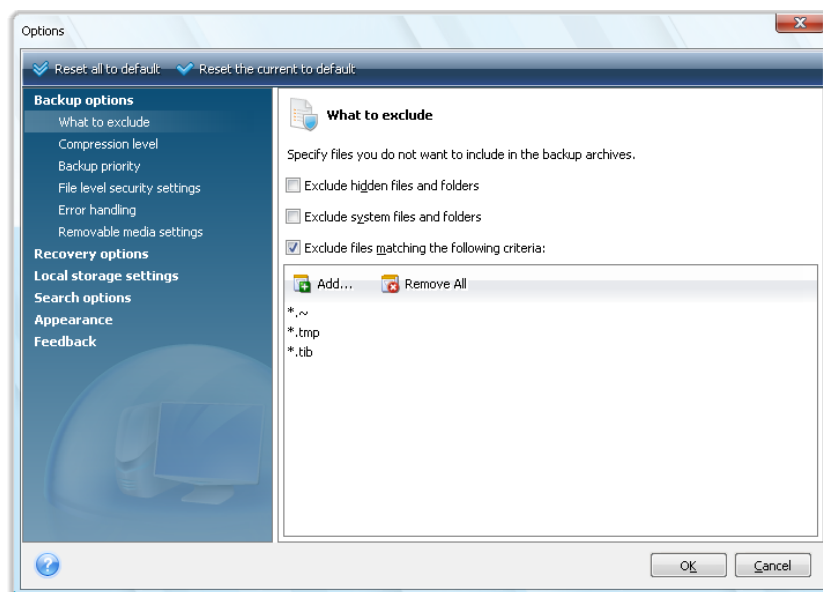


We will not bore you with a description of other screens, because many of them are self-explanatory and some are described in the appropriate chapters of this guide. In addition, you can always open contextual help by clicking the corresponding button.

Incidentally, you can also select most of the features through the main program menu, which is always at your disposal on the toolbar.

5.3 Options screen

Acronis True Image WD Edition has options related to its appearance and various program functions. To view or edit the default options, choose **Tools & Utilities**→ **Options** in the main program menu.



The **Backup options** item provides for making settings to be used by default in any backup task. You can modify the settings depending on your backup needs. For detailed information on the backup options and possible settings see *Fine-tuning your backups*. In addition, you can change the backup options while configuring a specific backup task. In such case the changed options will be used only for this task.

Similarly, the **Recovery options** item provides for making settings to be used by default by any recovery task. For detailed information on the recovery options and possible settings see *Setting default recovery options*. As with the backup options, you can change the recovery options for a specific recovery task.

The **Local storage settings** item provides for making other settings related to the backup process, for example, they may have a more or less noticeable effect on the backup process speed. For more information see *Fine-tuning your backups*.

The **Search options** allow you to enhance the Search function by integrating it with Windows Search or Google Desktop search engines. If you have one of those search engines installed, you can include tib files in their index files by selecting the appropriate box in the **Desktop search options** window. For more information see *Windows Search and Google Desktop integration*

The **Appearance** options allow modifying the appearance of the program's user interface by selecting a font to be used on screens, in dialogs, etc. You can also modify a font to be used in the menu items. To view the appearance of a concrete font, click the "..." button, select the font and have a look at the sample text. If you are satisfied with the font's appearance, click **OK**, otherwise try another font or click **Cancel**. In addition, the **Appearance** options let you filter all tasks created on your computer. By default you see only your own tasks, but you have the option to view or manage tasks created by other users. To do so, choose **Filter** and unselect the **Show only tasks created by a current user** box.

The **Feedback** option allows you to quit the Acronis Customer Experience Program, if you decided to join it during Acronis True Image WD Edition installation or join the program by selecting the **Yes, I**

want to participate in the program radio button. If you want to know more about the Customer Experience Program, click the **Learn more** link.

If modifying the default options does not provide the desired results or if you just want to restore the default options values set during Acronis True Image WD Edition installation, click **Reset all to default** on the toolbar. When you need to set the default values only for a selected option, click **Reset the current to default** on the toolbar.

6 Creating backup archives

6.1 Preparing for your first backup

First of all you should decide where to store your backups. Acronis True Image WD Edition supports quite a lot of storage devices. For more information see Supported storage media. Since hard disk drives are now quite inexpensive, in most cases purchasing an external hard drive for storing your backups will be an optimal solution. In addition to enhancing the security of your data – you can keep it off-site (for example, at home if you back up your office computer and vice versa), many models are hot-pluggable, so you can attach and detach the drive as required. You can choose various interfaces – USB, FireWire, eSATA depending on the configuration of your computer ports and the required data transfer rate. In many cases the best choice will be an external USB hard drive. If you have a Gigabit Ethernet home network and a dedicated file server or NAS, for example, Western Digital My Book World NAS Server, you can store backups on the file server or NAS practically like onto an internal drive. Blank optical discs such as DVD-R, DVD+R are very cheap, so they will be the lowest cost solution for backing up your data, though the slowest one, especially when backing up directly to DVDs. Furthermore, if your backup consists of several DVDs, data recovery from such backup will require a lot of disc swapping.

Due to the necessity of swapping discs, it is strongly recommended to avoid backing up to DVDs if the number of discs is more than three.

If you decide to use an external hard drive, NAS, etc., you will need to check whether Acronis True Image WD Edition detects the selected backup storage.

Some external hard drives are sold preformatted FAT32. If so, it is better to convert the external hard drive for backups from FAT32 into NTFS, because of the 4GB file size limit of the FAT32 system. Due to this limitation, large backup files will automatically split into 4GB chunks, thus increasing the chance that something will go wrong during data recovery.

If you plan to use an external USB hard drive with your desktop PC, connecting the drive to a rear connector using a short cable will usually provide the most reliable operation, reducing the chance of data transfer errors during backup/recovery.

6.2 Deciding what data to back up

As operating systems and application software become ever larger (for example, Windows Vista x64 requires 15GB of free space on a hard disk), usually it will take you several hours to reinstall your operating system and application software from original CDs or DVDs on a new hard disk. Furthermore, the practice of buying application software by downloading from the Internet is becoming more and more popular. If you lose your registration information, for example, the activation key and/or registration number, which are usually sent by software vendors by e-mail, you may have problems with restoring your right to use the application. So making a backup of your entire system disk (making a disk image) will save you a lot of valuable time in case of a disaster, as well as safeguard you against other possible problems.

Backing up the entire system disk takes more disk space, but enables you to recover the system in minutes in case of a system crash or hardware failure (for details see Disk/partition images (p. 12)).

You might think it would take a while to make a copy of your entire hard disk, but the proprietary technologies used in Acronis True Image WD Edition ensure that image creation is quite fast.

You should create images of your primary disk and any other partition you normally use. If you have multiple partitions on a drive, it is advisable to include all of them in the image, because failure of the hard drive in most cases will mean that all the partitions it contains also fail.

Although we strongly recommend you to create images of your hard disk on a regular basis, that is just part of a reliable backup strategy.

6.3 Some typical backup scenarios

Below are several scenarios of "classic" backups describing frequently used backup tasks. Depending on your backup strategy, you may find some of them useful.

6.3.1 Backing up a system partition

It is recommended to back up the system partition when your C: disk consists of a single partition, though in this case partition backup is equivalent to system disk backup. It is also makes sense to back up the system partition if it contains all your applications and important data or if you do not have enough free space for backing up the entire system disk. A system partition backup would be most helpful when you need to recover the operating system corrupted by a virus, malware or, for example, after Windows update installation. Recovery on a new hard disk drive is possible too, though it may be a bit complicated in case you want to create more than one partition on the new hard disk. Otherwise it is better to back up the entire system disk, especially if it has hidden recovery or diagnostic partitions created by your computer's manufacturer. Furthermore, a system disk backup is more convenient when recovering on a new disk. Backing up the system partition may also be advisable when you like testing a lot of applications or games. Most applications cannot be uninstalled without a trace, including Acronis True Image WD Edition itself. You can make a basic system partition backup containing your operating system and main applications like MS Office and Outlook. Thereafter you will always be able to recover that basic system state after trying new programs – if you don't like them or if something goes wrong.

6.3.2 Backing up an entire system disk

When your backup storage device has enough free space, it is advisable to back up the entire system disk. Such a backup is most suitable for recovering your system and applications both when you need to recover them on the original hard disk drive or a new one, e.g. after your hard drive failed. Incidentally, if your system disk contains several partitions, an entire disk backup also provides for recovery of any individual partition.

Because system disk backups are the most important for disaster recovery, it is advisable to check both the system disk and the hard disk to be used as the backup storage for errors with the help of Microsoft's Chkdsk utility, which is part of Windows. The utility can repair errors and locate bad sectors.

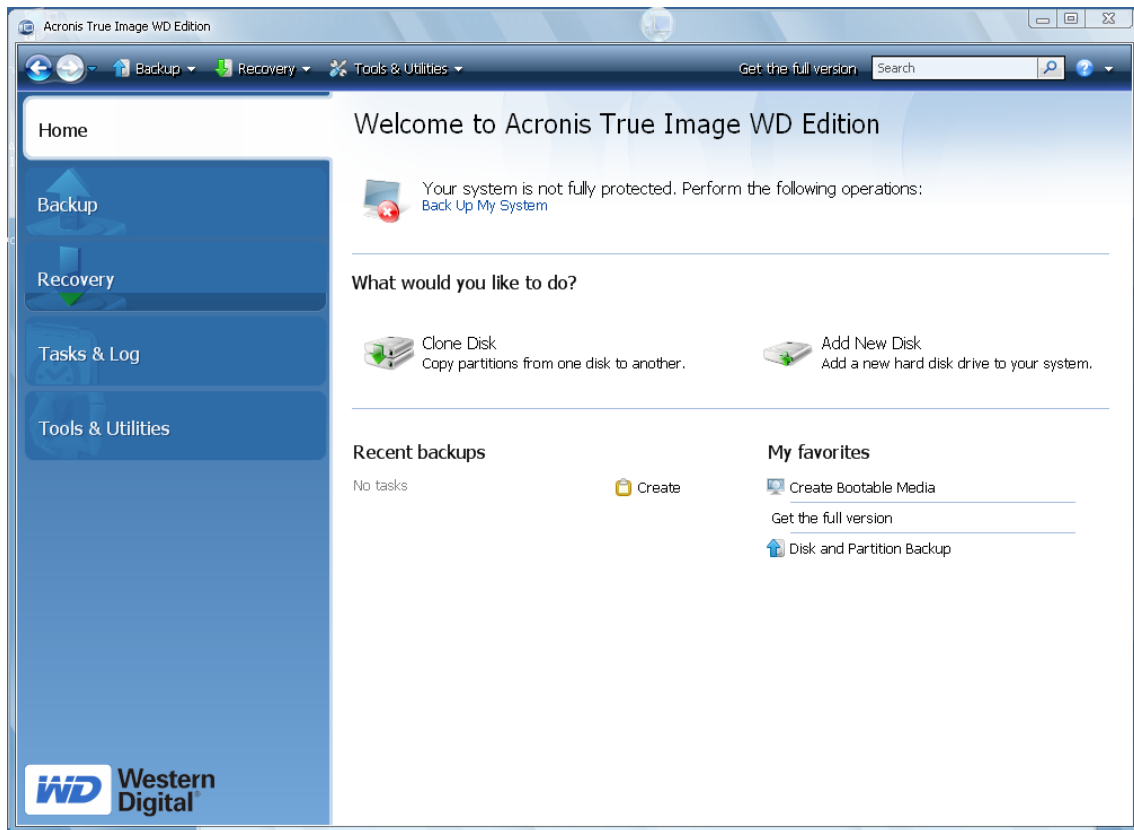
You can back up the system disk both in Windows and in the recovery environment. Before starting a system disk backup in Windows it is advisable to close such applications as MS Outlook and DBMS programs.

Though the program locks the system partition while making a so called "snapshot" (see Acronis True Image WD Edition basic concepts), some users still prefer backing up the system disk when Windows is not running.

The subsequent description is made under the assumption that you boot from your bootable rescue media and the program "sees" all your hard drives and other storage devices in the recovery environment. See Testing bootable rescue media.

Attach the external drive if it is to be used for backup storage and make sure that the drive is powered on. This must be done before booting from Acronis rescue media.

1. Arrange the boot sequence in BIOS so as to make your rescue media device (CD, DVD or USB stick) the first boot device. See Arranging boot sequence in BIOS (p. 93).
2. Boot from the rescue media and select Acronis True Image WD Edition (Full version).
3. Click the **My Disks** link under **Back Up** on the Welcome screen.



4. Select the system disk as the source for backup by checking the appropriate disk box (this will select all partitions on the disk, including the hidden ones).
5. Choose a target archive for the backup being configured – you can either add a new backup to an existing archive or create a new one. Choose the backup location and assign a name to the backup to be created. It is better to use meaningful names, e.g. Disk1_full.tib.
6. Carefully read the Summary of actions to be performed during backup and click **Proceed** if you are satisfied with the backup task settings, otherwise click **Options** on the Summary screen to change the settings.
7. Select a backup method. For a more detailed explanation of the methods see Full backup. When performing backups in the recovery environment many users prefer full backups, though you may choose another method depending on your needs.
8. Set the backup options. When backing up in the recovery environment you must set the options manually for each backup task. You can encrypt the backup for data protection and select a compression level (the program shows estimated backup sizes for each level). You can also choose to validate the backup immediately after its creation, though it can be done later. In any

case validation of a system disk backup is best performed in the recovery environment, as you will use the recovery environment when recovering the system partition or disk.

9. If you wish, provide comments to the backup. You will also be able to add comments later.
10. Click **Proceed** to start the backup.

It is extremely important to validate the system disk backup before trying to recover, because Acronis True Image WD Edition deletes the original partition(s) on the disk before starting recovery and if it finds a problem with the backup file during recovery, you are left with nothing. It is even better to try system disk recovery to a spare hard drive, if you have one.

6.3.3 Backing up a data partition or disk

Your personal data (MS Office documents, financial documents, pictures, music, videos, etc.) require protection in no less degree than your operating system. Such data is better kept separately from your operating system and applications on a dedicated partition or disk. This speeds up data partition or disk image backup, as well as recovery. It is recommended to perform data disk backup in Windows, because in most cases Windows drivers for storage devices operate better and faster than the respective Linux drivers used in the recovery environment. In addition, recovery of data disks and partitions usually occurs in Windows. Let's create a data disk backup task in Windows.

Attach the external drive if it is to be used as the backup destination and make sure that the drive is powered on. This must be done before starting Acronis True Image WD Edition.

1. Click the **My Disks** link under **Back Up** on the Welcome screen.
2. Select the box of your data partition or disk on the **What to back up** screen.
3. Choose a target archive for the backup task being configured – you can either add a new backup to an existing archive or create a new one. Choose the backup location and assign a name to the backup to be created. It is better to use meaningful names, e.g. Data_disk.tib. When you store different backup archives in the same location, e.g. on an external drive, you may want to create a new folder when creating a new backup archive. To do this, click **Create new folder** in the toolbar, then assign a meaningful name to the folder.
4. Carefully read the Summary of actions to be performed during backup and click **Proceed** if you are satisfied with the backup task settings, otherwise click **Options** on the Summary screen to change the settings.
5. Choose a backup method. For a more detailed explanation of the methods see Full backup. Let's reiterate that selection of the backup method may depend on the desired backup strategy.
6. Set the options for the backup task being created. For example, you can choose to validate the backup right immediately after its creation, though it can be done later.
7. If you wish, provide comments to the backup. You will also be able to add comments later.
8. Click **Proceed** when you are satisfied with the backup task settings.

If you have not included validation into the backup task settings, it is strongly recommended to validate the backup later – by performing the validation task manually. You should get into the habit of validating your backups.

6.3.4 Backing up to a network share

With Acronis True Image WD Edition you can back up your data to a network share. This may be desirable, for example, when you have a file server and want to use it for backing up data from PCs in your home network. Depending on your backup strategy, you may want to back up just files and folders or entire disks. One more consideration is the data transfer rate provided by your network.

For example, a Gigabit Ethernet network has a bandwidth sufficient for all amounts of data to be backed up. However backing up over Wi-Fi connection may be time-consuming when you need to back up a hundred gigabytes.

Files and folders or data partitions can be backed up and recovered in Windows. If you plan to back up your system disk or partition, please, make sure that the standalone version of Acronis True Image WD Edition can "see" the network share to be used for backups as system recovery will be done in the recovery environment. After booting from the rescue media make sure that you can browse to the share in the Backup wizard or Recovery wizard.

It may be advisable to first back up and recover some files to ensure that you can perform those operations over the network. In addition, it is not recommended to map the drive containing the network share. Specifying the UNC path makes it easier to establish network connection in most cases.

Let's suppose you want to back up your system partition.

1. Start Acronis True Image WD Edition and click the **My Disks** link under **Back Up** on the Welcome screen.
2. Select the check box of your system partition on the **Source selection** screen.
3. When you are connecting to a networked computer, in most cases you will need to provide the network credentials (user name and password) to access a network share. To do this, select the **Use NT authentication** box and enter the user name and password into the appropriate fields. Pressing the **Test authentication and connection** button allows testing the ability of the computer to connect to the selected network share. If testing results in an error message, check whether you provided the correct credentials and enter the right credentials for the network share. When the **Use NT authentication** box is left unselected, the computer will try to log on to the share with the credentials used for logging on to Windows. Having provided the required information, click **OK** to continue. Choose a target archive for the backup task being configured – you can either add a new backup to an existing archive or create a new one. It is better to use meaningful names, e.g. Disk_C.tib.
4. Carefully read the Summary of actions to be performed during backup and click **Proceed** if you are satisfied with the backup task settings, otherwise click **Options** on the Summary screen to change the settings.
5. Choose a backup method. For a more detailed explanation of the methods see Full backup. Let's reiterate that selection of the backup method may depend on the desired backup strategy.
6. Set the options for the backup task being created. You can choose to validate the backup immediately after its creation, though it can be done later.
7. If you wish, provide comments to the backup. You will also be able to add comments later.
8. Click **Proceed** when you are satisfied with the backup task settings.

7 Additional backup features

7.1 Backup Wizard – detailed information

The current version of Acronis True Image WD Edition allows you to choose only Disk backup type:

Disk backup:

- Choose the  **Disk and Partition Backup** parameter if you need to create an image of the entire disk or its partitions. Backing up the entire system disk (creating a disk image) takes up significant disk space, but enables you to recover the system in minutes in case of severe data damages or hardware failure.

We do not recommend backing up any data from drives protected by the BitLocker Drive Encryption feature, because in most cases recovering data from such backups will be impossible.

7.1.1 Selecting what data to back up

When the Backup Wizard screen appears, select what data to back up.

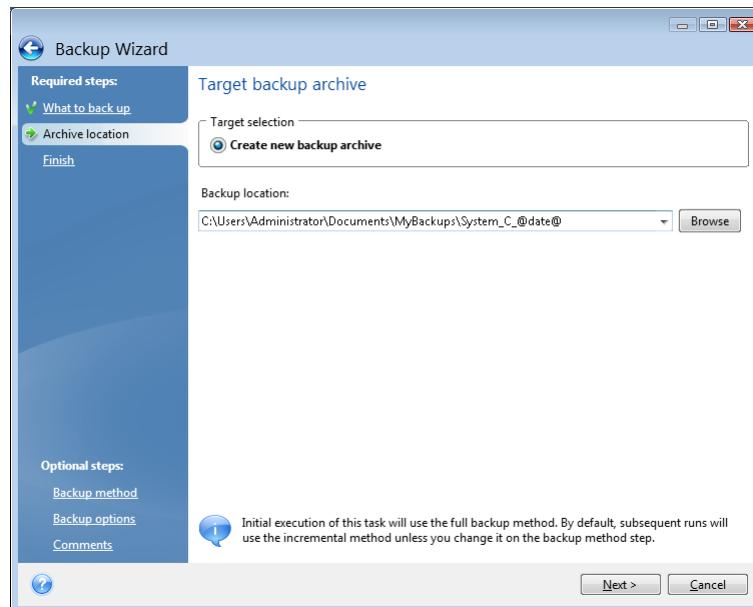
Disk and Partition Backup - select the disks or partitions to back up. You can select a random set of disks and partitions. The wizard's right pane shows the hard drives of your computer. Selecting a hard drive results in selecting all partitions on that drive. If a hard drive has more than one partition, you may want to select individual partitions for backing up. To do so, click on the Down arrow at the right of the drive's line. Select the desired partition(s) in the displayed partition list. By default the program copies only the hard disk sectors that contain data. However, sometimes it might be useful to make a full sector-by-sector backup. For example, perhaps you deleted some files by mistake and want to make a disk image before trying to undelete them because sometimes un-deleting may create havoc in the file system. To make a sector-by-sector backup, select the **Back up sector-by-sector (requires more storage space)** box. Please note that this mode increases processing time and usually results in a larger image file because it copies both used and unused hard disk sectors. In addition, when configuring a sector-by-sector backup of a complete hard disk you can include in the backup unallocated space on the hard disk by selecting **Back up unallocated space**. Thus you will include in the backup all physical sectors on the hard drive.

7.1.2 Selecting archive location

Select the location for the backup archive and specify the archive name.

If you are going to create a new archive (i.e. perform a full backup), select **Create new backup archive** and enter the path to the archive location and new archive file name in the **Backup Location:** field below or click **Browse**, select the archive location on the directory tree and enter the new file name in the **File name** line, or use the file name generator (a button to the right of the line).

If you want to change the location of added backup files, browse for a new backup location after clicking the **Browse** button, otherwise leave the location the same as that of the existing archive.



The "farther" you store the archive from the original folders, the safer it will be in case of disaster. For example, saving the archive to another hard disk will protect your data if the primary disk is damaged. Data saved to a network disk or removable media will survive even if all your local hard disks are damaged.

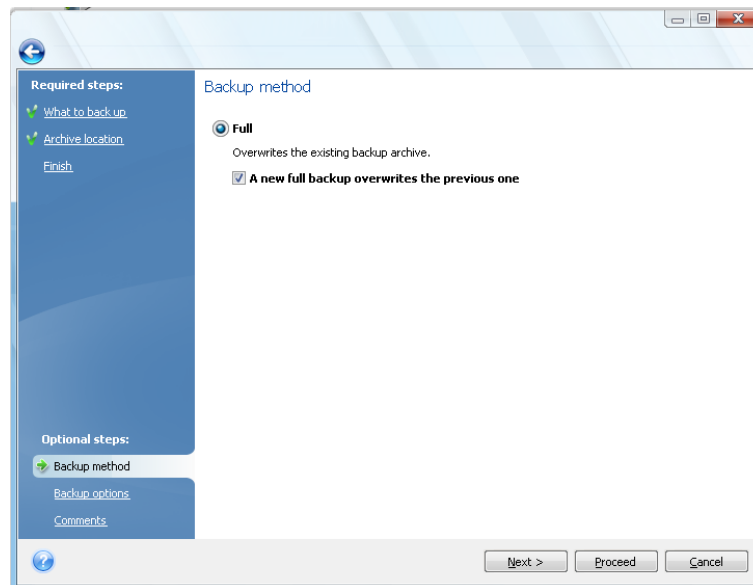
After selecting the archive location and naming the backup archive to be created, you have completed all the required steps for a backup task and this is confirmed by the fact that you come to the **Finish** step with the Summary of the backup task being displayed on the right pane. All the remaining steps are optional and in many cases you may omit them and just click **Proceed**. When you want to use the default backup options, you can omit the **Backup options** step, and so on.

Now let's see what optional steps you can set up while configuring a backup task. Click the **Options** button.

7.1.3 Backup method

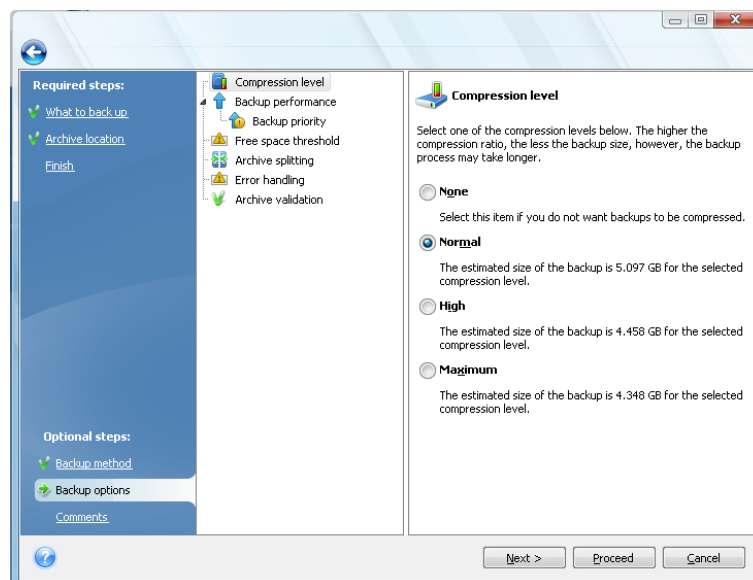
Select a full backup to be created. If you have not backed up the selected data yet, or the full archive is old and you want to create a new master backup file, choose full backup.

After selecting the **Full** method, you can also choose what to do with the previous full backup when creating a new one. By default Acronis True Image WD Edition overwrites the previous full backup, but you can choose to keep it by unselecting the **A new full backup overwrites the previous one** box.



7.1.4 Selecting the backup options

Select the backup options (that is, backup file-splitting, compression level, etc.). The settings of the options will be applied only to the current backup task.



Or, you can edit the default backup options and local storage settings if you want to save the current settings for future tasks. For more information see [Fine-tuning your backups](#).

7.1.5 Providing a comment

Providing a comment for the archive can help identify the backup and prevent you from recovering the wrong data. However, you can choose not to make any notes. The backup file size and creation date are automatically appended, so you do not need to enter this information.

In addition, you can provide or edit a comment after the backup has been executed. To edit or add a comment, go to the **Data recovery and backup management** screen by clicking **Recovery** on the sidebar, choose the appropriate backup, right-click and select **Edit comments** in the shortcut menu.

7.1.6 The backup process

Clicking **Proceed** after completing all the optional steps you need for configuring the current backup task will start the task execution.

The task progress will be shown in a special window. You can stop the procedure by clicking **Cancel**.

You can also close the progress window by clicking **Hide**. The backup creation will continue, but you will be able to start another operation or close the main program window. In the latter case, the program will continue working in the background and will automatically close once the backup archive is ready. If you prepare some more backup operations, they will be queued after the current one.

7.2 Fine-tuning your backups

You can fine-tune your backups to specific tasks. Such fine-tuning is made by configuring backup options before starting a backup task.

You can set temporary backup options by changing the default backup options while creating a backup task. If you would like to use the changed options for future tasks, make appropriate changes in the default backup options after selecting **Tools & Utilities** → **Options** → **Backup options**. Incidentally, you can always restore the default backup options to the values preset during installation of Acronis True Image WD Edition. To do this, click **Reset all to default** on the toolbar of the **Options** window. To reset just a single backup option, select it on the left pane and click **Reset the current to default**.

*Clicking **Reset all to default** will reset all the default options (for backup, recovery, etc.) to their preset values, so this button should be used with caution.*

7.2.1 Backup options

7.2.1.1 Compression level

The preset is **Normal**.

Let's consider such an example - you need to backup to a USB stick some files with a total size comparable to or exceeding the USB stick's capacity and want to make sure that the stick accommodates all the files. In this case use the **Maximum** compression for the files to be backed up. However, you should take into account that the data compression ratio depends on the type of files stored in the archive, for example, even the **Maximum** compression will not significantly reduce the backup size if it contains files with already compressed data like .jpg, .pdf or .mp3. It does not make any sense to select the **Maximum** compression for such files because in this case the backup operation will take significantly longer and you will not get an appreciable reduction of backup size. If you are not sure about the compression ratio of a file type, try to back up a couple of files and compare the sizes of the original files and backup archive file. A couple of additional tips: generally, you can use the **Normal** compression level, because in most cases it provides an optimal balance between backup file size and backup duration. If you select **None**, the data will be copied without any compression, which may significantly increase the backup file size, while making the fastest backup.

7.2.1.2 Backup priority

The preset is **Low**.

The priority of any process running in a system determines the amount of CPU usage and system resources allocated to that process. Decreasing the backup priority will free more resources for other CPU tasks. Increasing the backup priority might speed up the backup process by taking resources from the other currently running processes. The effect will depend on total CPU usage and other factors.

7.2.1.3 File-level security settings for backup

You can specify security settings for backed up files (these settings relate only to file/folder backups):

- **Preserve file security settings in archives** - selecting this option will preserve all the security properties (permissions assigned to groups or users) of the backup files for further recovery.
By default, files and folders are saved in the archive with their original Windows security settings (i.e. permissions for read, write, execute and so on for each user or user group, set in file **Properties** → **Security**). If you recover a secured file/folder on a computer without the user specified in the permissions, you may not be able to read or modify this file.
To eliminate this kind of problem, you can disable preserving file security settings in archives. Then the recovered files/folders will always inherit the permissions from the folder to which they are recovered (parent folder or disk, if recovered to the root).
Or, you can disable file security settings during recovery, even if they are available in the archive. The result will be the same.
- **In archives, store encrypted files in a decrypted state** (the preset is **disabled**) - check the option if there are encrypted files in the backup and you want them to be accessed by any user after recovery. Otherwise, only the user who encrypted the files/folders will be able to read them. Decryption may also be useful if you are going to recover encrypted files on another computer. If you do not use the encryption feature available in Windows XP and Windows Vista operating systems, simply ignore this option. (Files/folders encryption is set in **Properties** → **General** → **Advanced Attributes** → **Encrypt contents to secure data**).

These options relate only to file/folder backups.

7.2.1.4 Error handling

Ignore bad sectors

The preset is **disabled**.

This option lets you run a backup even if there are bad sectors on the hard disk. Although most disks do not have bad sectors, the possibility that they might occur increases during the course of the hard disk's lifetime. If your hard drive has started making strange noises (for example, it starts making quite loud clicking or grinding noises during operation), such noises may mean that the hard drive is failing. When the hard drive completely fails, you can lose important data, so it is necessary to back up the drive as soon as possible. There may be a problem though – the failing hard drive might already have bad sectors. If the **Ignore bad sectors** box is left unselected, a backup task is aborted in case of read and/or write errors that could occur on the bad sectors. Selecting this box lets you run a

backup even if there are bad sectors on the hard disk ensuring that you save as much information from the hard drive as possible.

Do not show messages and dialogs while processing (silent mode)

The preset is **disabled**.

You can enable this setting to ignore errors during backup operations. This feature was mainly designed for unattended backups when you cannot control the backup process. In this mode no notifications will be displayed if errors occur during backup. Instead you can view the detailed log of all operations after the task finishes by selecting **Tasks and Log** on the sidebar and then clicking the **Log** tab. You may use this option when configuring a backup task to be run during the night.

7.2.1.5 Removable media settings

When backing up to removable media, you can make this media bootable by writing additional components to it. Thus, you will not need a separate bootable disk.

Here the following settings are available:

- **Acronis True Image WD Edition (Full version)** - includes support of USB, PC Card (formerly PCMCIA) and SCSI interfaces along with the storage devices connected via them, and therefore is strongly recommended.
- **Acronis System Report** - the component allows you to generate system report that is used for collecting information about your system in case of any program problem. Report generation will be available before you start Acronis True Image WD Edition from the bootable media. The generated system report can be saved to a USB flash drive.
- **Ask for first media while creating backup archives on removable media**
You can choose whether to display the Insert First Media prompt when backing up to removable media. With the default setting, backing up to removable media may not be possible if the user is away, because the program will wait for someone to press OK in the prompt box.

7.2.2 Local storage settings

These settings also affect the backup process, for example, they may have a more or less noticeable effect on the backup process speed. Their values also depend on the physical characteristics of the local storage devices.

7.2.2.1 Free space threshold

The preset is **disabled**.

You may want to be notified when the free space on the backup storage becomes less than the specified value. To enable such notification, select the **On insufficient free disk space** box, then specify the free space threshold value in the below fields.

When this option is enabled, Acronis True Image WD Edition will monitor free space on your backup storage. If after starting a backup task Acronis True Image WD Edition finds out that the free space on the selected backup archive location is already less than the specified value, the program will not begin the actual backup process but will immediately inform you by displaying an appropriate message. The message offers you three choices - to ignore it and proceed with the backup, to browse for another location or to cancel the task. In case of choosing to cancel the backup you can either free some space on the storage and restart the task or create a new task with another location for

the backup archive. If you choose **Browse**, select another storage, click **OK** and the backup file will be created on that storage.

If the free space becomes less than the specified value while the backup task is being run, the program will display the same message and you will have to make the same decisions. However, if you choose to browse for another location, you will need to assign a name for the file that will contain the remaining data being backed up (or you may accept the default name assigned by the program).

Acronis True Image WD Edition can monitor free space on the following storage devices:

- Local hard drives
- USB cards and drives
- Networks shares (SMB/NFS)

This option cannot be enabled for FTP servers and CD/DVD drives.

The message will not be displayed if the "Do not show messages and dialogs while processing (silent mode)" box is selected in the "Error handling" settings.

7.2.2.2 Archive splitting

Sizeable backups can be split into several files that together form the original backup. A backup file can be split for burning to removable media.

Suppose you have a full backup of your PC on an external hard disk, but want to make one more backup copy of the system to keep it in a different location from the first one for added security. However, you do not have one more external hard disk, and a USB stick would not accommodate such a large backup. Using Acronis True Image WD Edition you can make a reserve backup copy on blank DVD-R/DVD+R discs, which are very cheap nowadays. The program can split large backups into several files that together form the original backup. If you have enough space on your PC's hard disk, you can first create a backup archive consisting of multiple files with a specified size on the hard disk and burn the archive to DVD+R discs later on. To specify the split file size, select **Fixed size** mode for **Archive splitting** and enter the desired file size or select it from the drop-down list.

If you do not have enough space to store the backup on your hard disk, select **Automatic** and create the backup directly on DVD-R discs. Acronis True Image WD Edition will split the backup archive automatically and will ask you to insert a new disc when the previous one is full.

Creating backups directly on CD-R/RW or DVD+R/RW might take considerably more time than it would on a hard disk.

7.2.2.3 Archive validation

Validate backup archive when it is created

The preset is **disabled**.

When enabled, the program will check the integrity of the just created or supplemented archive immediately after backup. When setting up a backup of critical data or a disk/partition backup, we strongly recommend you to enable the option to ensure that the backup can be used to recover lost data.

8 Data recovery with Acronis True Image WD Edition

The ultimate purpose of data backup is recovery of the backed up data when the original is lost due to hardware failure, fire, theft or just erroneous deletion of some important files.

There may be various reasons for recovering your system - from unstable operation after installing a new application, driver or Windows update to complete failure of the system hard drive or replacement of the old hard drive by a new larger one. In addition, it may be necessary to recover either only the system partition or the entire system disk comprising several partitions including hidden ones. Acronis True Image WD Edition provides for all these cases, though details of recovery may differ. In any case, it is better to perform system recovery when booting from the rescue media.

On the other hand, recovery of a data disk/partition or files and folders is usually performed in Windows.

8.1 Recovering your system partition

Let's first consider the simplest case - recovery of the system partition to the original location on the original hard disk drive.

As recovery of the system partition is one of the most important operations, it requires careful preparation even when you just want to recover a previous "known good" Windows state. While preparing for recovery you need to:

- a) create and test Acronis bootable rescue media. For more information on testing media see Testing bootable rescue media;
- b) boot from the rescue media and validate the backup you want to use for recovery. Such validation is very important because Acronis True Image WD Edition deletes the target partition (the system partition in this case) when starting partition recovery, so you may find yourself without your system and applications if the backup file is corrupted. In addition, there were reports from users that a backup archive that has been successfully validated in Windows is declared corrupted when being validated in the recovery environment. This may be due to the fact that Acronis True Image WD Edition uses different device drivers in Windows and the recovery environment.
- c) assign unique names to the disks and partitions used on your computer. This is strongly recommended because the drive lettering in Windows and in the recovery environment may differ. If you have not done this before making the backup, you can assign names now. The names will help you in finding the drive containing your backups as well as the target system partition.
- d) optionally check the system hard drive for errors using Microsoft's Chkdsk utility, which is part of Windows.

Assuming that you have carried out the above, let's proceed with recovery.

Attach the external drive if it contains the backup archive to be used for recovery and make sure that the drive is powered on. This must be done before booting from Acronis rescue media.

1. Arrange the boot sequence in BIOS so as to make your rescue media device (CD, DVD or USB stick) the first boot device. See Arranging boot sequence in BIOS (p. 93).
2. Boot from the rescue media and select Acronis True Image WD Edition (Full version).

3. Select **Recovery** → **Disk and Partition Recovery** in the main menu and then choose the image backup of your system partition (or entire system disk) that you want to use for recovery. Right-click on the backup and choose **Recover** in the shortcut menu.

If the disks have different disk letters in Windows and the recovery environment, the program will display the following error message: "Acronis True Image WD Edition cannot detect volume N of "Name" archive", where Name is the name of the required image backup archive and volume number (N) may be different depending on the number of backups in the archive. Click **Browse** and show the path to the archive.

4. Select **Recover whole disks and partitions** at the Recovery method step.
5. Select the system partition (usually C) on the **What to recover** screen. If the system partition has a different letter, select the partition using the **Flags** column. It must have the **Pri**, **Act** flags. As you are recovering the system partition to the original hard drive, there is no need to select the "MBR and track 0" box.
6. At the "Settings of partition C" (or the letter of the system partition, if it is different) step check the default settings and click **Next** if they are correct. Otherwise change the settings so as to suit you before clicking **Next**.
7. Carefully read the summary of operations at the **Finish** step. If you have not resized the partition, the sizes in the **Deleting partition** and **Recovering partition** items must match. If you do not want to validate the backup, click **Proceed**, otherwise click **Options** and select the "Validate backup archive before recovery" box before clicking **Proceed**.
8. When the operation finishes, exit the standalone version of Acronis True Image WD Edition, remove the rescue media and boot from the recovered system partition. After making sure that you recovered Windows to the state you need, restore the original boot sequence.

8.2 Recovering a disk backup to a different capacity hard disk

Recovery of a disk backup containing several partitions to a hard disk that has a different capacity using manual resizing of the partitions can be considered as one of the most complicated operations in Acronis True Image WD Edition. This is especially true when you have backed up the original hard disk containing a hidden diagnostic or recovery partition.

Recovering a dual/multiboot system disk e.g. with Windows and some flavor of LINUX may be even more fraught with difficulties. Quite often it requires some research on the appropriate forums before attempting to perform a recovery so this section does not cover such case.

Make the preparations described at the beginning of the previous section Recovering your system partition (p. 38). In case of upgrading the healthy system disk to a larger capacity new one, if you have not assigned unique names to the partitions on the system disk before making a system disk backup, it might make sense to assign such names and create a new backup of the entire disk. This will allow identifying the partitions by their names and not by the letters which may differ when booting from the rescue media. If you are recovering from a system disk drive failure, assign names now anyway. The names will help you find the drive containing your backups, as well as the target (new) drive.

The information on partition sizes, drive capacities, their manufacturers, and model numbers can also help in correctly identifying the drives.

One more recommendation - it is highly recommended to install the new hard drive to the same position in the computer and use the same cable and the same connector as for the original drive

(though this is not always possible, e.g. the old drive may be an IDE and the new drive may be a SATA). In any case, install the new drive to where it will be used.

8.2.1 Recovering a disk without a hidden partition

At first let's consider recovery of a system disk containing two partitions (none of them hidden) using a disk backup. In addition, we assume that the system disk does not contain a recovery partition which may not be hidden. If the disk contains, for example, three partitions, the procedure will be similar. We will describe recovery using the rescue media (as this approach usually gives the best recovery results).

Attach the external drive if it contains the backup archive to be used for recovery and make sure that the drive is powered on. This must be done before booting from Acronis rescue media.

1. Arrange the boot sequence in BIOS so as to make your rescue media device (CD, DVD or USB stick) the first boot device. See Arranging boot sequence in BIOS (p. 93).
2. Boot from the rescue media and select Acronis True Image WD Edition (Full version).
3. Select **Recovery** → **Disk and Partition Recovery** in the main menu, then choose the image backup of your system disk that you want to use for recovery.

If the disks have different disk letters in Windows and the recovery environment, the program will display the following error message: "Acronis True Image WD Edition cannot detect volume N of "Name" archive", where Name is the name of the required image backup archive and volume number (N) may be different depending on the number of backups in the archive. Click **Browse** and show the path to the archive.

4. Select **Recover whole disks and partitions** at the Recovery method step.
5. At the **What to recover** step select the boxes of the partitions to be recovered. Do not select the **MBR and Track 0** box, as this will result in selecting the entire disk for recovery. Recovering the entire disk does not allow you to resize partitions manually. If necessary, you can recover the MBR later. Select the partitions and click **Next**.

Selecting partitions leads to appearance of the relevant steps "Settings of partition ...". Take note that these steps are in ascending partition drive letter order and that this order cannot be changed. The order may differ from the physical order of the partitions on the hard disk. In the case being considered (no hidden or recovery partitions), the physical order of the partitions on the new disk does not have special importance as Acronis True Image WD Edition automatically fixes the appropriate Windows loader files.

Incidentally, this step allows you to find out whether the disk you are going to recover contains a hidden partition. Hidden partitions do not have disk letters and they go first in the "Settings of partition ..." steps. If you find a hidden partition, see Recovering a disk with a hidden partition (p. 41).

6. You can specify the following partition settings: location, type, and size. Most likely you will first specify the settings of the system partition as it usually has the letter C. Because you are recovering to the new disk, click **New location**. Select the destination disk by either its assigned name or capacity.

If you have not assigned names to the disks and have any doubts when selecting the destination disk, you may abort the recovery by clicking **Cancel** and try to identify the target disk by its model number, interface, etc. To see this information, select **Tools & Utilities** → **Add New Disk** in the main menu and the **Disk selection** screen will show the information. Use it for identifying the destination disk number, then click **Cancel**, start the Recovery Wizard again, repeat the above steps, and select the destination disk.

7. Clicking **Accept** will return you to the "Settings of partition ..." screen. Check the partition type and change it, if necessary. You should remember that the system partition must be primary and marked as active.
8. Proceed to specifying the partition size by clicking **Change default** in the Partition size area. By default the partition will occupy the entire new disk. You can resize and relocate the partition by dragging it or its borders with a mouse on the horizontal bar on the screen or by entering corresponding values into the appropriate fields (Partition size, Free space before, Free space after). While specifying the partition size remember that you need to leave as much unallocated (free) space *after* the newly resized partition as will be needed for the second partition. Usually the free space *before* partitions is equal to zero. Click **Accept** when the partition has the size you have planned for it, then click **Next**.
9. Begin specifying the settings for the second partition. Click **New location**, then select unallocated space on the destination disk that will receive the second partition. Click **Accept**, check the partition type (change, if necessary) and then proceed to specifying the partition size which by default is equal to the original size. Usually there is no free space after the last partition, so allocate all the unallocated space to the second partition, click **Accept** and then click **Next**.
10. Carefully read the summary of operations to be performed. If you do not want to validate the backup, click **Proceed**, otherwise click **Options** and select the "Validate backup archive before recovery" box before clicking **Proceed**.
11. When the operation finishes, exit the standalone version of Acronis True Image WD Edition.

Windows should not "see" both the new and old drive during the first boot after recovery. If you upgrade the old drive to a larger capacity new one, disconnect the old drive before the first boot otherwise there may be problems booting Windows.

Switch off the computer, if you need to disconnect the old drive, otherwise just reboot the computer after removing the rescue media.

Boot the computer to Windows. It may report that new hardware (hard drive) is found and Windows needs to reboot. After making sure that the system operates normally, restore the original boot sequence.

8.2.2 Recovering a disk with a hidden partition

Recovering a backup of the system disk with a hidden partition (e.g. created by the PC manufacturer for diagnostics or system recovery) to a different capacity hard drive, requires to take into account some additional factors. First of all, for the best chance of success, it is necessary to keep on the new drive the physical order of the partitions that exist on the old drive and place the hidden partition to the same location - usually at the start or the end of the disk space. In addition, it is better to recover the hidden partition without resizing to minimize the risk of possible problems.

So before proceeding with recovery, you need to know about all partitions existing on the system disk, their sizes, and physical order. To see this information, start Acronis True Image WD Edition and choose **Recovery** → **Disk and Partition Recovery** in the main menu. Select a backup of your system disk and click **Details** on the toolbar. Acronis True Image WD Edition will display information about the backed up disk, including a graphical view of all partitions the disk contains and their physical order on the disk. If any partition display is too small for accommodating the relevant information, hover the mouse pointer over the partition to see the information.

Assuming that you have got the information, let's proceed with recovery of a system disk using the rescue media.

Attach the external drive if it contains the backup archive to be used for recovery and make sure that the drive is powered on. This must be done before booting from Acronis rescue media.

1. Arrange the boot sequence in BIOS so as to make your rescue media device (CD, DVD or USB stick) the first boot device. See Arranging boot sequence in BIOS (p. 93).
2. Boot from the rescue media and select Acronis True Image WD Edition (Full version).
3. Select **Recovery** → **Disk and Partition Recovery** in the main menu and then choose the image backup of your system disk that you want to use for recovery.

If the disks have different disk letters in Windows and the recovery environment, the program will display the following error message: "Acronis True Image WD Edition cannot detect volume N of "Name" archive", where Name is the name of the required image backup archive and volume number (N) may be different depending on the number of backups in the archive.

4. Select **Recover whole disks and partitions** at the Recovery method step.
5. At the **What to recover** step select the boxes of the partitions to be recovered. Do not select the **MBR and Track 0** box, as this will result in selecting the entire disk for recovery. Recovering the entire disk does not allow you to resize partitions manually. You will recover the MBR later. Select the partitions and click **Next**.

Selecting partitions leads to appearance of the relevant steps "Settings of partition ...". Take note that these steps start with partitions without an assigned disk letter (as usually is the case with hidden partitions), then go in ascending order of partition disk letters and this order cannot be changed. The order may differ from the physical order of the partitions on the hard disk.

6. You can specify the following partition settings: location, type, and size. You will first specify the settings of the hidden partition as it usually does not have a disk letter. Because you are recovering to the new disk, click **New location**. Select the destination disk by either its assigned name or capacity.

If you have not assigned names to the disks and have any doubts when selecting the destination disk, you may abort the recovery by clicking **Cancel** and try to identify the target disk by its model number, interface, etc. To see this information, select **Tools & Utilities** → **Add New Disk** in the main menu and the **Disk selection** screen will show the information. Use it for identifying the destination disk number, then click **Cancel**, start the Recovery Wizard again, repeat the above actions, and select the destination disk.

7. Clicking **Accept** will return you to the "Settings of partition ..." screen. Check the partition type and change it, if necessary.
8. Proceed to specifying the partition size by clicking **Change default** in the Partition size area. By default the partition will occupy the entire new disk. You need to keep the hidden partition size unchanged, as well as place it to the same location on the disk (at the start or the end of disk space). To do this, resize and relocate the partition by dragging it or its borders with a mouse on the horizontal bar on the screen or by entering corresponding values into the appropriate fields (Partition size, Free space before, Free space after). Click **Accept** when the partition has the required size and location and then click **Next**.

Specify the settings for the second partition which in this case is your system partition. Click **New location**, then select unallocated space on the destination disk that will receive the partition. Click **Accept**, check the partition type (change, if necessary). You should remember that the system partition must be primary and marked as active. Specify the partition size which by default equals the original size. Usually there is no free space after the partition, so allocate all the unallocated space on the new disk to the second partition, click **Accept** and then click **Next**.

9. Carefully read the summary of operations to be performed. If you do not want to validate the backup, click **Proceed**, otherwise click **Options** and select the "Validate backup archive before recovery" box before clicking **Proceed**.

10. When the operation finishes, proceed to MBR recovery. In this case you need to recover the MBR as the PC manufacturer could change the generic Windows MBR or a sector on the track 0 to provide access to the hidden partition.
11. Select the same backup once more, right-click and select **Recover** in the shortcut menu, choose **Recover whole disks and partitions** at the Recovery method step and then select the **MBR and Track 0** box.
12. At the next step select the destination disk as the target for MBR recovery, click **Next** and then **Proceed**. After MBR recovery is complete, exit the standalone version of Acronis True Image WD Edition.

Windows should not "see" both the new and old drive during the first boot after recovery. If you upgrade the old drive to a larger capacity new one, disconnect the old drive before the first boot otherwise there may be problems booting Windows.

Switch off the computer, if you need to disconnect the old drive, otherwise just reboot the computer after removing the rescue media.

Boot the computer to Windows. It may report that new hardware (hard drive) is found and Windows needs to reboot. After making sure that the system operates normally, restore the original boot sequence.

8.3 Recovering a data partition or disk

As we already said, data partitions and disks are usually recovered in Windows because this allows you to avoid such issues as the program not detecting your hard drives, changing disk letters, etc. To reduce the risk of problems during recovery even more, validate the backup archive to be recovered and check the destination disk for errors using `chkdsk`.

Attach the external drive if it contains the backup archive to be used for recovery and make sure that the drive is powered on. This must be done before starting Acronis True Image WD Edition.

1. Start Acronis True Image WD Edition.
2. Select **Recovery** → **Disk and Partition Recovery** in the main menu, then choose the image backup containing the data partition you want to recover.
3. Select **Recover whole disks and partitions** at the Recovery method step.
4. As you are going to recover a data partition, there is no need to select the "Recover MBR and track 0" box at the **What to recover** step. Select just the data partition you want to recover.
5. The next step allows you to select settings for the partition to be recovered. When recovering the partition to the original location, you only need to check the settings. If you want to recover the partition to another location, select the new location and set the partition type you need (or leave the default setting). When the new location is an existing partition, usually you may leave its disk letter and size unchanged. When the new location is unallocated space e.g. after installing a new hard drive you intend to use for your data, specify the size of the new partition and assign a logical disk letter.
6. Carefully read the Summary. After making sure that you have made the correct settings, click **Proceed**, if you do not need to change the default recovery options, otherwise click **Options**.
7. The Options step allows setting the recovery options, for example, to check the file system after recovery. For more information about the recovery options see Setting default recovery options. After setting the recovery options click **Proceed**.

Recovering the entire data disk backup requires similar steps with few minor differences, for example, there is no "Check file system after recovery" option. When recovering to the original hard

drive the steps of the Recovery Wizard are straightforward - just make sure that you select the disk with the same number as the backed up disk, as the destination.

Recovering your data disk backup to a hard drive with a different capacity has some nuances depending on its capacity and geometry (the number of heads and sectors per track). When recovering to a smaller capacity hard drive, the partition(s) size will be proportionally reduced. When recovering to a larger capacity hard drive, there are two cases: 1) if the hard drive has the same geometry, the backed up disk will be recovered "as is" thus leaving unallocated space; and 2) if the hard drive has different geometry, the partition(s) size will be proportionally enlarged.

8.4 Recovering files and folders

Depending on the backup types you have used, there may be several methods of recovering files and folders. In most cases you recover files and folders in Windows. You can recover files and folders from a disk/partition image. To recover files/folders from an image, you can mount the image (see Mounting an image) and copy files/folders to a desired location using Windows Explorer.

If you need to recover just a single file/folder or a few files, double-click on the required image backup archive. Then drill-down to the folder containing the file(s) you need to recover, select the file(s), right-click and choose **Copy** in the shortcut menu, open a folder for saving the files to be recovered, right-click in the folder and choose **Paste** in the shortcut menu. You can also drag the files from the backup archive into the destination folder.

One more method of recovering files/folders from an image is described below. See Recovering files and folders from image archives.

8.4.1 Recovering files and folders from image archives

Image archives provide recovery of not only entire disks/partitions, but files/folders too.

1. Start the **Recovery Wizard** by selecting **Recovery** → **Disk and Partition Recovery** in the main program menu.
2. Select the archive.

Data recovery directly from an FTP server requires the archive to consist of files of no more than 2GB. If you suspect that some of the files are larger, first copy the entire archive (along with the initial full backup) to a local hard disk or a network share disk.

3. At the **Recovery method** step select **Recover chosen files and folders**.
4. Select where you want to recover the chosen files/folders. You can recover data to its original location or choose a new one, if necessary.

*When recovering files/folders under bootable rescue media, the **Original location** option is disabled, because drive letters in standalone Acronis True Image WD Edition might differ from the way Windows identifies drives.*

Choosing a new location results in appearance of one more required step, namely, **Destination**. When you choose a new location, by default the selected items will be recovered without recovering the original, absolute path. You may also wish to recover the items with their entire folder hierarchy. If this is the case, select **Recover absolute path**.

At the **Destination** step select a new location on the directory tree. You can create a new folder for the files to be recovered by clicking **Create new folder**.

5. Select the files and folders to recover. Make sure that you unselect all unnecessary folders. Otherwise you will recover a lot of excess files.

6. The first optional step allows you to keep useful data changes made since the selected backup was created. Choose what to do if the program finds a file in the destination folder with the same name as in the archive. By default, the program will overwrite existing files and folders, though more recent files and folders are protected from being overwritten. If necessary, you can protect the system, hidden files and folders from being overwritten by selecting the appropriate check boxes.

In addition, you can protect the files that meet the criteria you specify in this window from being overwritten.

Unselecting the **Overwrite existing files** checkbox will give the files on the hard disk unconditional priority over the archived files.

7. Select the options for the recovery process (that is, recovery process priority, file-level security settings, etc.). The options you set on this page will be applied only to the current recovery task.
8. Up to this point, you can make changes in the created task by choosing the step you want to change and editing its settings. Clicking **Proceed** will launch the task execution.
9. The task progress will be shown in a special window. You can stop the procedure by clicking **Cancel**. Please keep in mind that the aborted procedure may still cause changes in the destination folder(s).

9 Additional recovery information

9.1 Recovery Wizard - detailed information

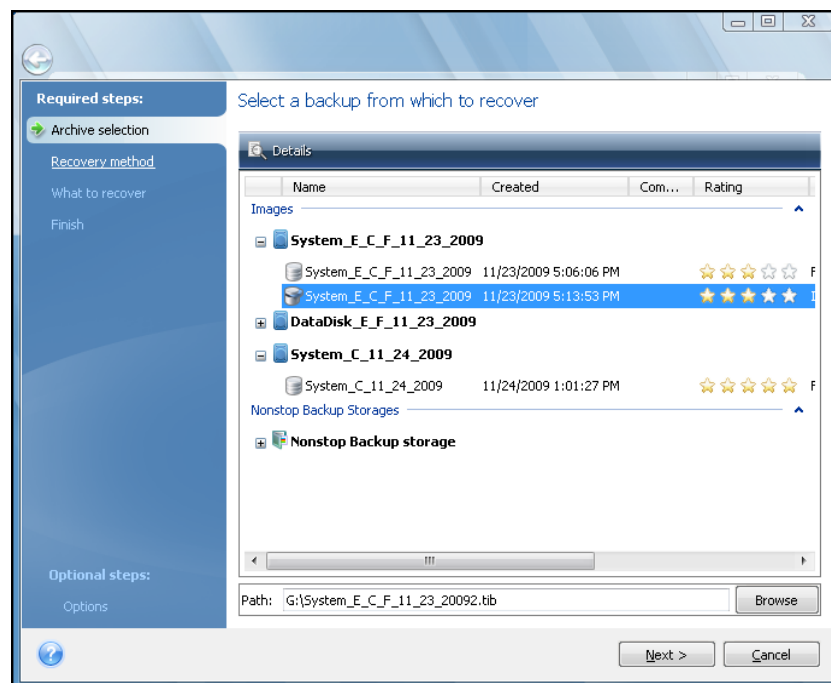
The below description of the Recovery Wizard refers to recovering partitions/disks from image backups. If you need to recover files and folders, see Recovering files and folders.

9.1.1 Starting the Recovery Wizard

Start the **Recovery Wizard** by selecting **Recovery** → **Disk and Partition Recovery** in the main program menu.

9.1.2 Archive selection

1. Select the archive. Acronis True Image WD Edition will show the list of backup archives whose locations it knows from the information stored in its database. If the program has not found the backup you need (for example, when the backup was made in the recovery environment or by a previous Acronis True Image WD Edition version), you can find it manually by clicking **Browse** and then selecting the backup location on the directory tree and choosing the backup in the right pane.



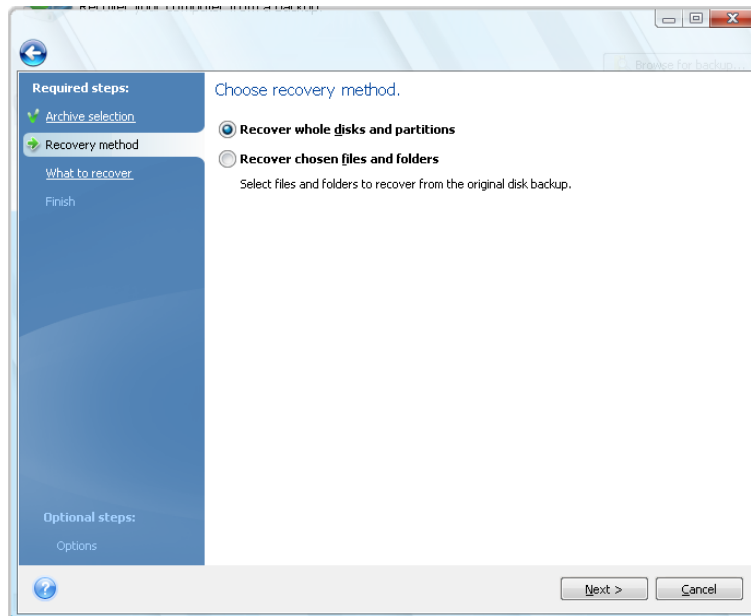
If the archive is located on removable media, e.g. CD, first insert the last CD and then insert disks in reverse order when the Recovery Wizard prompts you.

Data recovery directly from an FTP server requires the archive to consist of files of no more than 2GB each. If you suspect that some of the files are larger, first copy the entire archive (along with the initial full backup) to a local hard disk or network share disk.

When recovering a backup of Windows Vista or Windows 7 system disk containing restore points, some of your restore points (or all of them) may be missing if you boot from the recovered system disk and open the System Restore tool.

9.1.3 Recovery method selection

Select what you want to recover:



Recover whole disks and partitions

Having chosen a disk and partition recovery type, you may need to select the following option.

Recover chosen files and folders

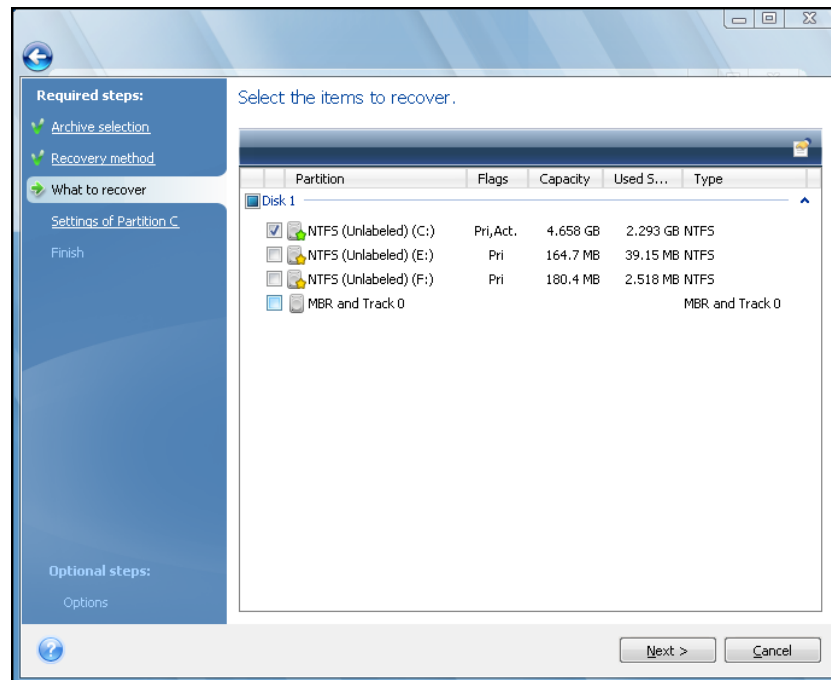
If you are not going to recover the system, but only want to repair damaged files, select **Recover chosen files and folders**.

You can recover files from disk/partition images only if they have the FAT or NTFS file systems.

9.1.4 Selecting a disk/partition to recover

The selected archive file can contain images of several partitions or even disks. Select which disk/partition to recover.

During a single session, you can recover several partitions or disks, one by one, by selecting one disk and setting its parameters first and then repeating these actions for every partition or disk to be recovered.



Disk and partition images contain a copy of track 0 along with the MBR (master boot record). It appears in this window in a separate line. You can choose whether to recover the MBR and track 0 by selecting the corresponding box. Recover the MBR if it is critical to your system booting.

When MBR recovery is chosen, the "Recover disk signature" box will appear in the bottom left corner at the next step. Recovering disk signature may be desirable due to the following reasons:

1. Acronis True Image WD Edition creates scheduled tasks using the signature of the source hard disk. If you recover the same disk signature, you don't need to re-create or edit the tasks created previously.
2. Some installed applications use disk signature for licensing and other purposes.
3. If you use Windows Restore Points, they will be lost when the disk signature is not recovered.
4. In addition, recovering disk signature allows to recover VSS snapshots used by Windows Vista and Windows 7's "Previous Versions" feature.

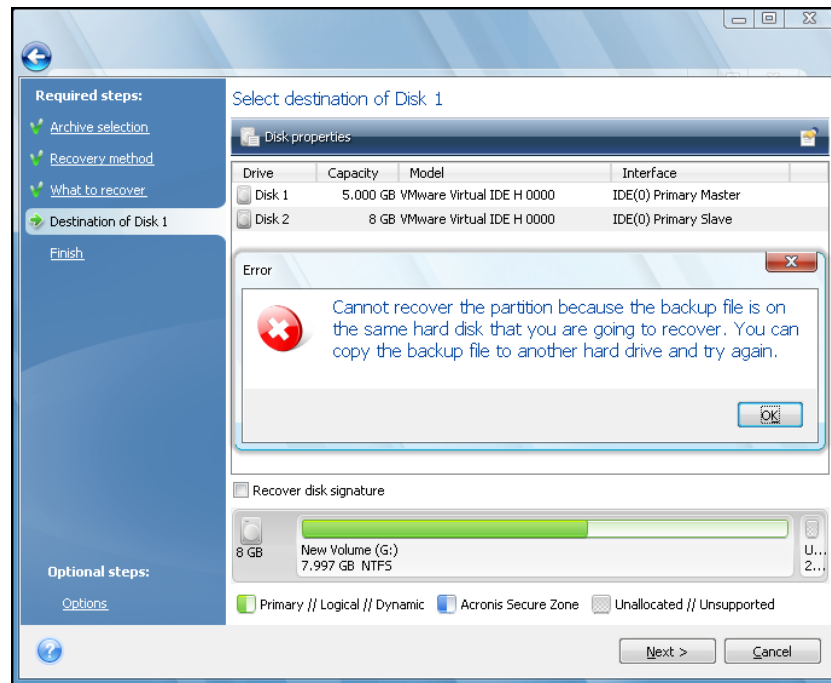
If the box is unselected, Acronis True Image WD Edition generates a new disk signature for the recovered drive. This may be needed when you use an image backup not for disaster recovery but for cloning your Windows Vista hard drive to another one. Trying to boot Windows after cloning with both drives connected will result in a problem. During Windows booting, its loader checks the disk signatures of all the connected drives, and if it finds two identical disk signatures, the loader changes the signature of the second disk, which would be the clone disk. Once this happens, the clone disk would not be able to boot up independently of the original disk, because the MountedDevices fields in the clone's registry reference the disk signature of the original disk, which will not be available if the original disk is disconnected.

9.1.5 Selecting a target disk/partition

1. Select a target disk or partition where you want to recover the selected image. You can recover data to its initial location, to another disk/partition or to an unallocated space. The target partition should be at least the same size as the uncompressed image data.

All the data stored on the target partition will be replaced by the image data, so be careful and watch for non-backed-up data that you might need.

2. When recovering an entire disk, the program will analyze the target disk structure to see whether the disk is free.



If there are partitions on the target disk, you will be prompted by the confirmation window stating that the destination disk contains partitions, perhaps with useful data.

You will have to select between:

- **OK** – all existing partitions will be deleted and all their data will be lost.
- **Cancel** – no existing partition will be deleted, discontinuing the recovery operation. You will then have to cancel the operation or select another disk.

*Note that no real changes or data destruction will be performed at this time! For now, the program will just map out the procedure. All changes will be implemented only when you click **Proceed** in the wizard's **Summary** window.*

9.1.6 Changing the recovered partition type

When recovering a partition, you can change its type, though it is not required in most cases.

To illustrate why you might need to do this, let's imagine that both the operating system and data were stored on the same primary partition on a damaged disk.

If you are recovering a system partition to the new (or the same) disk and want to load the operating system from it, you will select **Active**.

Acronis True Image WD Edition automatically corrects boot information during recovery of the system partition to make it bootable, even if it was not recovered to the original partition (or disk).

If you recover a system partition to another hard disk with its own partitions and OS, most likely you will need only the data. In this case, you can recover the partition as **Logical** to access the data only.

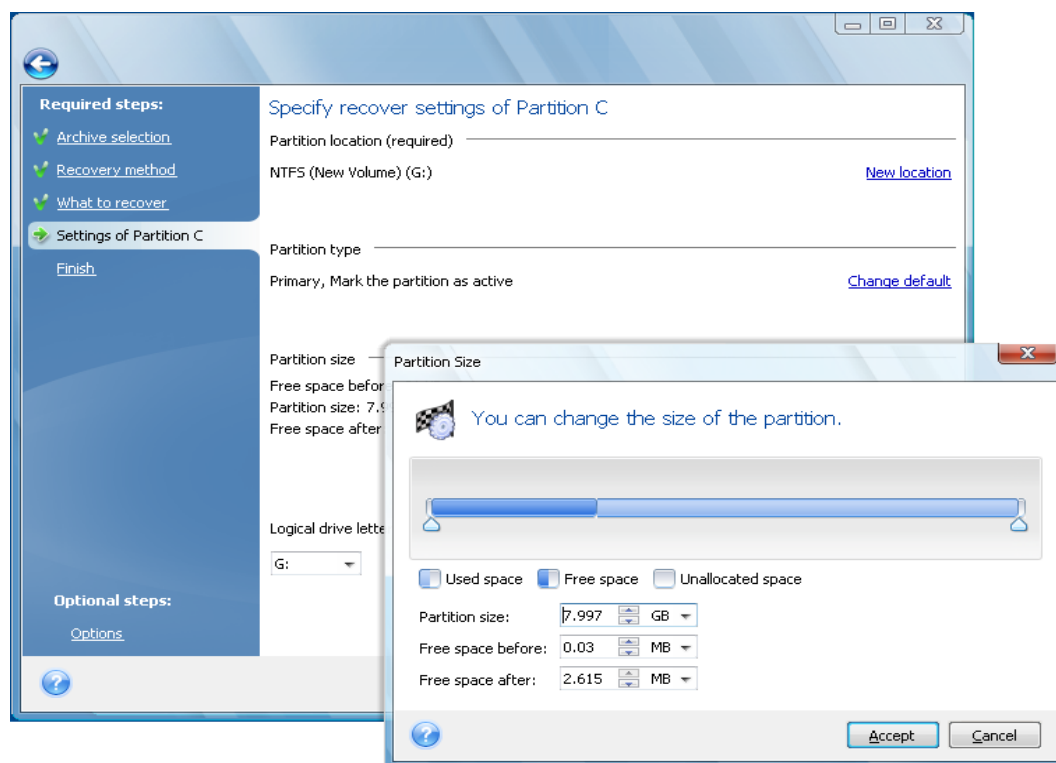
By default, the original partition type is selected.

*Selecting **Active** for a partition without an installed operating system could prevent your computer from booting.*

9.1.7 Changing the recovered partition size and location

You can resize and relocate a partition by dragging it or its borders with a mouse on the horizontal bar on the screen or by entering corresponding values into the appropriate fields.

Using this feature, you can redistribute the disk space among partitions being recovered. In this case, you will have to recover the partition to be reduced first.



These changes might be useful if you are going to copy your hard disk to a new high-capacity one by creating its image and recovering it to a new disk with larger partitions.

9.1.8 Assigning a letter to the recovered partition

Acronis True Image WD Edition will assign an unused letter to a recovered partition. You can select the desired letter from a drop-down list or let the program assign a letter automatically by selecting the **Auto** setting.

You should not assign letters to partitions inaccessible to Windows, such as to those other than FAT and NTFS.

9.1.9 Setting recovery options

Clicking **Options** at the **Finish** step allows selecting the options for the recovery process (that is, recovery process priority, etc.). The settings will be applied only to the current recovery task. Or, you can edit the default options. See Setting default recovery options for more information.

9.1.10 Executing recovery

Up to this point, you can make changes in the created task by choosing the step you want to change and editing its settings. If you click **Cancel**, no changes will be made to the disk(s). Clicking **Proceed** will launch the task execution.

The task progress will be shown in a special window. You can stop the procedure by clicking **Cancel**. However, it is critical to note that the target partition will be deleted and its space unallocated – the same result you will get if the recovery is unsuccessful. To recover the "lost" partition, you will have to recover it from the image again.

9.2 Setting default recovery options

To set the recovery options to be used by default during any data recovery, select **Tools & Utilities** → **Options** → **Recovery options**. You can always restore the default recovery options to the values preset during installation of Acronis True Image WD Edition. To do this, click **Reset the current to default** on the toolbar of the **Options** window. To reset just a single recovery option, select it on the left pane and click **Reset the current to default**.

*Clicking **Reset all to default** will reset all the default options (for backup, recovery, etc.) to their preset values, so this button should be used with caution.*

9.2.1 File recovery options

You can select the following file recovery options:

- **Recover files with their security settings** - if the file security settings were preserved during backup (see Backup security settings), you can choose whether to recover them or let the files inherit the security settings of the folder where they will be recovered to. This option is effective only when recovering files from file/folder archives.
- **Validate backup archive before recovery** - if you suspect that the archive might have been corrupted, check this option to verify the backup before recovery.
- **Check the file system after recovery** - check this parameter to verify the integrity of the file system after recovery. Verification of the file system is available only when recovering disks/partitions under Windows and for FAT16/32 and NTFS file systems. Note, that the file system will not be checked if a reboot is required during recovery, for example, when recovering the system partition to its original place.

9.2.2 Overwrite file options

This option is not applicable to recovery of disks and partitions from images.

By default, the program will overwrite existing files and folders, though more recent files and folders are protected from overwriting.

You can set default filters for the specific types of files you wish to preserve during archive recovery. For example, you may want hidden and system files and folders, newer files and folders, as well as files matching selected criteria not to be overwritten by the archive files.

While specifying the criteria, you can use the common Windows wildcard characters. For example, to preserve all files with extension .exe, add ***.exe**. **My???.exe** will preserve all .exe files with names consisting of five symbols and starting with "my".

Unselecting the **Overwrite existing files** check box will give the files on the hard disk unconditional priority over the archived files.

9.2.3 Recovery priority

The preset is **Low**.

The priority of any process running in a system determines the amount of CPU usage and system resources allocated to that process. Decreasing the recovery priority will free more resources for other CPU tasks. Raising recovery priority may speed up the recovery process as it takes resources from other currently running processes. The effect will depend on total CPU usage and other factors.

10 Creating bootable media

10.1 Creating Linux-based rescue media

You can run Acronis True Image WD Edition from an emergency boot disk on a bare-metal system or a crashed computer that cannot boot. You can even back up disks on a non-Windows computer, copying all its data into the backup archive by imaging the disk one sector at a time. To do so, you will need bootable media that has a copy of the standalone Acronis True Image WD Edition version installed on it.

You can create bootable media using the Bootable Media Builder. For this, you will need a blank CD-R/RW, a blank DVD+R/RW or any other media from which your computer can boot, such as a Zip drive.

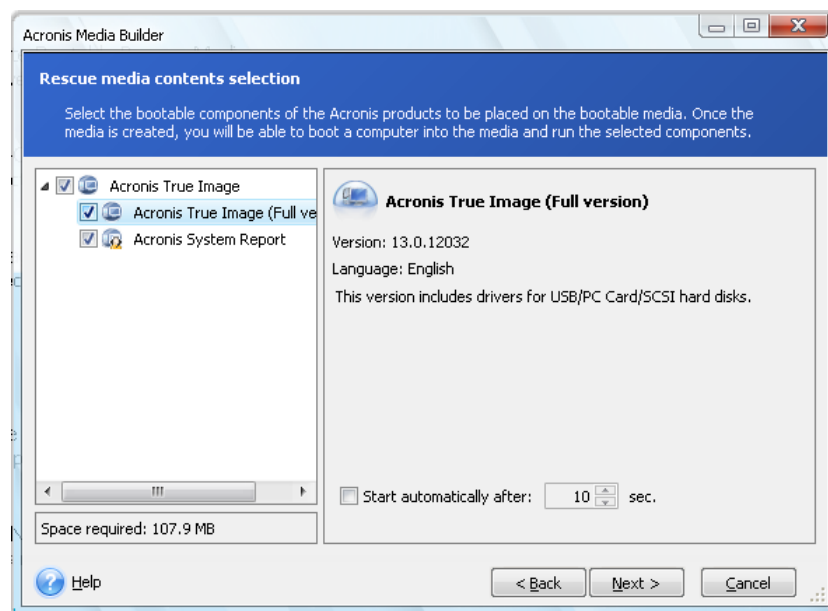
Acronis True Image WD Edition also provides the ability to create an ISO image of a bootable disc on the hard disk.

If you have other Acronis products, such as Acronis Disk Director Suite installed on your computer, you can include standalone versions of these programs on the same bootable disk as well.

If you have chosen not to install the Bootable Media Builder during Acronis True Image WD Edition installation, you will not be able to use this feature.

When booting from the Rescue Media, you cannot perform backups to disks or partitions with Ext2/Ext3, ReiserFS, and Linux SWAP file systems.

1. Choose **Create Bootable Rescue Media** in the **Tools & Utilities** menu. You can also run the Bootable Rescue Media Builder without loading Acronis True Image WD Edition by choosing **Programs → Acronis → Acronis True Image WD Edition → Bootable Rescue Media Builder** from the **Start** menu.
2. Select which components of the Acronis programs you want to place on the bootable media.



Acronis True Image WD Edition offers the following components:

Acronis True Image WD Edition full version

Includes support of USB, PC Card (formerly PCMCIA) and SCSI interfaces along with the storage devices connected via them, and therefore is strongly recommended.

Acronis System Report

This component allows you to generate a system report after booting from the rescue media when both Windows and Acronis True Image WD Edition full version cannot start.

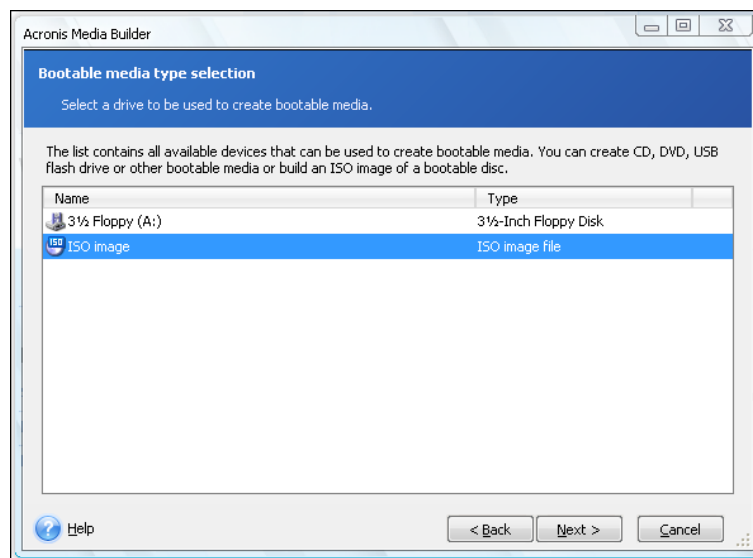
In the next window you can set Bootable media startup parameters in order to configure rescue media boot options for better compatibility with different hardware. Several options are available (nouseb, nomouse, noapic, etc.). For all the available startup parameters see Startup Parameters (p. 99). These parameters are provided for advanced users. If you encounter any hardware compatibility problems while testing boot from the rescue media, it may be best to contact Acronis Technical Support.

The **Start automatically after** parameter specifies the timeout interval for the boot menu. If this parameter is not specified, the program will display the boot menu and wait for you to select whether to boot the OS or the Acronis component. If you set, for example, **10 sec** for Acronis rescue media, the standalone Acronis True Image WD Edition will launch 10 seconds after the menu is displayed.

To find out more about components of other Acronis products, see their respective user guides.

3. Select the type of bootable media (CD-R/RW, DVD+R/RW or 3.5" diskettes) to create. If your BIOS has this feature, you can create other bootable media such as removable USB flash drives. You can also choose to create a bootable disk ISO image.

When using 3.5" diskettes, you will only be able to write one component at a time (for example, the full version of Acronis True Image WD Edition) on a set of diskettes. To write another component, start Bootable Media Builder again.



1. If you are creating a CD, DVD or any removable media, insert a blank disc so the program can determine its capacity. If you choose to create a bootable disc ISO image, specify the ISO file name and the folder in which to place it.
2. Next, the program will estimate how many blank diskettes are required (in case you have not chosen ISO or CD/DVD) and give you time to prepare them. When you are finished, click **Proceed**.

After you create a bootable media, mark it and keep it in a safe place.

Please keep in mind that the backups created by the later program version may be incompatible with the previous program versions. Due to this reason, we strongly recommend that you create a new

bootable media after each Acronis True Image WD Edition upgrade. One more thing you should remember – when booting from the rescue media and using a standalone version of Acronis True Image WD Edition, you cannot recover files and folders encrypted with use of the encryption feature available in Windows XP and later operating systems. For more information see File-level security settings. On the other hand, backup archives encrypted using the Acronis True Image WD Edition encryption feature can be recovered.

11 Exploring archives and mounting images

Acronis True Image WD Edition offers two kinds of archive contents management: mounting and exploring for images.

Mounting images as virtual drives lets you access them as though they were physical drives. Such ability means that:

- a new disk with its own letter will appear in the drives list
- using Windows Explorer and other file managers, you can view the image contents as if they were located on a physical disk or partition
- you will be able to use the virtual disk in the same way as the real one: open, save, copy, move, create, delete files or folders. If necessary, the image can be mounted in read-only mode.

The operations described in this chapter are supported only for the FAT and NTFS file systems.

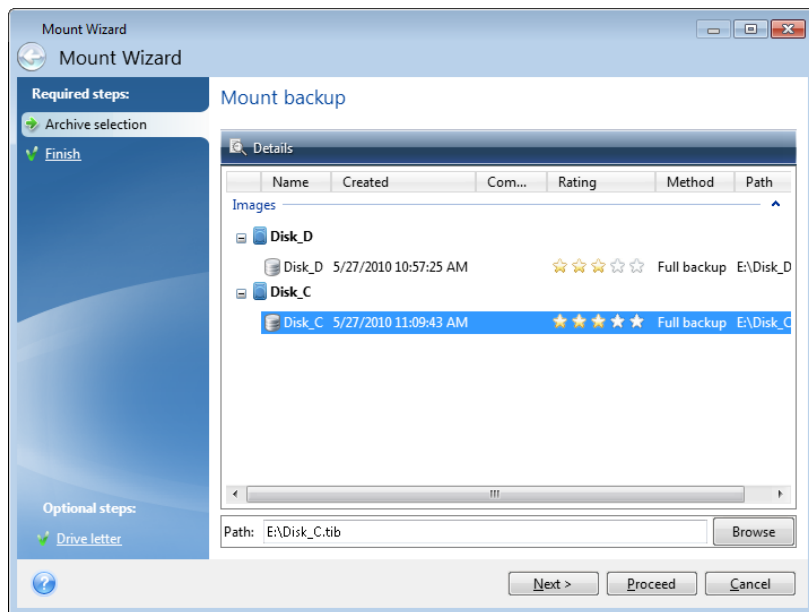
Please keep in mind that, though both file archives and disk/partition images have a default ".tib" extension, only **images** can be mounted. If you want to view file archive contents, use the Explore operation. The following is a brief summary of the Explore vs Mount operation:

	Explore	Mount
Archive type	Disk or partition image	Partition image
Assigning a letter	No	Yes
Archive modification	No	No
File extraction	Yes	Yes

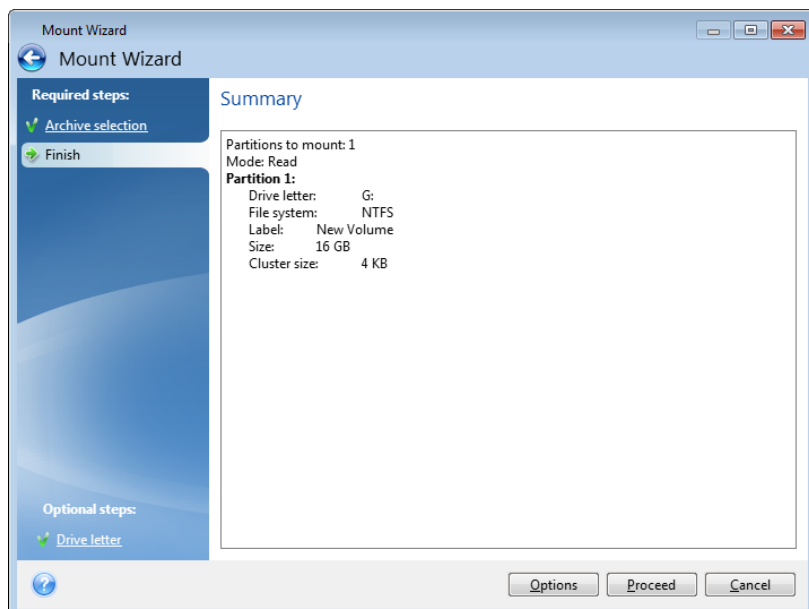
11.1 Mounting an image

1. Start the **Mount Wizard** by selecting **Tools & Utilities** → **Mount Image** in the main program menu or by right-clicking on an image archive on the **Data recovery and backup management** screen and selecting **Mount Image** in the shortcut menu.

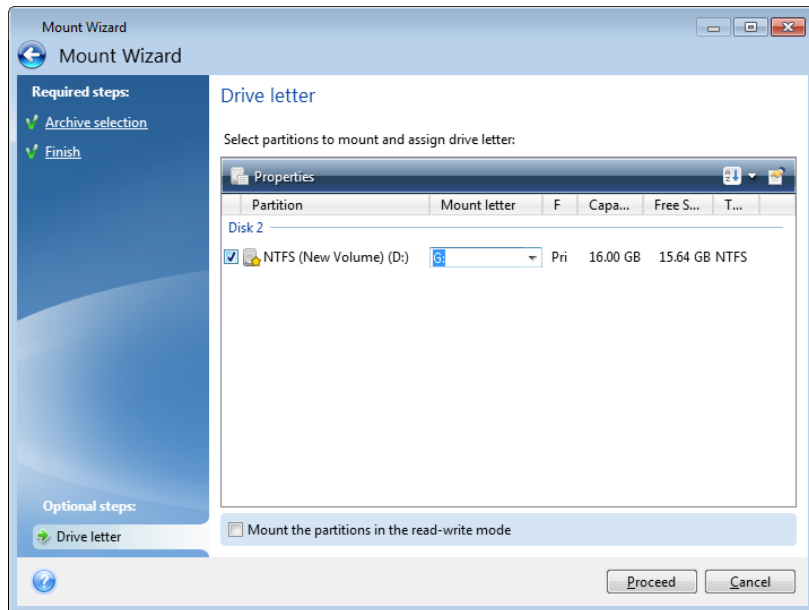
2. Select the archive for mounting.



3. Select a partition to mount as a virtual disk. (Note that you cannot mount an image of the entire disk except in the case when the disk consists of one partition). If the image contains several partitions, by default all of them will be selected for mounting with automatically assigned drive letters. If you would like to assign different drive letters to the partitions to be mounted, click **Options**.



You can also select a letter to be assigned to the virtual disk from the **Mount letter** drop-down list. If you do not want to mount a partition, select **Do not mount** in the list or unselect the partition's checkbox.



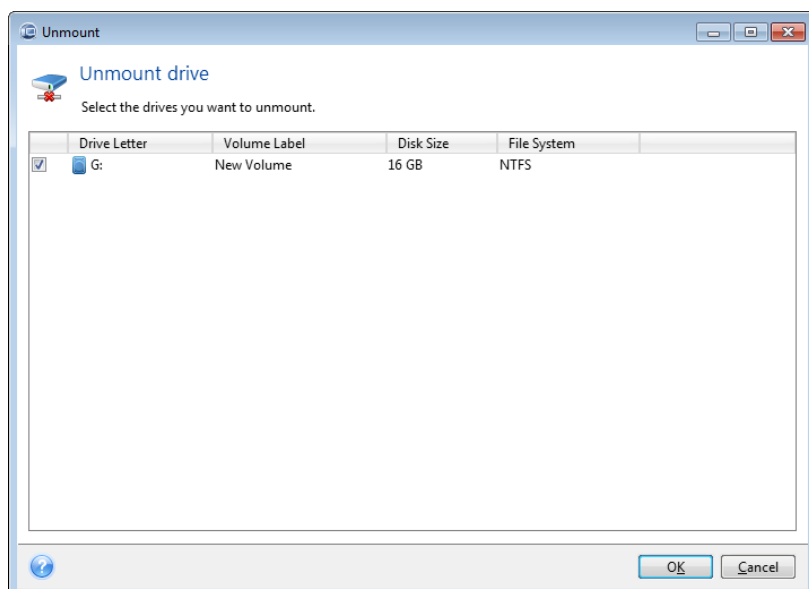
4. Having finished the settings, click **Proceed** to connect the selected partition images as virtual disks.
5. After the image is connected, the program will run Windows Explorer, showing its contents. Now you can work with files or folders as if they were located on a real disk.

11.2 Unmounting an image

We recommend that you unmount the virtual disk after all necessary operations are finished, as maintaining virtual disks takes considerable system resources. If you do not unmount the disk, it will disappear after your computer is turned off.

To disconnect the virtual disk, choose **Tools & Utilities** → **Unmount Image**, select the disk to unmount and click **OK**.

If you have mounted several partitions, by default all of them will be selected for unmounting. You can disconnect all mounted drives together or disconnect only those you do not need mounted anymore.



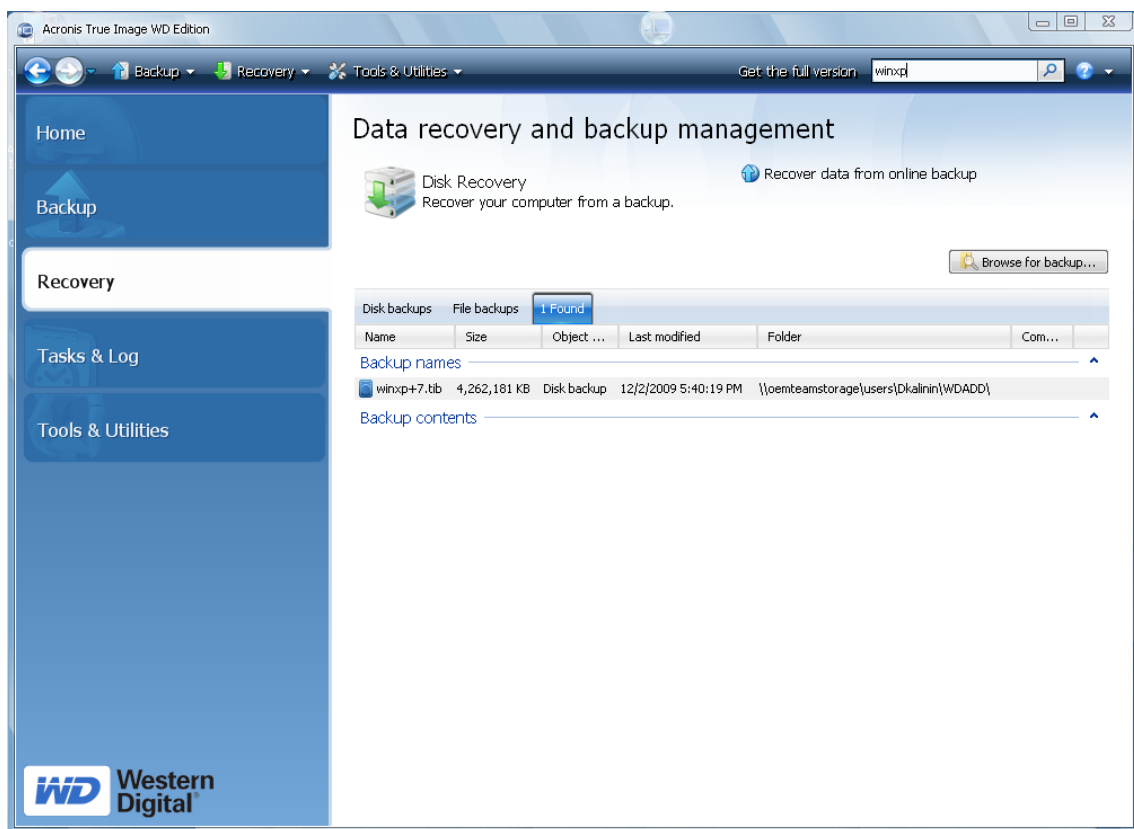
You can also do this in Windows Explorer by right-clicking on the disk icon and choosing **Unmount**.

12 Searching backup archives and their content

12.1 Searching

In addition to the ability to explore backup archives, Acronis True Image WD Edition provides a search facility for tib archives themselves, for files in tib archives only, as well as offering full-text search in the comments to archives. This facilitates searching for the information you need for using Acronis True Image WD Edition and for recovering files from your backup archives. Here's how you can search for the data you need.

1. Enter a search string into the Search field at the top right of the Acronis True Image WD Edition window and then click the magnifying glass icon. You will be taken to the **Data recovery and backup management** screen. The search results are output in the corresponding tab of the window.



2. By default the search is performed in all the sources where Acronis True Image WD Edition can search information. You can select an information source of interest by choosing the appropriate area among **Backup names** and **Backup contents**.

*Acronis True Image WD Edition cannot perform search on network shares and devices that are recognized by Windows as **Devices with removable storage**.*

- The **Backup names** area shows the results of the search for tib archives by archive filename. Double-clicking on a filename opens the corresponding archive in Windows Explorer where you can explore the archive contents. You can validate or recover the archive by right-clicking on its filename and choosing the appropriate item in the shortcut menu. The shortcut menu contains the following items: **Recover**, **Mount** (for image backups), **Validate**, **Move**, **Remove**, **Explore backup**, **Edit Comments**, and **Details** buttons for tib archives.

- The **Backup contents** area shows results of searches for files and folders in tib archives. Double-clicking on a filename opens the file. You can recover the file by right-clicking on its filename and choosing Recover in a shortcut menu. This shortcut menu also enables you to open the file or the parent folder that contains that file.

To help you better understand the search results, here is some information on the algorithms used by the Search feature.

1. When searching files in tib archives you can type all or part of the filename and use the common Windows wildcard characters. For example, to find all batch files in the archives, type "*.bat". Typing my???.exe will allow you to find all .exe files with names consisting of five symbols and starting with "my". It should be noted that search is case-insensitive, i.e. "Backup" and "backup" is the same search string. Furthermore, the search stops after the program finds 100 files corresponding to a search criterion you have typed. If the search results do not contain the file you need, you will have to refine the search criterion.

*When a file is included in several backups and it has not been modified, the search results will show it only once in the oldest backup file. If such a file has been changed, the search results will show all backup files containing **differing** versions of the file.*

2. Search in the comments to backup archives is carried out differently. First of all, you cannot use "*" and "?" as Windows wildcard characters. As in this case the program uses full text search, it will just find all occurrences of these characters in the comments (if any). The full text search uses the following rules:
 - Search criteria consist of words separated by space character(s) or by a logical operator: "AND", "OR", "NOT" (please, take note of the upper case).
 - Only one logical operator is allowed (the first one that occurs in a search string), otherwise they are ignored and interpreted as search words.
 - All space-separated words must be in a topic for successful match.

The **Backup names** area shows the archive files whose comments satisfy the search criterion. Double-clicking on an archive opens it for exploring.

12.2 Windows Search and Google Desktop integration

Acronis True Image WD Edition has plug-ins for Google Desktop and Windows Search (WDS). If you use any of these search engines on your computer, Acronis True Image WD Edition will detect the search engine you use and install an appropriate plug-in for indexing your tib backup archives. Indexing of backups will speed up searches in the backup archives. After such indexing you will be able to search archive content by entering a filename into the Google Desktop or Windows Search deskbar query field without opening Acronis True Image WD Edition. The search results will be shown in a browser window. Using the search results you can:

- Select any file and open it for viewing and/or save that file back to anywhere in the file system (not in the archive) or where it was before
- See in which archive a given file is stored and recover that archive

Google Desktop has a "Quick Find" window. This window is filled with the most relevant results from your computer. The results change as you type, so you can quickly get to what you want on your computer. Windows Search provides similar functionality.

In addition to indexing the files in backup archives by their names, the Google Desktop and Windows Search provide Acronis True Image WD Edition with the ability to perform full-text indexing of many files in tib archives, so you will be able to use this feature and perform searches of the files' content.

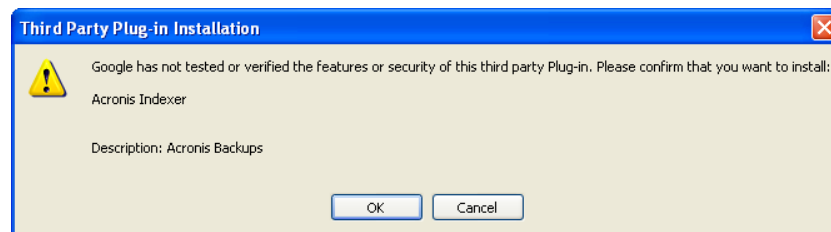
Full-text indexing of files in backup archives is provided only for the file types recognizable by Google Desktop and Windows Search. They recognize text files, Microsoft Office files, all Microsoft Office Outlook and Microsoft Outlook Express items, and more.

12.2.1 Using Google Desktop with Acronis True Image WD Edition

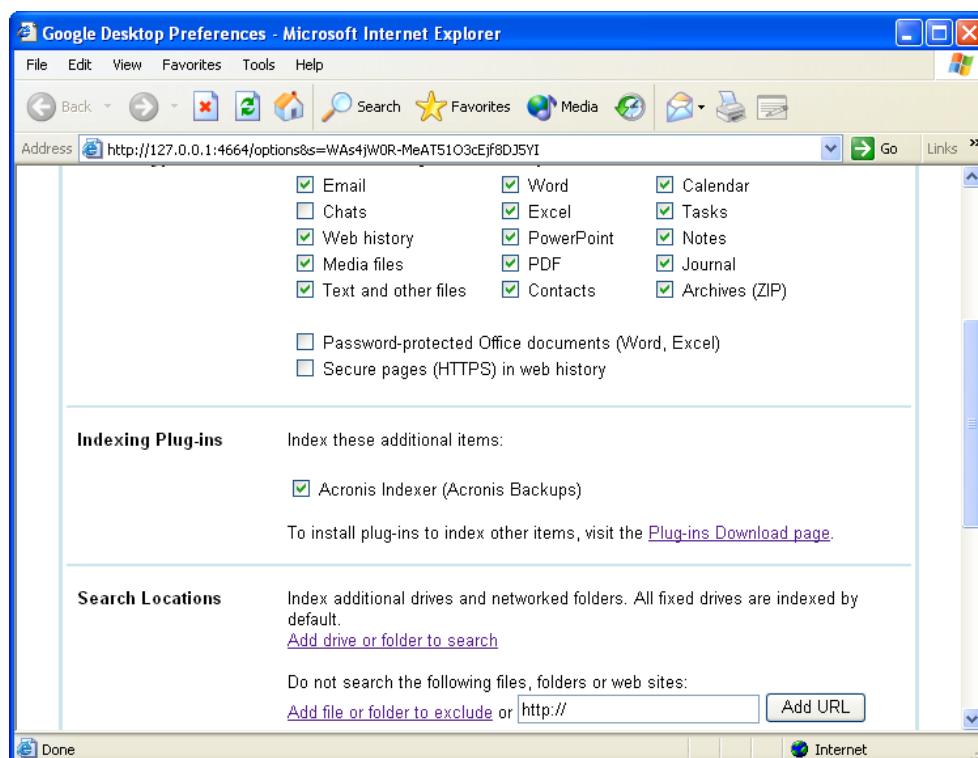
If you do not have Google Desktop, it can be downloaded for free from Google's Web site. Click Google Desktop and follow the instructions for download and installation.

To enable using Google Desktop for searching files in tib archives:

1. To install the plug-in, choose **Tools & Utilities** on the sidebar. Then click **Search settings** on the right pane and select the appropriate check box in the Desktop Search Options window. The following window appears.



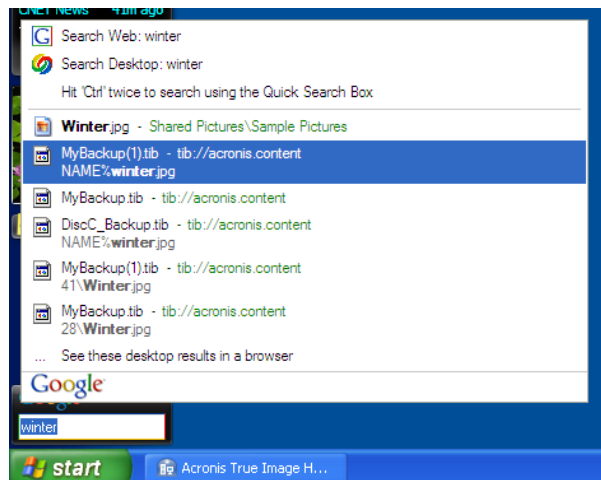
2. Verify that the plug-in is installed. Right-click on the Google Desktop icon in your system tray and select **Options** in the context menu. Google Desktop opens the **Preferences** window in your browser. Make sure that Acronis **Indexer (Acronis Backups)** is selected in the **Indexing Plug-ins** area.



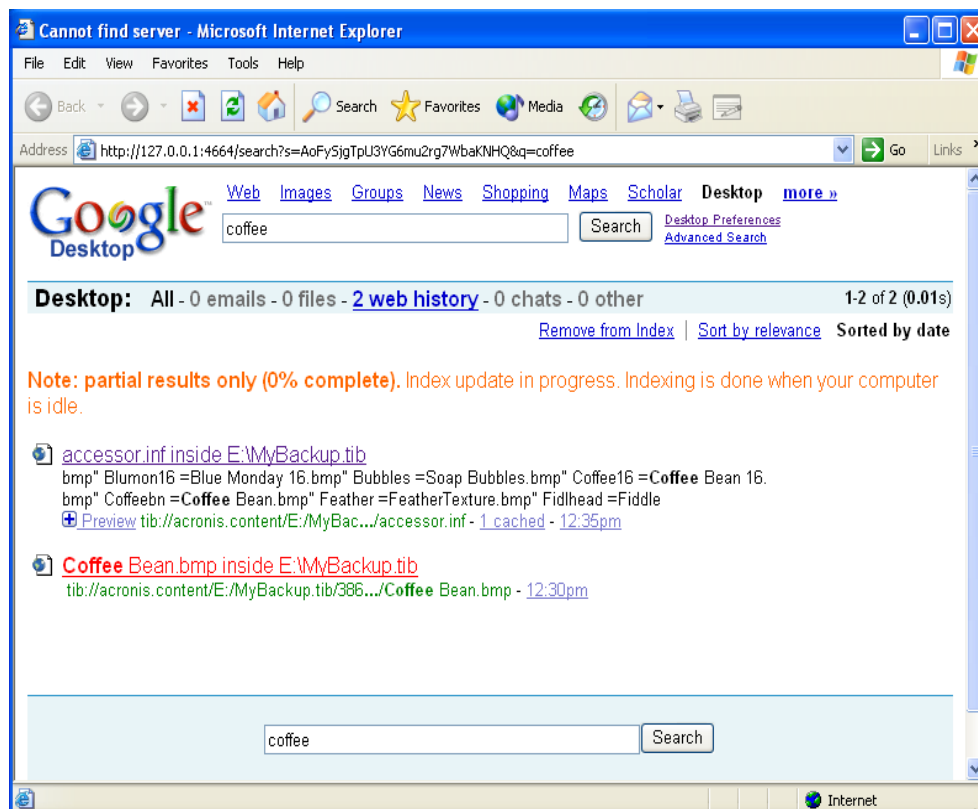
3. Right-click on the Google Desktop icon in your system tray once more and select **Indexing → Re-Index**. Click **Yes** in the confirmation window that appears. Google Desktop will add all the new content to the existing index.

Give Google Desktop some time for indexing all tib files on your computer's hard disks and adding the indexing information to its index database. The required time depends on the number of tib archives and the number of files they contain.

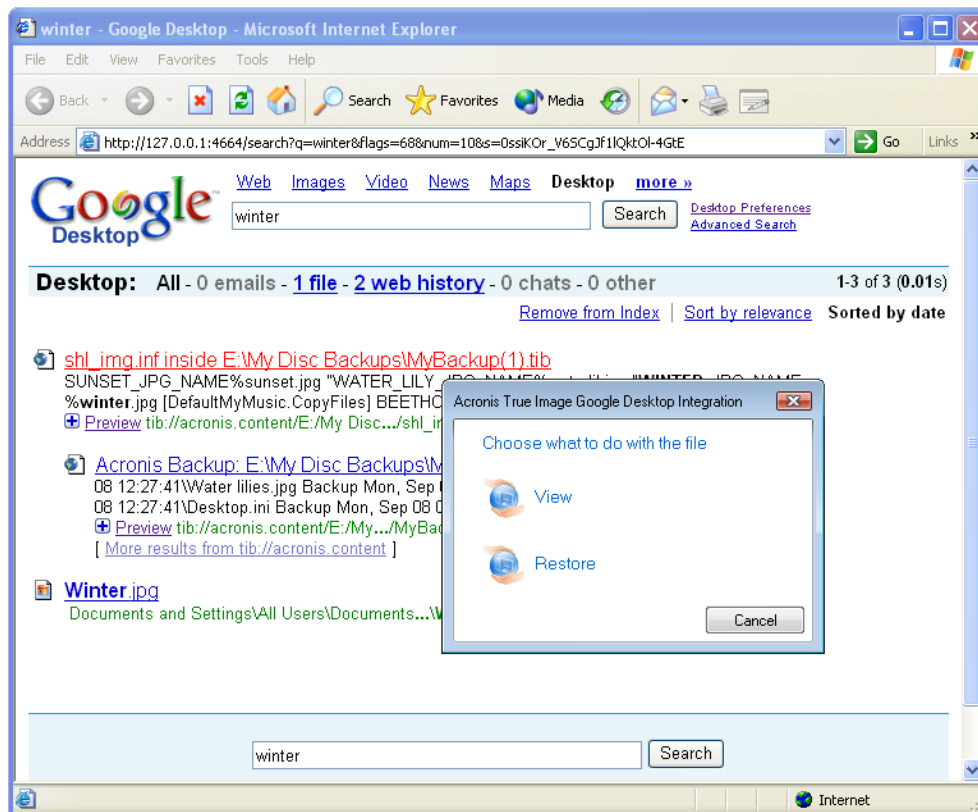
After for example an hour, check whether Google Desktop has indexed the tib archives by entering in its query field the name of a file which you know for sure that you backed up. If Google Desktop has completed indexing, it will show you the tib archives where it has found the file.



If you want to see all the search results, click the "See all N results in a browser" and you will see something like the screen shot below.



Clicking in the browser window on a line related to the desired file version opens a small dialog with just two options: **View** and **Recover**.



Choosing **View** starts the application associated with this file type and opens the file. Choosing **Recover** starts Acronis True Image WD Edition and you can then recover the file to a desired location.

12.2.2 Using Windows Search with Acronis True Image WD Edition

If you use any edition of Windows Vista or Windows 7 that has built-in Desktop Search functionality or Windows Desktop Search 3.0 or later, you can enable Windows Search support for tib files.

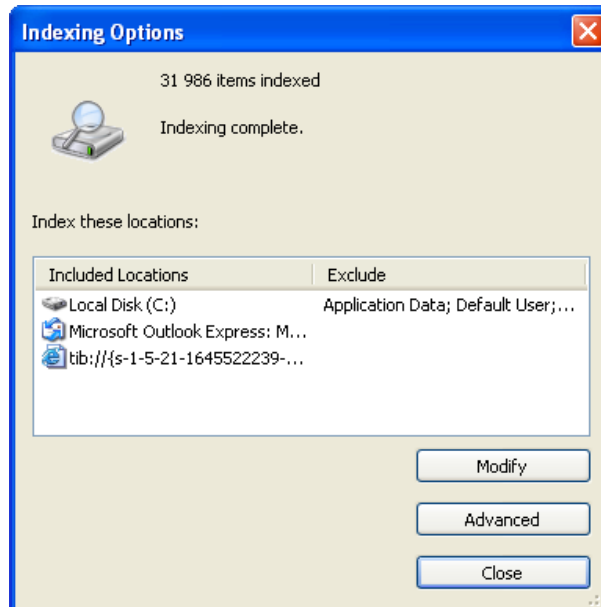
If you do not have Windows Search installed, but would like to use it, you can download Windows Search 4.0 for free from Microsoft's Web site. To download, click Windows Search 4.0. Double-click on the downloaded file and follow the instructions for installation.

Windows Search does not support indexing of zip files content.

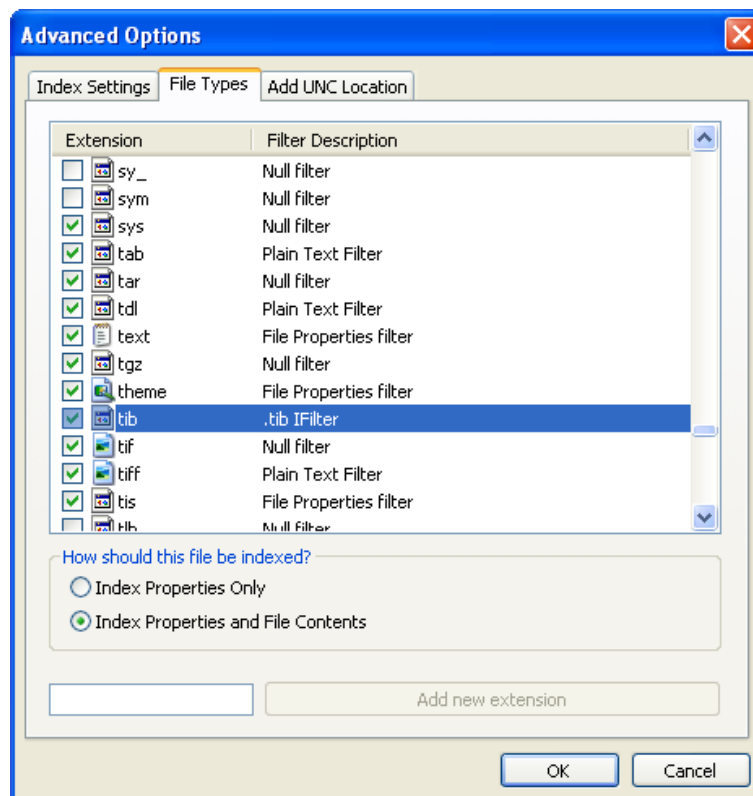
To use Windows Search support:

1. To register the plug-in, choose **Tools & Utilities** on the sidebar. Click **Search settings** on the right pane and select the appropriate check box in the Desktop Search Options window. After successful registration of the plug-in Acronis True Image WD Edition will display the "Plug-in registration succeeded" information window.
2. You can verify that the tib support is enabled. Right-click on the Windows Search icon in your system tray and select **Windows Desktop Search Options...** in the context menu. The following window appears. Make sure that the "tib://..." item is present in the Included Locations list.

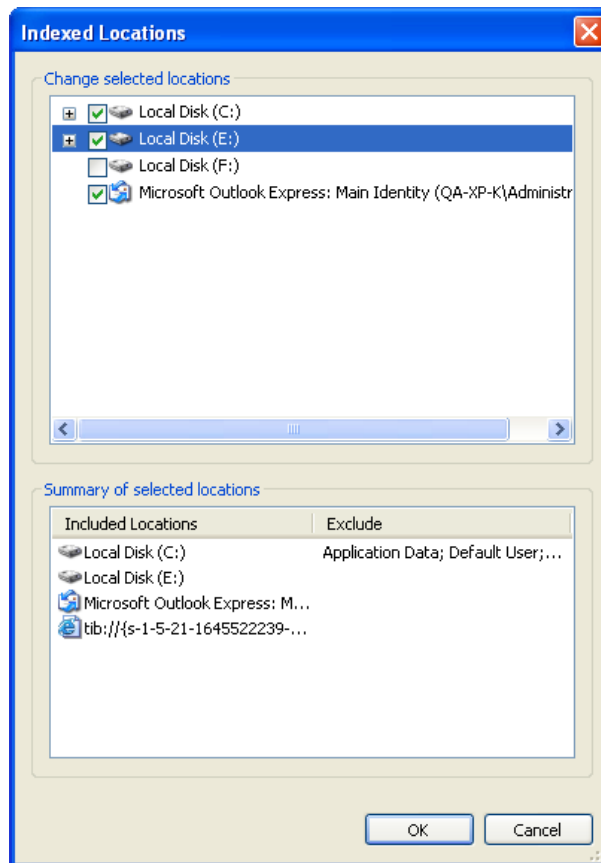
To open the Indexing Options window in Windows Vista, open the Control Panel and then double-click the **Indexing Options** icon. The Windows Vista indexing options have some differences in content and appearance, though most of the following information is applicable to Windows Vista as well.



3. Click **Advanced**, select the **File Types** tab and then make sure that the **tib** extension is selected and ".tib IFilter" is shown in the Filter Description field. **Select Index Properties and File Contents.**

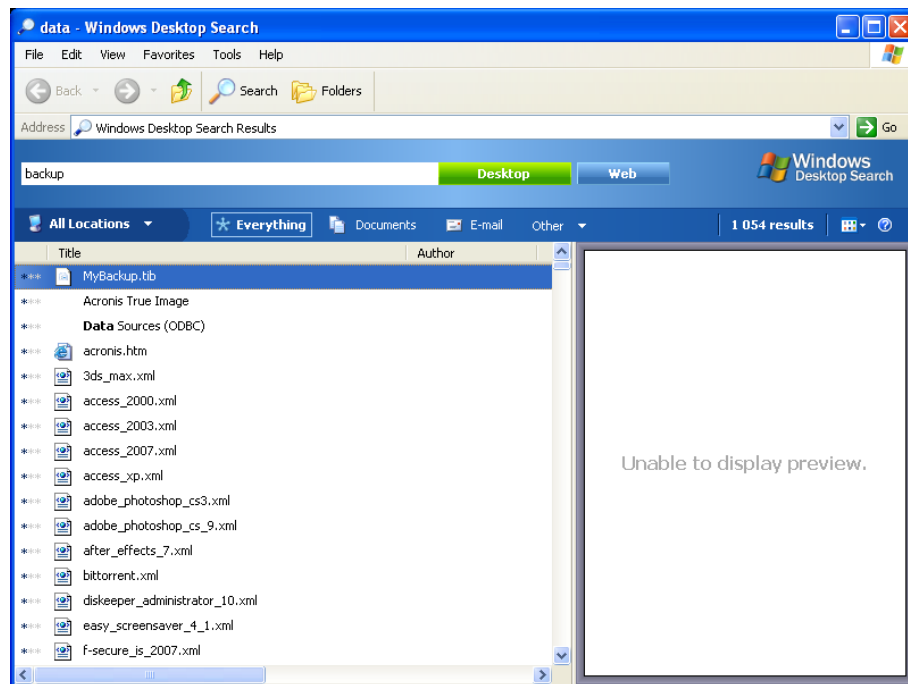


4. Click **OK** and while the **Indexing Options** window is open, check that the disks where you store your tib backup archives are shown in the "Included Locations" list. If the list does not contain those disks, the tib files will not be indexed. To include the disks, click **Modify** and select them in the window that appears.

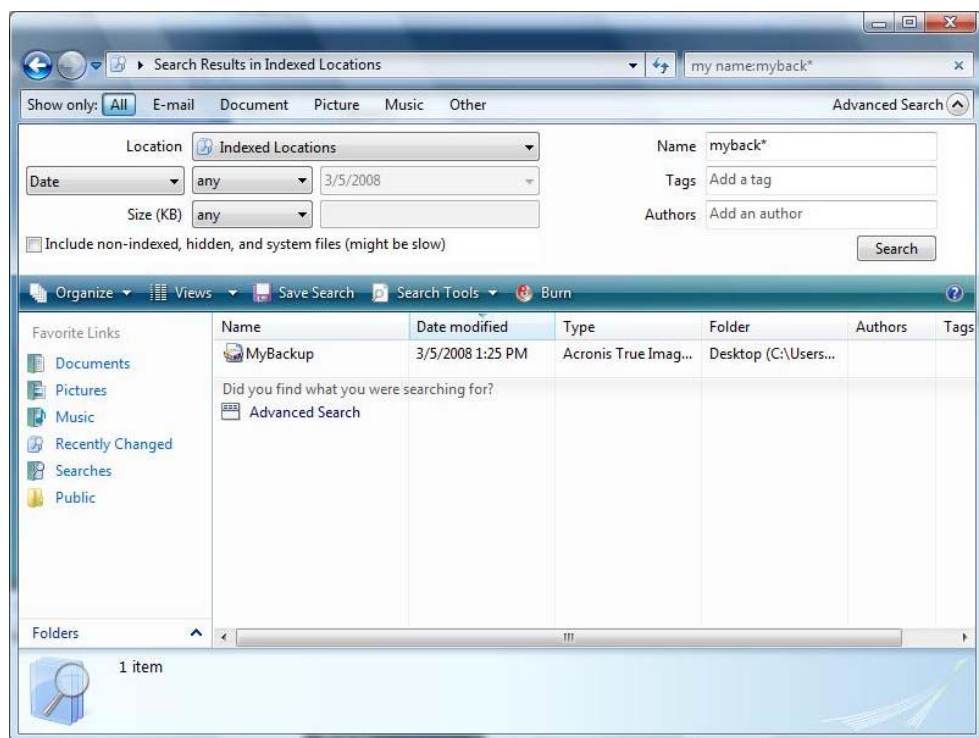


*If you store backups on a network share, Windows Search can index them too. You just have to add the share to the Indexed Locations list by typing the appropriate UNC path after selecting the **Add UNC Location** tab of **Advanced Options**.*

Give Windows Search some time for indexing all tib files on your computer's hard disks and adding the indexing information to its index database. The required time depends on the number of tib archives and the number of files they contain. After completing the indexing, the Desktop Search will be able to search files in tib backup archives. The search engines in WDS and Windows Vista have similar functionalities, though search results are presented somewhat differently:



Windows Search results



Windows Vista Search results

13 Other operations

13.1 Validating backup archives

The validation procedure checks whether you will be able to recover data from a particular backup, so when you select for validation:

- a full backup, the program validates the full backup only.

You can perform such validations using the **Validate Wizard**.

1. To validate an archive, click **Recovery** on the sidebar.
2. Select the archive to validate and click **Validate** on the toolbar.
3. Clicking **Proceed** will start the validation procedure. After the validation is complete, you will see the results window. You can cancel validation by clicking **Cancel**.

13.2 Viewing Tasks and Logs

Acronis True Image WD Edition has a Tasks and Log screen that allows you to view its working logs. The logs can provide information, for instance, about creating backup or validation results, including reasons for any failures.

Most Acronis True Image WD Edition operations write their own entries in the logs, though logs are not provided for image mounting/unmounting and bootable media creation.

The logs contain only partial information on operation of backup. The remaining information on operation of those features is written to their own log. That log is not available to users as it is intended for Acronis Support personnel to help in troubleshooting the issues users have with those features. It is included in Acronis System Report.

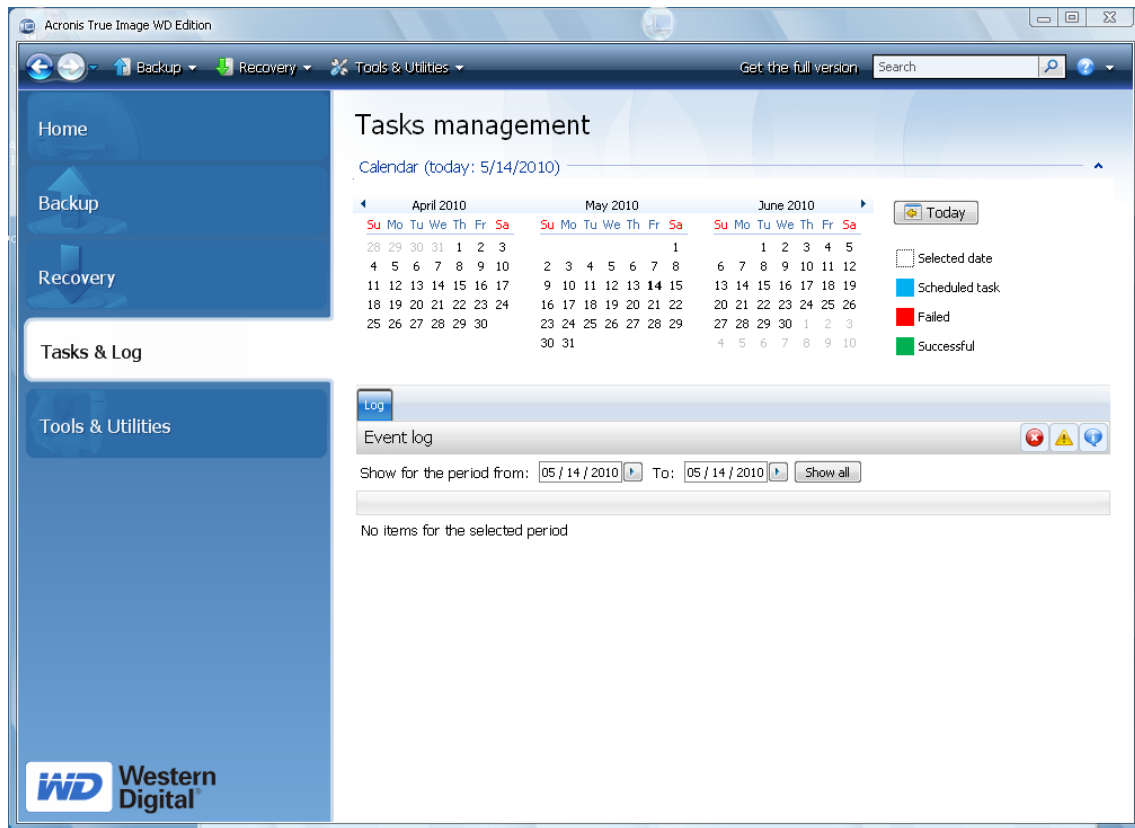
To open the **Tasks & Log** screen, click **Tasks & Log** on the sidebar. By default, the screen opens with the **Logs** tab selected. The tab shows logs for the selected date. If there are no logs for that date, an appropriate message appears.

The color marks in the calendar show information about the days with tasks completed with errors, and successfully completed tasks.

The buttons with left and right arrows at the sides of the calendar allow you to browse the months being shown in the calendar. If you have gone several months back or forward, clicking the **Today** button will quickly return you to the current month and date.

Clicking any day in the past takes you to the **Log** tab and shows logs for the selected date. If there are no logs for that date, an appropriate message appears.

When the **Log** tab is selected, the upper pane shows the calendar, while the lower one shows logs' contents.



To view the logs for a specific period, select the period by clicking the right arrow buttons in the **From:** and **To:** fields of the **Show for the period** area. Clicking the arrow in the **From:** field opens a pop-up calendar where you can set the start day of the period by double-clicking the appropriate day. Then set the end day using the same procedure for the **To:** field. You can change months and years in the pop-up calendars using the left and right arrows in the month name area. In addition, you can enter the desired period start and end dates directly in the fields. If you would like to see all the logs, click the **Show all** button.

To delete a log entry, select it and click the **Delete** button on the toolbar. To delete all log entries, click the **Delete all** button. You can also save a log entry to file by clicking the **Save** button. To save all logs to file, click **Save all**.

If any step shown in the logs was terminated by an error, the corresponding log will be marked with a red circle with a white cross inside.

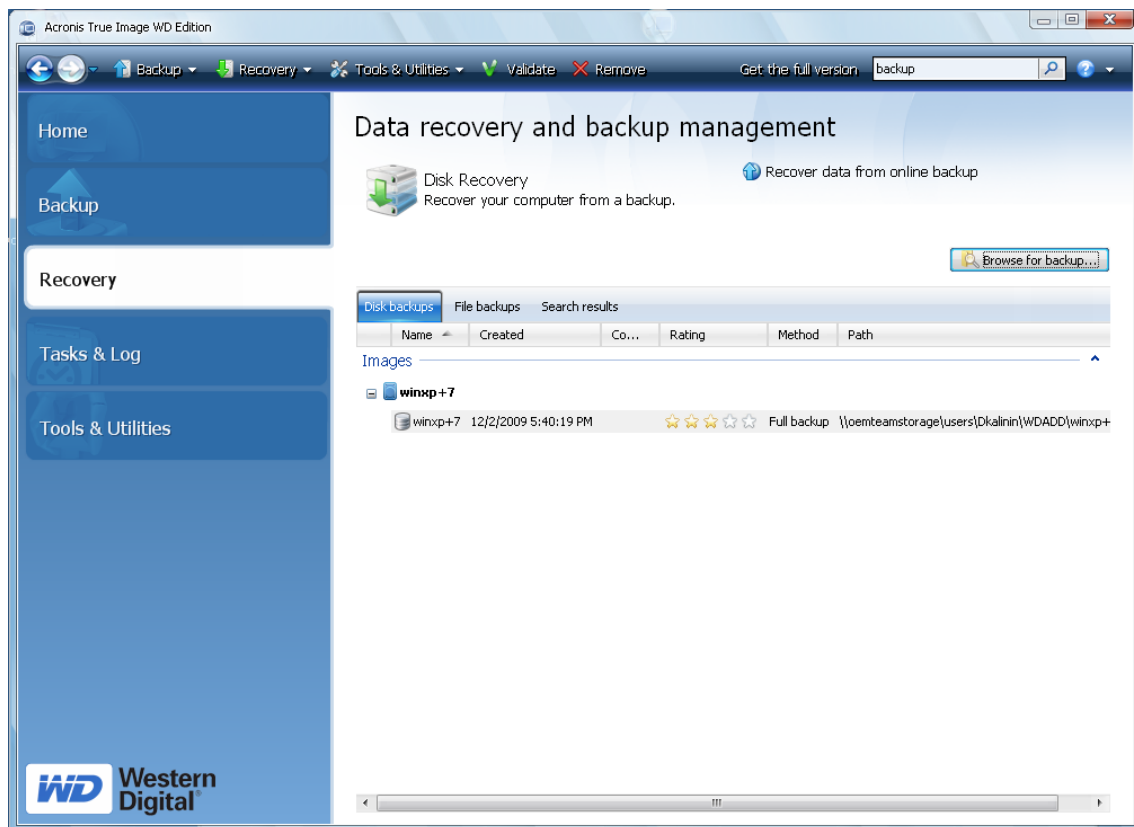
The three buttons to the right control message filters: the white cross in the red circle filters error messages, the exclamation mark in a yellow triangle filters warnings, and the "i" in the blue circle filters information messages.

To better view the details of the current step, you can hide the calendar by clicking the **Up** arrow at the top right of the calendar pane. This will enlarge the logs area. To view the calendar again, click the **Down** arrow at the top right of the calendar pane.

13.3 Managing backup archives

After a while you may wish (or be forced) to manage your backup archives, for example, in order to free up some space for new backups by removing the oldest backups or those you no longer need. As now Acronis True Image WD Edition stores information about the backup archives in a metadata information database, you must manage backup archives (e.g. delete or move some of them) by using the program's tools and not Windows Explorer. To manage your backup archives, go to the **Data recovery and backup management** screen by selecting **Recovery** on the sidebar.

The **Disk backups** tab lists the image backups.

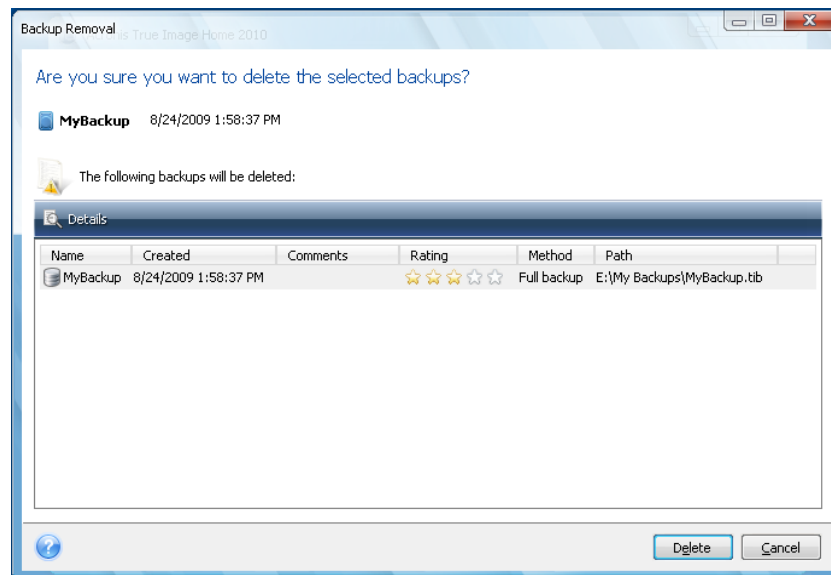


The shortcut menu opened by right-clicking on a desired backup archive provides the following operations with backups:

- **Explore** - see Exploring archives and mounting images
- **Recover** - see Recovery Wizard - detailed information (p. 46)
- **Validate Archive** - see Validating backup archives
- **Mount Image** (only for images) - see Mounting an image (p. 58)
- **Edit Comments** - editing comments made during backup creation
- **Rename** - renaming backup archives or individual backups (a backup is renamed only in the program's metadata database, however, the backup filename remains unchanged)
- **Move** - see Moving backup archives (p. 71)
- **Remove** - see Removing backup archives
- **Details** - viewing detailed information on the selected backup

13.4 Removing backup archives

You may want to remove backups and backup archives you no longer need. Because Acronis True Image WD Edition stores information on the backup archives in a metadata information database, deleting unneeded archive files using Windows Explorer will not delete information about these archives from the database and Acronis True Image WD Edition will consider that they still exist. This will result in errors when the program tries to perform operations on the backups that no longer exist. So you must only remove obsolete backups and backup archives using the tool provided by Acronis True Image WD Edition. To remove the entire backup archive, select it and click **Remove** on the toolbar or right-click on the full backup of the backup archive and choose **Remove** in the shortcut menu. The following screen appears:



If you click **Delete**, the program will remove the backup archive from its metadata information database as well as from the hard disk.

13.5 Moving backup archives

Now Acronis True Image WD Edition allows you to move backup archives to another location. This may come in handy if you want to free space for a new backup, but want to keep an earlier backup archive at another location, for example, a network share. Another possible scenario - you want to recover a disk used for keeping your archives. As the program cannot recover if the backup archive is on the same disk you are going to recover, you need to move the archive to another hard disk.

1. Select the archive for moving after clicking **Recovery** on the sidebar.
2. To move the archive, select it on the **Data recovery and backup management** screen. If the archive consists of several backups, you can select any of them because Acronis True Image WD Edition always moves the entire archive.
3. After making your selection, right-click and choose **Move** in the shortcut menu.
4. When moving is complete, the path to the archive will change in the **Path** column of the Data recovery and backup management screen.

14 Transferring the system to a new disk

14.1 General information

Sooner or later, most computer users find that their hard disk is too small. If you just don't have space for more data, you can add another disk just for data storage as described in the following chapter.

However, you might find that your hard disk does not have enough space for the operating system and installed applications, preventing you from updating your software or installing new applications. In this case, you have to transfer the system to a higher-capacity hard disk.

To transfer the system, you must first install the disk in the computer (see details in Hard disks and boot sequence (p. 93)). If your computer doesn't have a bay for another hard disk, you can temporarily install it in place of your CD drive or use a USB connection to the external target disk. If that is not possible, you can clone a hard disk by creating a disk image and recovering it to a new hard disk with larger partitions.

There are two transfer modes available: automatic and manual.

In the automatic mode, you will only have to take a few simple steps to transfer all the data, including partitions, folders and files, to a new disk, making it bootable if the original disk was bootable.

There will be only one difference between these disks – partitions on the newer disk will be larger. Everything else, including the installed operating systems, data, disk labels, settings, software and everything else on the disk, will remain the same.

This is the only result available in the automatic mode. The program can only duplicate the original disk layout to the new one. To obtain a different result, you will have to answer additional questions about cloning parameters.

The manual mode will provide more data transfer flexibility. You will be able to select the method of partition and data transfer:

- as is
- new disk space is proportionally distributed between the old disk partitions
- new disk space is distributed manually

On program screens, damaged partitions are marked with a red circle and a white cross inside in the upper left corner. Before you start cloning, you should check such disks for errors and correct the errors using the appropriate operating system tools.

The current Acronis True Image WD Edition version does not support cloning of dynamic and GPT disks.

14.2 Security

Please note the following: if the power goes off or you accidentally press **RESET** during the transfer, the procedure will be incomplete and you will have to partition and format or clone the hard disk again.

No data will be lost because the original disk is only being read (no partitions are changed or resized). The system transfer procedure does not alter the original disk at all. After the procedure finishes, you

might want to format the old disk or securely wipe the data it contains. Use Windows tools or Acronis DriveCleanser for these tasks.

Nevertheless, we do not recommend that you delete data from the old disk until you are sure it is correctly transferred to the new disk, the computer boots up from it and all applications work.

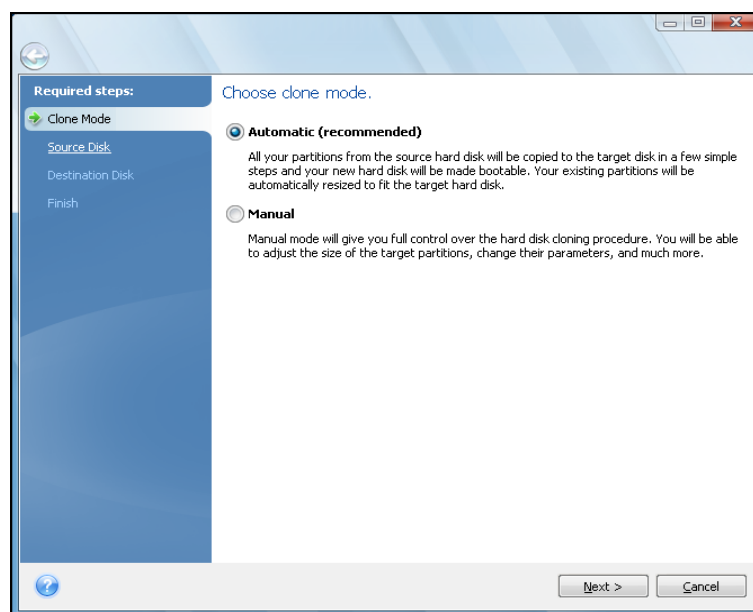
14.3 Executing transfers

For best results, install the target (new) drive where you plan to use it and the source drive in another location, e.g. in an external USB enclosure. This recommendation is especially important for laptops.

To start cloning, select **Tools & Utilities** → **Clone disk** in the main program menu.

14.3.1 Selecting Clone mode

You will see the **Clone Mode** window.

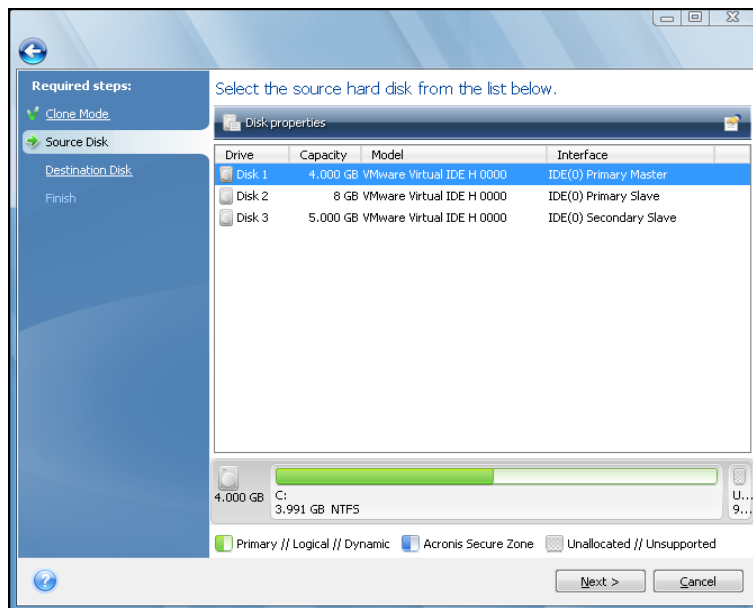


We recommend using automatic mode in most cases. The manual mode can be useful if you need to change the disk partition layout.

If the program finds two disks, one partitioned and another unpartitioned, it will automatically recognize the partitioned disk as the source disk and the unpartitioned disk as the destination disk. In such case, the next steps will be bypassed and you will be taken to the cloning Summary screen.

14.3.2 Selecting source disk

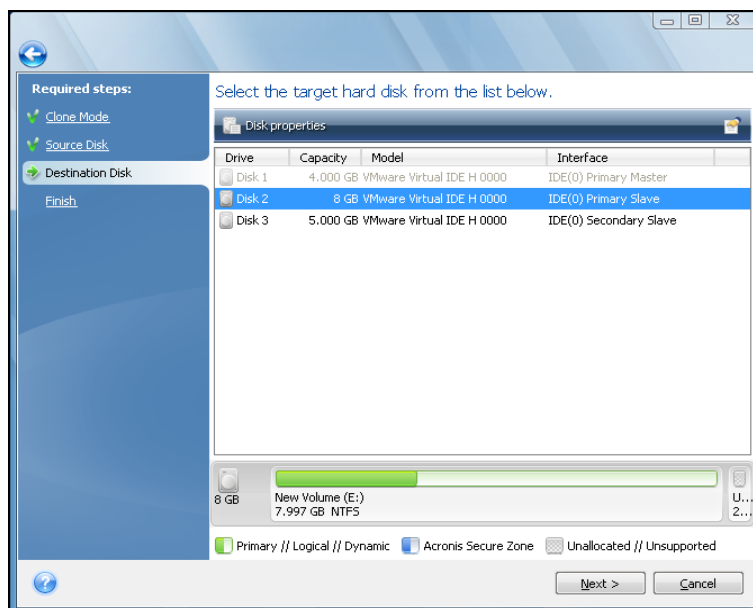
If the program finds several partitioned disks, it will ask you which one is the source (i.e. the older data disk).



You can determine the source and destination using the information provided in this window (disk number, capacity, label, partition, and file system information).

14.3.3 Selecting destination disk

After you select the source disk, you have to select the destination where the disk information will be copied.

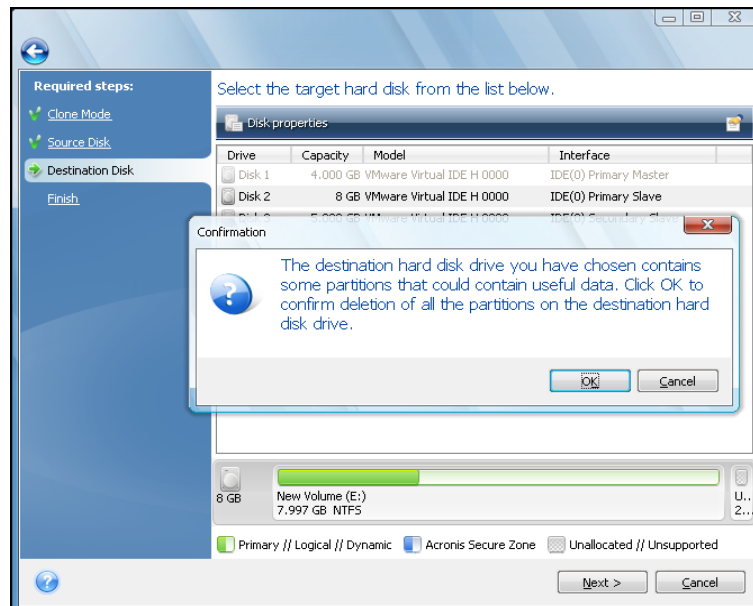


The previously selected source becomes grayed-out and disabled for selection.

If any disk is unpartitioned, the program will automatically recognize it as the destination and bypass this step.

14.3.4 Partitioned destination disk

At this point, the program checks to see if the destination disk is free. If not, you will be prompted by the Confirmation window stating that the destination disk contains partitions, perhaps with useful data.



To confirm deletion of the partitions, click **OK**.

*Note that no real changes or data destruction will be performed at this time! For now, the program will just map out cloning. All changes will be implemented only when you click **Proceed**.*

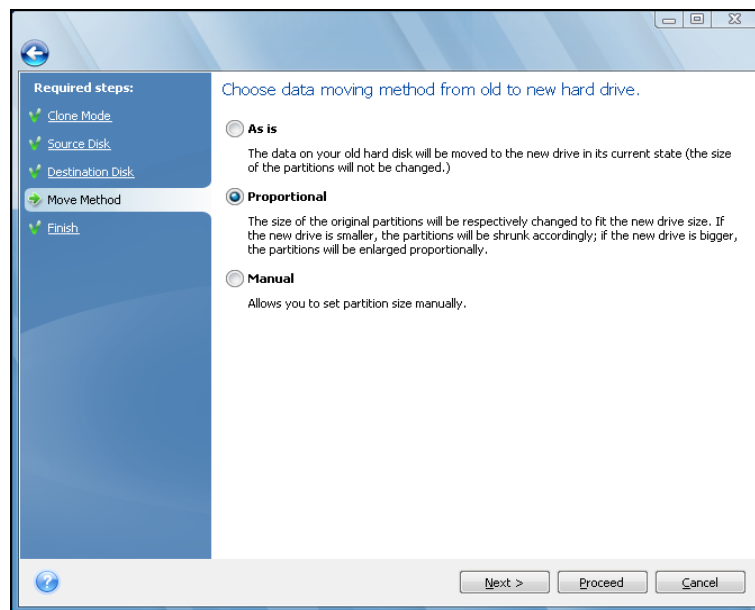
If you selected the automatic mode, the program will not ask you anything else and will take you to the cloning summary window.

14.3.5 Selecting partition transfer method

When you select the manual cloning mode, Acronis True Image WD Edition will offer you the following data move methods:

- **As is**
- **Proportional** – the new disk space will be proportionally distributed among cloned partitions

- **Manual** – you will specify the new size and other parameters yourself



If you elect to transfer information "as is," a new partition will be created for every old one with the same size and type, file system and label. The unused space will become unallocated. Afterwards, you will be able to use the unallocated space to create new partitions or to enlarge the existing partitions with special tools, such as Acronis Disk Director Suite.

As a rule, "as is" transfers are not recommended as they leave a lot of unallocated space on the new disk. Using the "as is" method, Acronis True Image WD Edition transfers unsupported and damaged file systems.

If you transfer data proportionally, each partition will be enlarged, according to the proportion of the old and new disk capacities.

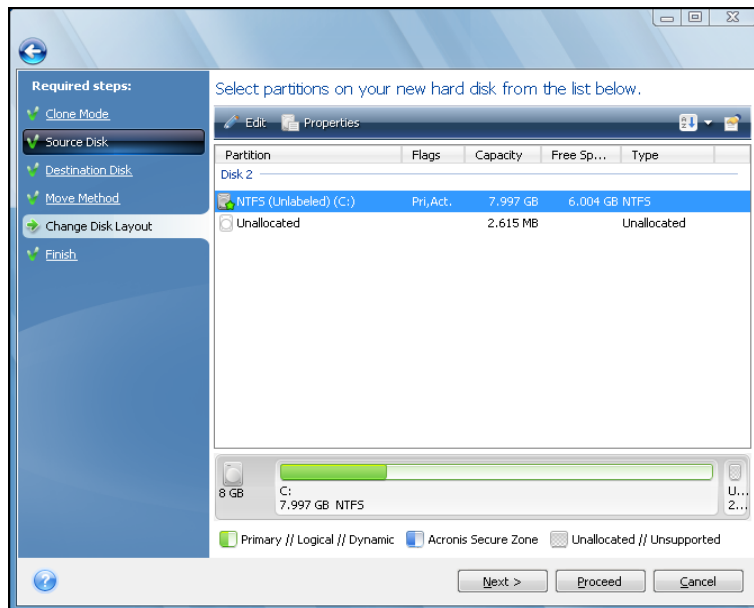
FAT16 partitions are enlarged less than others, as they have a 4GB size limit.

Depending on the selected combination, you will proceed to either the cloning summary window, or the Change disk layout step (see below).

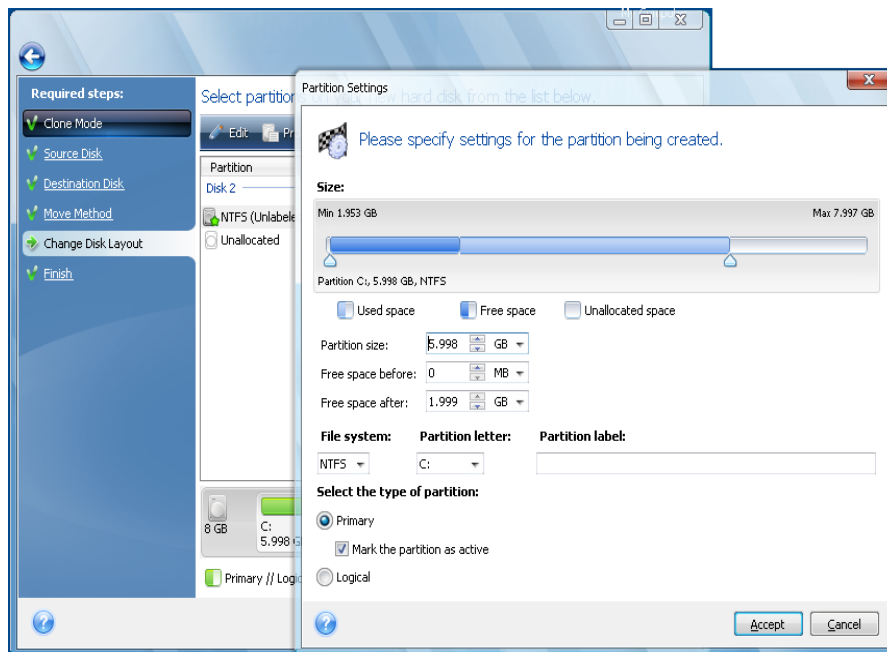
14.3.6 Cloning with manual partitioning

The manual transfer method enables you to resize partitions on the new disk. By default, the program resizes them proportionally. In the next window, you will see the new disk layout.

Along with the hard disk number, you will see disk capacity, label, partition, and file system information. Different partition types, including primary, logical, and unallocated space are marked with different colors.



First, select a partition to resize and click **Edit** on the toolbar. This will open the Partition Settings window, where you can resize and relocate the partition.



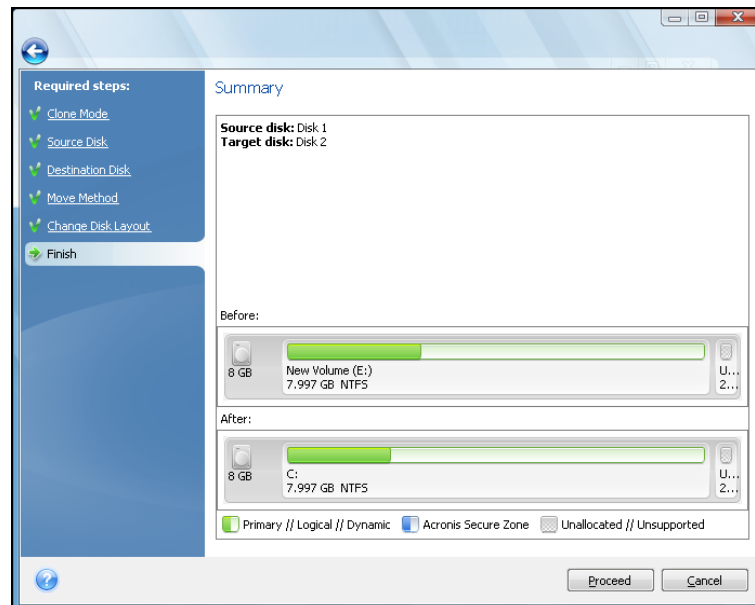
You can do this by entering values in the **Free space before**, **Partition size**, **Free space after** fields, by dragging partition borders or the partition itself.

If the cursor turns into two vertical lines with left and right arrows, it is pointed at the partition border and you can drag it to enlarge or reduce the partition's size. If the cursor turns into four arrows, it is pointed at the partition, so you can move it to the left or right (if there's unallocated space near it).

Having provided the new location and size, click **Accept**. You will be taken back to the Change disk layout window. You might have to perform some more resizing and relocation before you get the layout you need.

14.3.7 Cloning summary

The cloning summary window graphically (as rectangles) illustrates information about the source disk (partitions and unallocated space) and the destination disk layout. Along with the disk number, some additional information is provided: disk capacity, label, partition and file system information. Partition types — primary, logical and unallocated space — are marked with different colors.



Cloning a disk containing the currently active operating system will require a reboot. In that case, after clicking **Proceed** you will be asked to confirm the reboot. Canceling the reboot will cancel the entire procedure. After the clone process finishes you will be offered an option to shut down the computer by pressing any key. This enables you to change the position of master/slave jumpers and remove one of the hard drives.

Cloning a non-system disk or a disk containing an operating system, but one that is not currently active, will proceed without the need to reboot. After you click **Proceed**, Acronis True Image WD Edition will start cloning the old disk to the new disk, indicating the progress in a special window. You can stop this procedure by clicking **Cancel**. In that case, you will have to repartition and format the new disk or repeat the cloning procedure. After the cloning operation is complete, you will see the results message.

15 Adding a new hard disk

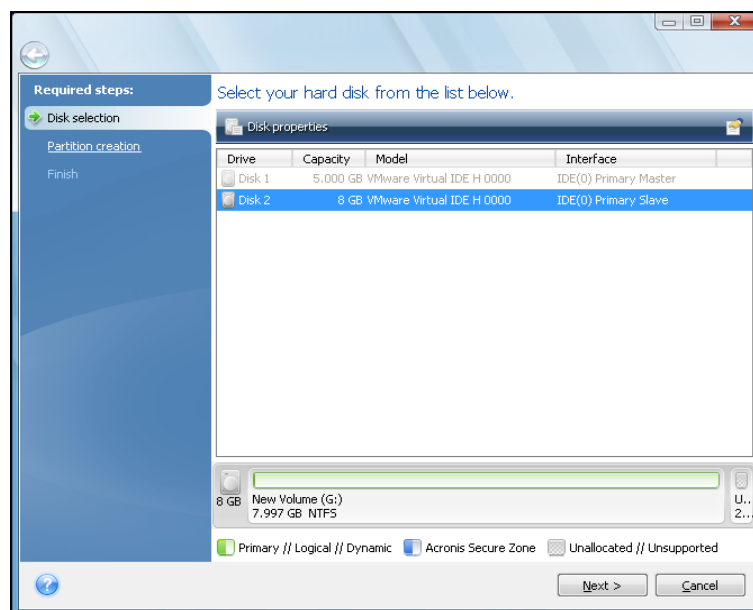
If you don't have enough space for your data, you can either replace the old disk with a new higher-capacity one (data transfers to new disks are described in the previous chapter), or add a new disk only to store data, leaving the system on the old disk. If the computer has a bay for another disk, it would be easier to add a data disk drive than to clone a system drive.

To add a new disk, you must first install it in your computer.

15.1 Selecting a hard disk

To start the Add New Disk Wizard, select **Tools & Utilities** → **Add New Disk** in the main program menu.

Select the disk that you've added to the computer.



If there are any partitions on the new disk, you will be shown a warning window. For you to be able to add the disk, they must be deleted first, so click **OK** to continue.

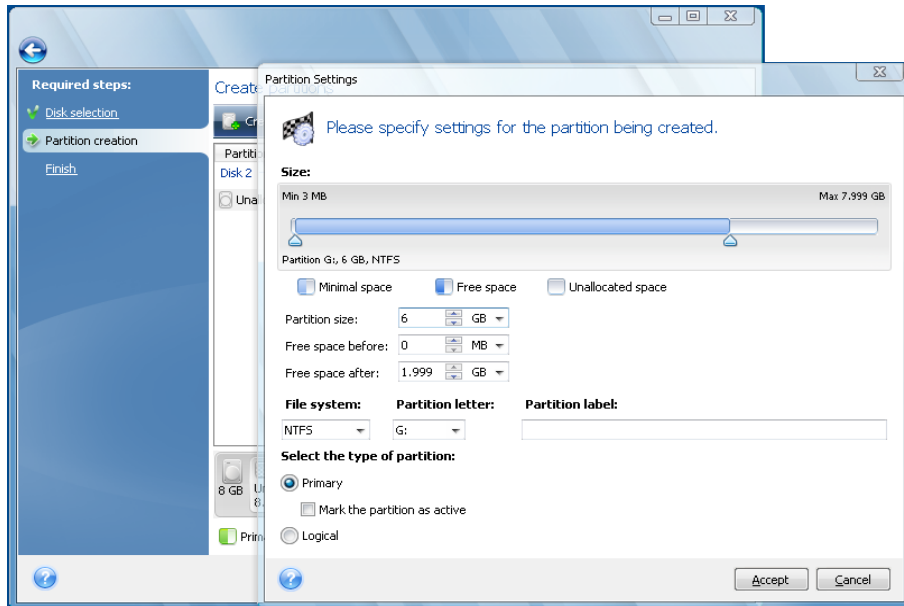
15.2 Creating new partitions

Next you will see the current partition layout. Initially, all disk space will be unallocated. This will change after you add new partitions.

To create a partition, click **Create new partition** on the toolbar and set the new partition location and size. You can do this both by entering values in the **Free space before**, **Partition size**, **Free space after** fields, and by dragging partition borders or the partition itself.

If the cursor turns into two vertical lines with left and right arrows, it is pointed at the partition border and you can drag it to enlarge or reduce the partition size. If the cursor turns into four arrows, it is pointed at the partition, so you can move it to the left or right (if there is unallocated space near it).

Select a file system for the new partition. You may select a partition letter of your choice (or leave the default one) and input a label for the new partition in the corresponding field. Finally, select a partition type.

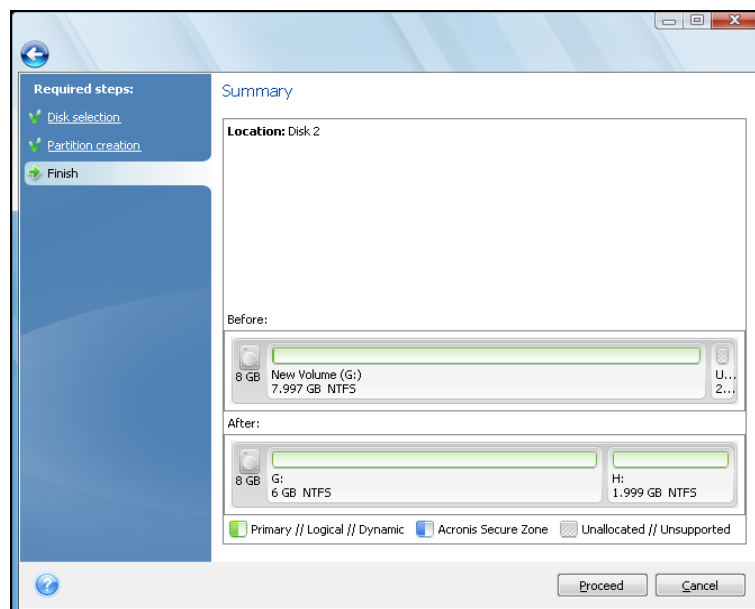


Click the **Accept** button and you will be taken back to the Partition Creation screen. Check the resulting partition's settings and start creating another partition by clicking **Create new partition** again. You can also edit the new partition's settings by clicking **Edit** on the toolbar or delete it by clicking **Delete**.

*If you allocate all unallocated space on the disk to the new partition, the **Create new partition** button disappears.*

15.3 Disk add summary

Clicking **Next** after creating a desired partition layout takes you to the disk add summary. The disk add summary contains a list of operations to be performed on disks.



After you click **Proceed**, Acronis True Image WD Edition will start creating new partition(s), indicating the progress in a special window. You can stop this procedure by clicking **Cancel**. You will then have to repartition and format the new disk or repeat the disk add procedure.

16 Security and Privacy Tools

Acronis True Image WD Edition includes tools for secure destruction of data on an entire hard disk drive, individual partitions.

These tools ensure the security of your confidential information, as well as maintain your privacy when you work with a PC, because they clean-up the evidence showing your actions (records in various system files) that you don't even know about. This could include usernames and passwords.

If you need to:

- **securely destroy data** on selected partitions and/or disks so it can't be recovered, run **Acronis DriveCleanser**.

16.1 Acronis DriveCleanser

Many operating systems do not provide users with secure data destruction tools, so deleted files can be recovered easily by using simple applications. Even a complete disk reformat cannot guarantee you permanent confidential data destruction.

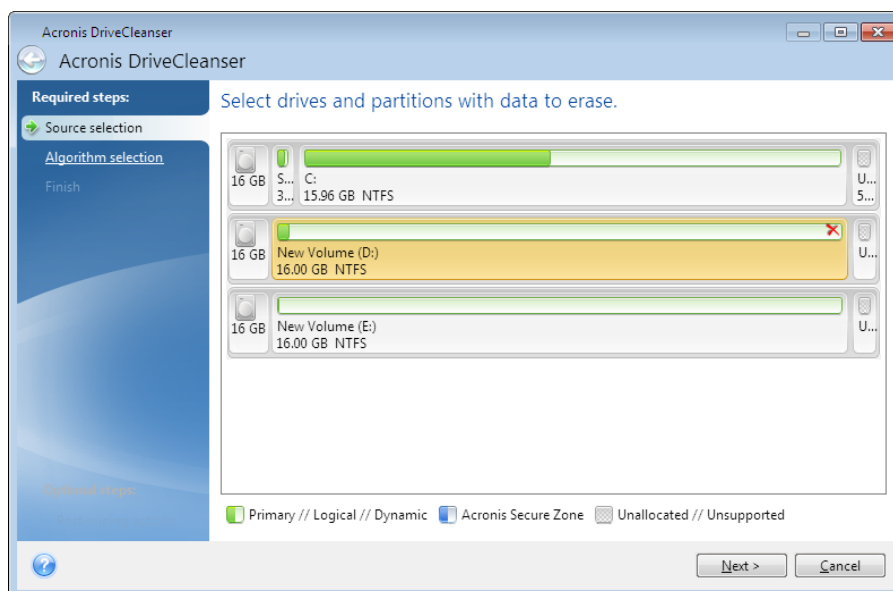
Acronis DriveCleanser solves this problem with guaranteed and permanent data destruction on selected hard disks and/or partitions. It allows you to select from a number of data destruction methods depending on the importance of your confidential information.

To start Acronis DriveCleanser, select **Tools & Utilities** → **Acronis DriveCleanser** in the main program menu. Acronis DriveCleanser allows you to do the following:

- clean up selected hard disks or partitions using preset methods;
- create and execute custom user methods of hard disk clean-up.

Acronis DriveCleanser is based on a **wizard** that **scripts** all hard disk operations, so no data destruction is performed until you click **Proceed** in the wizard's Summary window. At any moment, you can return to the previous steps to select other disks, partitions or data destruction methods.

First, you must select the hard disk partitions where you want to destroy data.



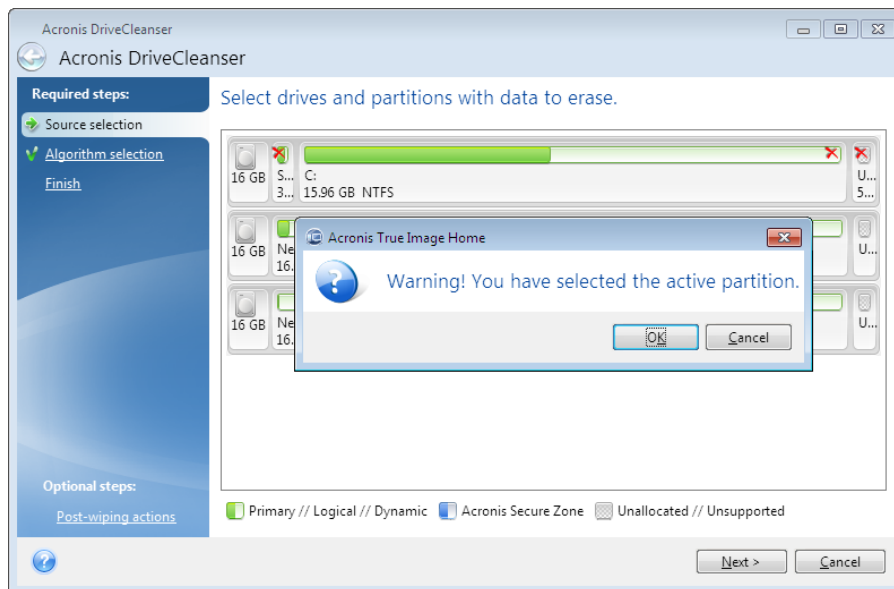
To select a partition, click the corresponding rectangle. You will see a red mark in the upper right corner indicating that the partition is selected.

You can select an entire hard disk or several disks for data destruction. To do this, click the rectangle corresponding to the hard disk (with a device icon, disk number and capacity).

You can simultaneously select several partitions located on different hard disk drives or on several disks, as well as unallocated space on disks.

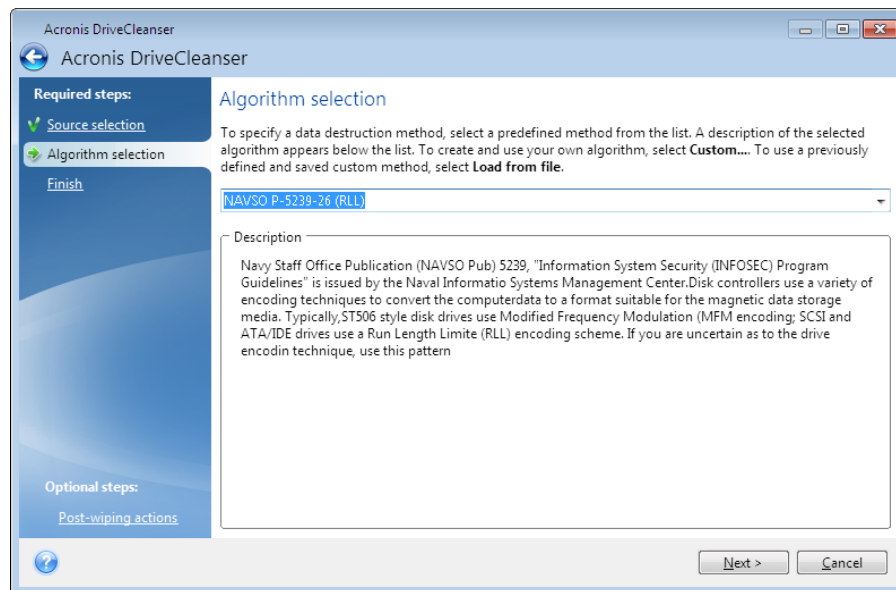
Click **Next** to continue.

If the disks and/or partitions you have selected include the system disk or partition, you will see a warning window.



Be careful, because clicking **OK** in this warning window and then **Proceed** in the Summary window will result in wiping the system partition containing your Windows operating system.

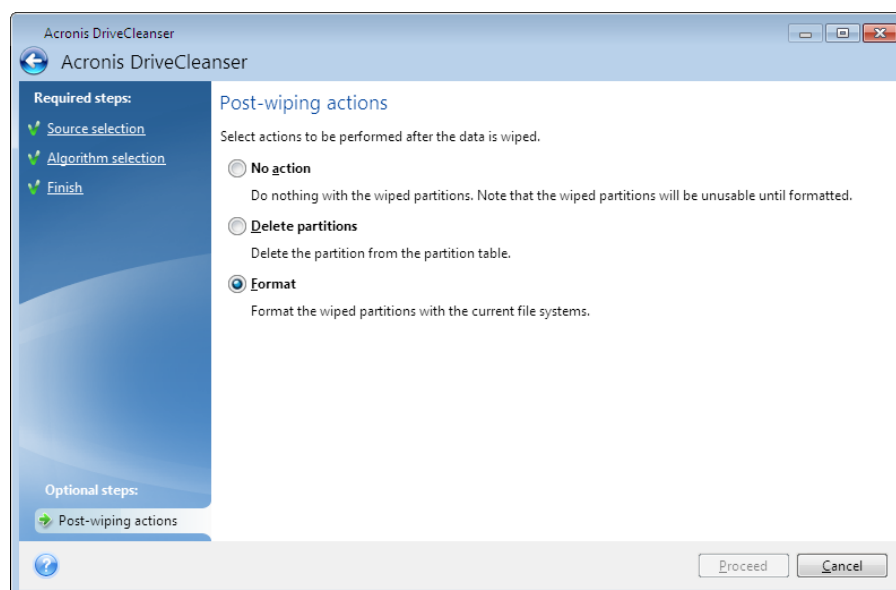
Acronis DriveCleanser utilizes a number of the most popular data destruction methods described in detail in Hard Disk Wiping Methods (p. 97) of this manual. If you want to create a custom data destruction algorithm, choose **Custom...** and go to Creating custom algorithms of data destruction (p. 85).



After selecting or creating the disk wiping method click **Next** to continue. Acronis DriveCleanser will display the data destruction task summary. You can click **Proceed** after selecting the **Wipe the selected partitions irreversibly** box or click **Options** to select the post-wiping action on the partitions selected for data destruction, if the default action, namely, **Format** does not suit you.

In the **Post-wiping actions** window Acronis DriveCleanser offers you three choices:

- **No action** — just destroy data using the method selected below
- **Delete partitions** — destroy data and delete partition(s)
- **Format** — destroy data and format partition (default)



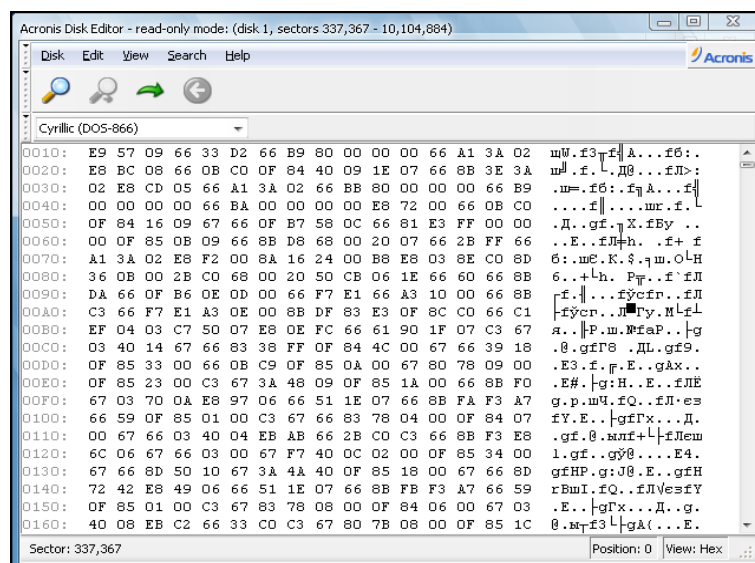
In this example, the switch is set to **Format**. This will allow you to see the results of partition and data destruction, along with the reformatting of the partition.

You cannot delete partitions on dynamic and GPT disks.

Up to this point, you can make changes in the created task. Clicking **Proceed** after you select a post-wiping action will launch the task execution (if the **Proceed** button is unselectable, click **Finish** on the sidebar and select the **Wipe the selected partitions irreversibly** box to enable the **Proceed** button). Acronis DriveCleanser will perform all actions necessary for destroying the contents of the selected partition or disk. After this is done, you will see a message indicating the successful data destruction.

Acronis DriveCleanser offers you another useful capability — to estimate the results of executing a data destruction method on a hard disk or partition. To view the state of your cleaned disks or partitions, choose **Tools & Utilities** on the sidebar. The Acronis DriveCleanser area in the right pane contains the **View the current state of your hard drives** link. Click on the link and then choose the partition whose cleaning results you wish to view. This opens an integrated Acronis Disk Editor (in read-only mode).

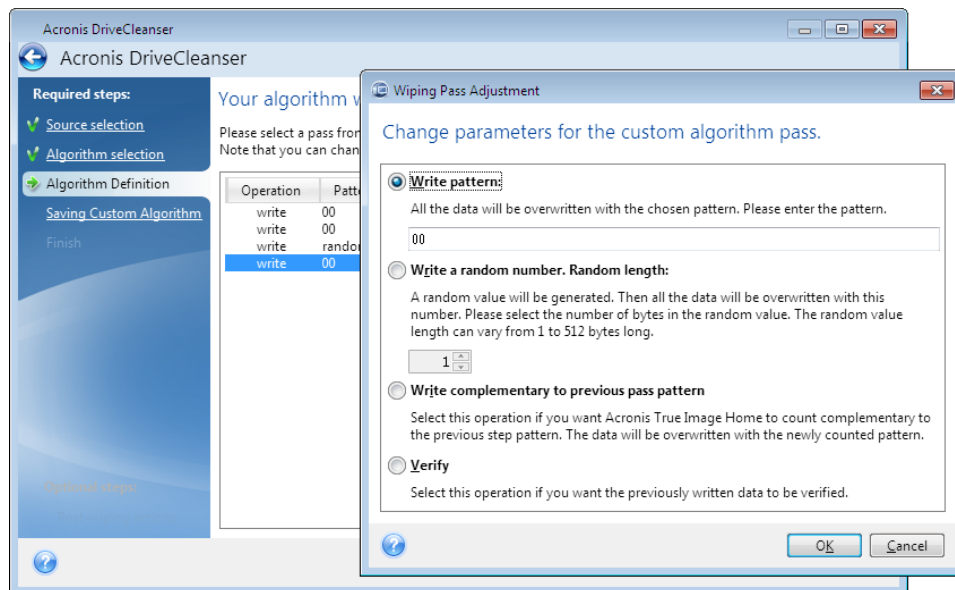
The aforementioned algorithms offer various levels of confidential data destruction. Thus the picture you might see on a disk or partition depends on the data destruction method. But what you actually see are disk sectors filled with either zeros or random symbols.



16.2 Creating custom algorithms of data destruction

Acronis DriveCleanser gives you the opportunity to create your own algorithms for wiping hard disks. Although the software includes several levels of data destruction, you can choose to create your own. This is recommended only for users familiar with the principles of data destruction used in secure disk wiping methods.

Creating a custom method of hard disk wiping is possible after choosing "**Custom...**" from the drop-down list in the **Algorithm selection** window. In this case some new required steps appear in the DriveCleanser wizard and you will be able to create a data destruction algorithm matching your security requirements.



Having created a custom method, you can save the algorithm you created. This will be handy if you are going to use it again.

To save your algorithm, you need to give it a filename and show the path to the folder you want to store it in by selecting the folder from the tree shown in the left pane.

Each custom algorithm is stored in a separate file with its own name. If you try to write a new algorithm to a pre-existing file, the existing file's contents will be erased.

If you created and saved your algorithm for data destruction while working with Acronis DriveCleanser, you can use it later in the following way:

- In the **Algorithm selection** window, choose **Load from file...** from the drop-down list and select the file with custom data destruction algorithm parameters. By default, such files have a *.alg extension.

17 Troubleshooting

17.1 General

The below sections may help you in troubleshooting issues encountered during installation and use of Acronis True Image WD Edition. Among other information the Troubleshooting chapter includes links to Acronis Support Knowledge Base (KB) articles intended for helping to solve issues with Acronis products. If the appropriate Troubleshooting section does not provide a solution to your issue, you can click any link to go to the KB and then use the Search function – just enter the key words related to your problem. Since the Troubleshooting chapter covers just the most common issues, maybe the KB has recommendations on solving your specific problem. Furthermore, Acronis Support team continuously adds new articles to the KB. When you are not able to find the solution to your problem in the KB or the suggested solution does not help, feel free to contact Acronis Customer Central.

Acronis Support personnel may request you to provide the system report. To create the report, select Generate System Report in the Help menu (if you are able to start the program in Windows), then save the report and send it to Acronis Customer Central. If the issue prevents booting to Windows, try booting from Acronis rescue media and create the report in the standalone version of Acronis True Image WD Edition, selecting the same item in the Help menu.

You can also start system report generation by simultaneously pressing the Ctrl+F7 keys both in Windows and the standalone version of Acronis True Image WD Edition, even when a wizard is opened, a task is running or an error message is displayed.

Furthermore, now you can add to your rescue media Acronis System Report tool that allows you to generate the system report after booting from the rescue media when both Windows and Acronis True Image WD Edition (full version) cannot start. In this case you will need a USB flash drive that will be used for saving the report.

Quite often the cause of an issue may be trivial, for example, a loose connection of an external hard drive. Before trying other solutions described in this chapter, it is advisable to check if the issue is caused by one of the following:

- loose connections to the external drive;
- poor quality connecting cable;

When using an external USB hard drive, try the following additional suggestions:

- if the drive is connected through a hub, connect it directly to a rear connector of your PC;
- to prevent conflict with other USB devices attached to your PC, try disconnecting all the USB devices (except the mouse and keyboard).

17.2 Installation issues

When you cannot install Acronis True Image WD Edition, try the following solutions:

1. If you selected "Install for the current user only" during the installation, try to select "Install for all users that share this computer" and vice versa.
2. Launch the installation file in the following way: right-click on the file and select "Run as administrator".
3. Log in to Vista's built-in administrator account and try to install the program:

- a. Click **Start** → **All Programs**, then find and open the "Accessories" folder.
- b. Right-click on the "Command Prompt" item and select "Run as administrator".
- c. Type the following command line in to the opened window:
net user administrator /active:yes
Take note that there is a space between "Administrator" and "/active:yes".
- d. Log off the current account and log in to the "Administrator" account.
- e. Try to install the application again.

If these solutions do not help, an AcronisSupport Knowledge base article may help you in troubleshooting and resolving the issue. Just follow the steps in the appropriate scheme. See Troubleshooting Installation Issues of Acronis Software

17.3 Backup and validation issues

1) When you get a problem with backup or validation, first of all make sure that you have the latest build of Acronis True Image WD Edition. You can download it through your Acronis account. This is because Acronis are continuously working on improving our products. The latest build may contain bug fixes and provide enhanced hardware compatibility.

2) Errors encountered while backing up data or validating backup archives may be caused by hard disk errors and/or bad sectors, so check the source and destination disks if you encounter an issue when backing up or check the backup archive storage disk when validating a backup archive. To do this, use the Windows chkdsk utility as follows:

- Go to the Command Prompt (Start → Run → cmd)

- Enter the following command: "chkdsk DISK: /r" (where DISK is the partition letter you need to check, e.g. D:). Please note, that checking the C: drive may require you to reboot the PC.

3) The reason for errors may be defective RAM modules. To test the memory modules of your PC, please download one of the archives depending on what media type you are going to use:

- memtest archive for diskette
- memtest archive for USB Flash drive
- memtest archive for CD

Unpack the archive and create bootable media with the memory test. Instructions on how to do it can be found in README.txt in the archive.

4) Check whether this section contains a solution to your problem:

The RPC server is unavailable

When a backup task is supposed to run after starting a task manually, you get an error message: Error #1722 - "The RPC server is unavailable". In such case try the solution provided in Acronis Support KB article "RPC Server is Unavailable (Error Code: 1722)" by clicking the following link: <http://kb.acronis.com/content/1521>.

Network backup issues

Instructions on how to troubleshoot issues with backing up to a network share in Windows can be found in the Acronis Support KB article "Troubleshooting Network Backup Issues in Windows" through the following link: <http://kb.acronis.com/content/1684>.

Backups to a mapped drive fail from time to time

Explanation of why saving an image to a mapped drive may sometimes fail and how to prevent this can be found in the Acronis Support KB article "Saving an Image to a Mapped Drive from an Acronis True Image Task Fails Sporadically" through the following link: <http://kb.acronis.com/content/1545>.

"Insert next volume" message when backing up to a USB flash drive

Acronis True Image WD Edition treats your USB flash drive as removable media. If it is formatted in FAT32, the size of one file is limited to 4GB, so when your backup exceeds this size the program automatically splits it into 4GB volumes and waits for insertion of the next media for the next volume. Just click OK and the backup process will continue. Repeat this if the message is displayed again until your backup finishes. For more detailed information see the Acronis Support KB article "Acronis True Image Asks to Insert Next Volume When Backing Up to USB Flash Drive" at <http://kb.acronis.com/content/1805>.

Issue with backing up an NTFS-compressed partition

Acronis True Image may fail to back up an NTFS-compressed partition due to some limitations on working with such partitions. If it is possible, decompress the partition before backing it up. For more detailed information, see the Acronis Support KB article "Acronis True Image Fails to Back Up a Compressed Partition" available at <http://kb.acronis.com/content/1811>.

Acronis True Image WD Edition states that a backup is corrupted

Instructions on how to troubleshoot and resolve issues with corrupt backups can be found in the Acronis Support KB article "Troubleshooting Issues with Corrupt Backups" available at <http://kb.acronis.com/content/1517>.

17.4 Recovery issues

System and/or data recovery after a disaster is the most important operation performed with Acronis True Image WD Edition. Indeed what's the value of a backup program that cannot recover backed up data? If you have problems with recovery, try the following actions:

- 1) First of all make sure that you have the latest build of Acronis True Image WD Edition. You can download it through your Acronis account.
- 2) If you recover the image from an external drive, try to copy that image to another storage and retry recovery as the issue may be related to the hardware.
- 3) If you have tried recovery in Windows, boot to the rescue media and try the recovery procedure once more.
- 4) If this is a data partition backup, you can try mounting it to recover at least some files and folders.
- 5) If the above suggestions have not helped to solve the problem, check whether this section gives a solution to your problem.

Network share with a backup not found by standalone Acronis True Image WD Edition

There can be several reasons why you are not able to locate the desired network share when using a standalone version of Acronis True Image. See the Acronis Support KB article "Standalone Version of Acronis True Image Cannot Find Network Share with an Image Archive".

You cannot log on to a network share after booting to rescue media

How to solve the problem when a standalone version of Acronis True Image WD Edition cannot log you on to the network where the image archive is, and keeps asking for the user name and password again and again. See the Acronis Support KB article "Standalone Version of Acronis True Image Recovery Wizard Keeps Asking for User Name and Password When Trying to Restore an Image from a Network Share".

New user profile created after recovering My mail backup of Microsoft Outlook

You can find the solution in the Acronis Support KB article "Restoring E-Mail Backup of Microsoft Outlook Creates a New Profile".

You cannot get access to recovered files or folders

After recovering files/folders with Acronis True Image you get "Access denied" message when trying to access them. To solve the issue, see the Acronis Support KB article "Access Denied to Files or Folders Restored with Acronis True Image".

17.5 Bootability after recovery issues

If a system was bootable at the time of backup, you expect that it will boot after recovery. However, the information the operating system stores and uses for booting up may have become outdated at the time of recovery, especially if you change partition sizes, locations or destination drives. Acronis True Image WD Edition automatically updates Windows loaders after recovery. Other loaders might also be fixed, but there are cases when you have to re-activate the loaders. Specifically when you recover Linux volume in a dual boot configuration, it is sometimes necessary to apply fixes or make booting changes so that Linux can boot and load correctly. Below is a summary of typical situations that require additional user actions when the recovered operating system becomes unbootable.

The machine BIOS is configured to boot from another hard disk drive (HDD).

Solution: Configure the BIOS to boot from the HDD where the operating system resides.

In some cases BIOS has two menus for setting the boot sequence: one for setting the boot devices priority and the other - for setting the HDD boot order.

Windows was recovered to a dynamic volume that cannot be set bootable

Solution: Recover Windows to a basic or simple dynamic volume.

A system partition was recovered to a disk that does not have an MBR

When you configure recovery of a system partition to a disk that does not have an MBR, the program prompts whether you want to recover the MBR along with the system partition. Opt for not recovering only if you do not want the system to be bootable.

Solution: Recover the partition once again along with the MBR of the corresponding disk.

Windows fails to boot with "NTLDR is missing" error message

Solution: Instructions on how to make Windows XP bootable if it reports "NTLDR is missing" after being recovered with Acronis True Image WD Edition, can be found in the Acronis Support KB article "Windows Fails to Boot With "NTLDR is missing" at <http://kb.acronis.com/content/1759>.

17.6 Other issues

Installation of Acronis True Image WD Edition makes shared folders inaccessible

To learn why local shared folders on the machine cannot be accessed after installation of Acronis True Image WD Edition on this computer, see the Acronis Support KB article "Shared Folders Cannot be Accessed after Installation of Acronis True Image" at <http://kb.acronis.com/content/1554>.

Acronis True Image WD Edition does not find any hard disks in Windows

If the Acronis product reports that it has not found any hard disks in Windows, the issue is probably in a third party software blocking access to the hard disks. For more details see the Acronis Support KB article "Acronis Product Does Not Detect Hard Disks in Windows" at <http://kb.acronis.com/content/1515>.

Acronis True Image WD Edition and Windows BitLocker

To back up and recover the system encrypted with BitLocker you need to create a sector-by-sector image after booting from Acronis rescue media. For more detailed information see the "Compatibility of Acronis True Image with Windows Vista BitLocker" article at <http://kb.acronis.com/content/1734>.

Disk clone operation in Windows aborted after reboot

Acronis product reboots in Windows Native Mode, but the cloning process finishes after a few seconds with no result. To handle the issue, see the Acronis Support KB article "Acronis Product Fails to Clone After Reboot" at <http://kb.acronis.com/content/1757>.

The standalone version of Acronis True Image WD Edition does not detect your hard drive(s) or NIC card.

This is because the recovery environment does not have the appropriate drivers. The issue can be solved as follows:

- Create Acronis System Report and request Acronis Customer Central to provide you with an iso file of the rescue media that contains the required drivers.
- Create a Windows-based recovery environment that includes the required drivers. See "Working with Acronis True Image Plug-In for BartPE" at <http://kb.acronis.com/content/1506>.

Partition analysis is accompanied by multiple "Failed to read from sector..." error messages

To resolve the issue, try running chkdsk and updating Acronis drivers. For more details see the following Acronis Support KB article: "Multiple "Failed to read from sector..." Error Messages During Partition Analysis" at <http://kb.acronis.com/content/1514>.

Wrong capacity of cloned hard drive

If the capacity of the cloned drive is the same as that of the original drive, when it should not be, then the issue is caused by Host Protected Area. For details see the following Acronis Support KB article: "HPA Makes the Cloned Drive Display Wrong Capacity" at <http://kb.acronis.com/content/1710>.

The "Access denied" message appears when exploring a mounted image archive

Why you may get this message while trying to explore some folders in a mounted image and solutions to this issue can be found through the following link to the Acronis Support KB article: "When Trying to Explore Certain Folders of a Mounted Image Archive, Access Denied Message Appears" at <http://kb.acronis.com/content/1549>.

You fail to mount an image spanned over several CD/DVDs

For an explanation of the issue with mounting a spanned image see "Mounting an Image Spanned over Several CD or DVD Discs Fails" at <http://kb.acronis.com/content/1546>.

It takes a long time to start Acronis True Image WD Edition

Try the following solutions to resolve this issue:

- make sure that you have the latest build of Acronis True Image WD Edition
- install the latest Acronis drivers. If you do not have them, request them from Acronis Customer Central
- disable the "Distributed Link Tracking Client" service
- add Acronis executable files to trusted applications in your antivirus software
- delete Vista restore points, if you do not need them

18 Hard Disks and Boot Sequence

18.1 Arranging boot sequence in BIOS

BIOS has a built-in setup utility for initial computer configuration. To enter it, you have to press a certain key combination (**Del**, **F1**, **Ctrl+Alt+Esc**, **Ctrl+Esc**, or some other, depending on your BIOS) during the POST (power-on self test) sequence that starts immediately after you turn your computer on. Usually the message with the required key combination is displayed during the startup test. Pressing this combination takes you to the menu of the setup utility that is included in your BIOS.

The menu can differ in appearance, sets of items and their names, depending on the BIOS manufacturer. The most widely known BIOS makers for PC motherboards are Award/Phoenix and AMI. Moreover, while items in the standard setup menu are mostly the same for various BIOSes, items of the extended (or advanced) setup heavily depend on the computer and BIOS version.

Among other things, the BIOS menu allows you to adjust the **boot sequence**. **Boot sequence** management differs for various BIOS versions, e.g. for AMI BIOS, AWARDBIOS, and brand-name hardware manufacturers.

Computer BIOS allows booting operating systems not only from hard disks, but also from CD-ROMs, DVD-ROMs, and other devices. Changing the boot sequence may be required, for example, to make your rescue media (CD, DVD or USB stick) device the first booting device.

If there are several hard disks installed in your computer labeled as C:, D:, E:, and F:, you can reorder the boot sequence so that an operating system is booted from, for example, disk E:. In this case, you have to set the boot sequence to look like E:, CD-ROM:, A:, C:, D:.

*This does not mean that booting is done from the first device in this list; it only means that the **first attempt** to boot an operating system will be from this device. There may be no operating system on disk E:, or it may be inactive. In this case, BIOS queries the next device in the list.*

The BIOS numbers disks according to the order in which they are connected to IDE controllers (primary master, primary slave, secondary master, secondary slave); next go the SCSI hard disks.

This order is broken if you change the boot sequence in BIOS setup. If, for example, you specify that booting has to be done from hard disk E:, numbering starts with the hard disk that would be the third in usual circumstances (it is usually the secondary master for IDE hard drives).

After you have installed the hard disk in your computer and have configured it in BIOS, one can say that the PC (or the motherboard) "knows" about its existence and its main parameters. However, it is still not sufficient for an operating system to work with the hard disk. In addition, you have to create partitions on the new disk and format the partitions using Acronis True Image WD Edition. See Adding a new hard disk (p. 79).

18.2 Installing hard disk drives in computers

18.2.1 Installing an IDE hard disk drive, general scheme

To install a new IDE hard disk, you should do the following (**we will assume you have powered OFF your PC before you start!**):

1. Configure the new hard disk as **slave** by properly installing jumpers on its controller board. Disk drives generally have a picture on the drive that shows the correct jumper settings.
2. Open your computer and insert the new hard disk into a 3.5" or 5.25" slot with special holders. Fasten down the disk with screws.
3. Plug the power cable into the hard disk (four-threaded: two black, yellow and red; there is only one way you can plug in this cable).
4. Plug the 40- or 80-thread flat data cable into the sockets on the hard disk and on the motherboard (plugging rules are described below). The disk drive will have a designation on the connector or next to it that identifies Pin 1. The cable will have one red wire on the end that is designated for Pin 1. Make sure that you place the cable in the connector correctly. Many cables are also "keyed" so that they can only go in one way.
5. Turn your computer on and enter BIOS setup by pressing the keys that are displayed on the screen while the computer is booting.
6. Configure the installed hard disk by setting the parameters **type, cylinder, heads, sectors** and **mode** (or **translation mode**; these parameters are written on the hard disk case) or by using the IDE autodetection BIOS utility to configure the disk automatically.
7. Set the boot sequence to A:, C:, CD-ROM or some other, depending on where your copy of Acronis True Image WD Edition is located. If you have a boot diskette, set the diskette to be the first; if it is on a CD, make the boot sequence start with the CD-ROM.
8. Quit BIOS setup and save changes. Acronis True Image WD Edition will automatically start after reboot.
9. Use Acronis True Image WD Edition to configure hard disks by answering the wizard's questions.
10. After finishing the installation, turn off the computer, set the jumper on the disk to the **master** position if you want to make the disk bootable (or leave it in **slave** position if the disk is installed as additional data storage).

18.2.2 Motherboard sockets, IDE cable, power cable

There are two slots on the motherboard to which the hard disks can be connected: **primary IDE** and **secondary IDE**.

Hard disks with an IDE (Integrated Drive Electronics) interface are connected to the motherboard via a 40- or 80-thread flat marked cable: one of the threads of the cable is red.

Two IDE hard disks can be connected to each of the sockets, i.e. there can be up to four hard disks of this type installed in the PC (there are three plugs on each IDE cable: two for hard disks and one for the motherboard socket).

As noted, IDE cable plugs are usually designed so that there is only one way to connect them to the sockets. Usually, one of the pinholes is filled on the cable plug, and one of the pins facing the filled hole is removed from the motherboard socket, so it becomes impossible to plug the cable in the wrong way.

In other cases, there is a jut on the plug on the cable, and an indentation in the sockets of the hard disk and the motherboard. This also ensures that there is only one way to connect the hard disk and the motherboard.

In the past, this design of plug did not exist, so there was an empirical rule: **the IDE cable is connected to the hard disk socket so that the marked thread is the closest to the power cable**, i.e. the marked thread connected to pin #1 of the socket. A similar rule was used for connecting cables with the motherboard.

Incorrect connection of the cable with either the hard disk or the motherboard does not necessarily damage the electronics of the disk or the motherboard. The hard disk is simply not detected or initialized by BIOS.

There are some models of hard disks, especially the older ones, for which incorrect connection damaged the electronics of the drive.

We will not describe all the types of hard disks. Currently the most widely used are those with IDE or SCSI interfaces. Unlike IDE hard disks, there can be from six to 14 SCSI hard disks installed in your PC. However, you need a special SCSI controller (called a host adapter) to connect them. SCSI hard disks are not usually used in personal computers (workstations), but are found mostly in servers.

Aside from an IDE cable, a four-thread power cable must be connected to the hard disks. There is only one way to plug in this cable.

18.2.3 Configuring hard disk drives, jumpers

A hard disk drive can be configured in a computer as **master** or as **slave**. The configuring is done using special connectors (called jumpers) on the hard disk drive.

The jumpers are either located on the electronic board of the hard disk or a special socket that provides for the connection of the hard disk and the motherboard.

There is usually a sticker on the drive that explains the markings. Typical markings are **DS**, **SP**, **CS** and **PK**.

Each jumper position corresponds to one hard disk(s) installation mode:

- **DS – master/factory default**
- **SP – slave (or no jumper required)**
- **CS – cable select for master/slave:** the purpose of the hard disk is determined by its physical position with respect to the motherboard
- **PK – jumper parking position:** the position where one can put the jumper if it is not necessary in the existing configuration

The hard disk with the jumper in **master** position is treated by the basic input/output system (BIOS) as bootable.

The jumpers on hard disks that are connected to the same cable can be in the **cable select for master/slave** position. In this case, BIOS will deem as "master", the disk that is connected to the IDE cable, which is closer to the motherboard than the other one.

Unfortunately, hard disk markings were never standardized. You might well find that markings on your hard disk differ from the ones described above. Moreover, for old types of hard disks, their purpose could be defined by two jumpers instead of one. You should study the markings carefully before installing your hard disk in the computer.

It is not enough to physically connect the hard disk to the motherboard and set the jumpers properly for the hard disk to function — hard disks have to be properly configured with the motherboard BIOS.

18.2.4 Installing a SATA hard drive

Most recently manufactured PCs use the SATA interface for hard drives. In general, installing a SATA hard drive is easier than an IDE drive, as it is not necessary to configure master-slave jumpers. SATA drives use a thin interface cable with seven-pin keyed connectors. This improves airflow through the PC case. Power is supplied to SATA drives through 15-pin connectors. Some SATA drives also support legacy four-pin power connectors (Molex) — you can use a Molex or SATA connector but do not use both at the same time, because this could damage the hard drive. You'll also need a free power lead fitted with a SATA power connector. Most systems that come with SATA ports have at least one SATA power connector. If this is not the case, you will need a Molex-to-SATA adapter. In case your system has the SATA power connector but it is already occupied, use a Y-adapter that splits a lead in two.

18.2.5 Steps for installing a new internal SATA drive

1. Find an unused SATA port using the documentation provided with your PC. If you are going to connect your new SATA drive to a SATA controller card, install the card. If you are going to connect the SATA drive to the motherboard, enable applicable motherboard jumpers, if any. Most hard drive kits include a SATA interface cable and mounting screws. Attach one end of the SATA interface cable to a SATA port on the motherboard or interface card, and the other to the drive.
2. Then plug the power-supply lead or use a Molex-to-SATA adapter.
3. Prepare your drive. If you're installing a SATA 300 hard drive, check your PC's (or SATA host adapter's) documentation to make sure it supports SATA 300 drives. If it doesn't, you might need to change a jumper setting on the drive (see the drive's manual for instructions). If you have a SATA 150 hard drive, you don't need to change any settings.
4. Turn on the PC and look for the new drive in the boot-up messages. If you don't see it, enter the PC's CMOS setup program and search the BIOS configuration menu for an option that will let you enable SATA for the ports you are using (or maybe you will just need to enable SATA). See your motherboard documentation for instructions specific to your BIOS.
5. If the operating system does not recognize the SATA drive, you need the appropriate drivers for your SATA controller. If the drive is recognized, go to step 8.

Usually, it is best to obtain the latest driver version from the motherboard or SATA controller manufacturer's Web site.

If you download a copy of the SATA controller drivers, place the driver files to a known location on your hard drive.

6. Boot from the old hard drive.
The operating system should detect the SATA controller and install the appropriate software. You might need to provide the path to the driver files.
7. Ensure that the SATA controller and the connected SATA hard drive are correctly detected by the operating system. To do this, go to the Device Manager.
SATA controllers usually appear under the SCSI and RAID controllers section of Device Manager, while hard drives are listed under the Disk drives section.
The SATA controller and SATA hard drive must not be displayed in the Device Manager with a yellow exclamation mark or any other error indication.
8. After you have installed the hard disk in your computer and have configured it in BIOS, one can say that the PC "knows" about its existence and its main parameters. However, it is still not enough for the operating system to work with the hard disk. In addition, you have to create partitions on the new disk and format the partitions using Acronis True Image WD Edition. See

Adding a new hard disk (p. 79). Then configure your BIOS to boot from the SATA controller and boot from the SATA hard drive to ensure it works.

18.3 Hard Disk Wiping methods

Information removed from a hard disk drive by non-secure means (for example, by simple Windows delete) can easily be recovered. Utilizing specialized equipment, it is possible to recover even repeatedly overwritten information. Therefore, guaranteed data wiping is more important now than ever before.

The **guaranteed wiping of information** from magnetic media (e.g. a hard disk drive) means it is impossible to recover data by even a qualified specialist with the help of all known tools and recovery methods.

This problem can be explained in the following way: Data is stored on a hard disk as a binary sequence of 1 and 0 (ones and zeros), represented by differently magnetized parts of a disk.

Generally speaking, a 1 written to a hard disk is read as 1 by its controller, and 0 is read as 0. However, if you write 1 over 0, the result is conditionally 0.95 and vice versa – if 1 is written over 1 the result is 1.05. These differences are irrelevant for the controller. However, using special equipment, one can easily read the «underlying» sequence of 1's and 0's.

It only requires specialized software and inexpensive hardware to read data "deleted" this way by analyzing magnetization of hard disk sectors, residual magnetization of track sides and/or by using current magnetic microscopes.

Writing to magnetic media leads to subtle effects summarized as follows: every track of a disk stores **an image of every record** ever written to it, but the effect of such records (magnetic layer) becomes more subtle as time passes.

18.3.1 Functioning principles of Information wiping methods

Physically, the complete wiping of information from a hard disk involves the switching of every elementary magnetic area of the recording material as many times as possible by writing specially selected sequences of logical 1's and 0's (also known as samples).

Using logical data encoding methods in current hard disks, you can select **samples** of symbol (or elementary data bit) sequences to be written to sectors in order to **repeatedly and effectively wipe confidential information**.

Methods offered by national standards provide (single or triple) recording of random symbols to disk sectors that are **straightforward and arbitrary decisions, in general**, but still acceptable in simple situations. The most effective information-wiping method is based on deep analysis of subtle features of recording data to all types of hard disks. This knowledge speaks of the necessity of complex multipass methods to **guarantee** information wiping.

The detailed theory of guaranteed information wiping is described in an article by Peter Gutmann. Please see:

Secure Deletion of Data from Magnetic and Solid-State Memory.

18.3.2 Information wiping methods used by Acronis

The table below briefly describes information wiping methods used by Acronis. Each description features the number of hard disk sector passes along with the number(s) written to each sector byte.

The description of built-in information wiping methods

No.	Algorithm (writing method)	Passes	Record
1.	United States Department of Defense 5220.22-M	4	1 st pass – randomly selected symbols to each byte of each sector, 2 – complementary to written during the 1 st pass; 3 – random symbols again; 4 – writing verification.
2.	United States: NAVSO P-5239-26 (RLL)	4	1 st pass – 0x01 to all sectors, 2 – 0x27FFFFFF, 3 – random symbol sequences, 4 – verification.
3.	United States: NAVSO P-5239-26 (MFM)	4	1 st pass – 0x01 to all sectors, 2 – 0x7FFFFFFF, 3 – random symbol sequences, 4 – verification.
4.	German: VSITR	7	1 st – 6 th – alternate sequences of: 0x00 and 0xFF; 7 th – 0xAA; i.e. 0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF, 0xAA.
5.	Russian: GOST P50739-95	1	Logical zeros (0x00 numbers) to each byte of each sector for 6 th to 4 th security level systems. Randomly selected symbols (numbers) to each byte of each sector for 3 rd to 1 st security level systems.
6.	Peter Gutmann's method	35	Peter Gutmann's method is very sophisticated. It's based on his theory of hard disk information wiping (see Secure Deletion of Data from Magnetic and Solid-State Memory).
7.	Bruce Schneier's method	7	Bruce Schneier offers a seven-pass overwriting method in his Applied Cryptography book. 1 st pass – 0xFF, 2 nd pass – 0x00, and then five times with a cryptographically secure pseudo-random sequence.
8.	Fast	1	Logical zeros (0x00 numbers) to all sectors to wipe.

19 Startup Parameters

Additional parameters that can be applied prior to booting Linux kernel.

19.1 Description

Additional parameters that can be applied prior to booting Linux kernel

Description

The following parameters can be used to load Linux kernel in a special mode:

- **acpi=off**

Disables ACPI and may help with a particular hardware configuration.

- **noapic**

Disables APIC (Advanced Programmable Interrupt Controller) and may help with a particular hardware configuration.

- **nousb**

Disables loading of USB modules.

- **nousb2**

Disables USB 2.0 support. USB 1.1 devices still work with this option. This option allows using some USB drives in USB 1.1 mode, if they do not work in USB 2.0 mode.

- **quiet**

This parameter is enabled by default and the startup messages are not displayed. Deleting it will result in the startup messages being displayed as the Linux kernel is loaded and the command shell being offered prior to running the Acronis program.

- **nodma**

Disables DMA for all IDE disk drives. Prevents kernel from freezing on some hardware.

- **nofw**

Disables FireWire (IEEE1394) support.

- **nopcmcia**

Disables PCMCIA hardware detection.

- **nomouse**

Disables mouse support.

- **[module name]=off**

Disables the module (e.g. **sata_sis=off**).

- **pci=bios**

Forces to use PCI BIOS, and not to access the hardware device directly. For instance, this parameter may be used if the machine has a non-standard PCI host bridge.

- **pci=nobios**

Disallows use of PCI BIOS; only direct hardware access methods are allowed. For instance, this parameter may be used if you experience crashes upon boot-up, probably caused by the BIOS.

- **pci=biosirq**

Uses PCI BIOS calls to get the interrupt routing table. These calls are known to be buggy on several machines and they hang the machine when used, but on other computers it is the only way to get the interrupt routing table. Try this option, if the kernel is unable to allocate IRQs or discover secondary PCI buses on your motherboard.

- **vga=ask**

Gets the list of the video modes available for your video card and allows selecting a video mode most suitable for the video card and monitor. Try this option, if the automatically selected video mode is unsuitable for your hardware.