

Acronis



Acronis True Image for BIWIN

USER GUIDE

Table of contents

1	Introduction	5
1.1	What is Acronis True Image for BIWIN?	5
1.2	System requirements and supported media	5
1.2.1	Minimum system requirements	5
1.2.2	Supported operating systems	5
1.2.3	Supported file systems	6
1.2.4	Supported storage media	6
1.3	Installing Acronis True Image for BIWIN	6
1.4	Upgrading Acronis True Image for BIWIN	7
1.4.1	Acronis True Image advanced features	7
1.5	Technical Support	9
2	Getting started	10
2.1	User interface language	10
2.2	Protecting your system	10
2.2.1	Step 1. Backing up your computer	10
2.2.2	Step 2. Creating bootable rescue media	11
2.3	Backing up all data on your PC	12
2.4	Cloning your hard drive	13
2.5	Recovering your computer	14
3	Basic concepts	16
3.1	Basic concepts	16
3.2	The difference between file backups and disk/partition images	18
3.3	Full, incremental and differential backups	18
3.4	FAQ about backup, recovery and cloning	19
3.5	FTP connection	20
3.6	Authentication settings	20
3.7	Backup file naming	21
3.8	Wizards	21
4	Backing up data	23
4.1	Backing up disks and partitions	23
4.2	Backup options	24
4.2.1	Backup schemes	24
4.2.2	Notifications for backup operation	27
4.2.3	Image creation mode	27
4.2.4	Pre/Post commands for backup	28
4.2.5	Backup splitting	28
4.2.6	Backup validation option	29
4.2.7	Backup reserve copy	29
4.2.8	Removable media settings	30
4.2.9	Backup comment	30
4.2.10	Error handling	30
4.2.11	Computer shutdown	31

4.2.12	Performance of backup operation.....	31
4.3	Operations with backups	33
4.3.1	Backup operations menu.....	33
4.3.2	Validating backups	34
4.3.3	Backing up to various places	34
4.3.4	Adding an existing backup to the list.....	35
4.3.5	Deleting backups and backup versions.....	35
5	Recovering data	36
5.1	Recovering disks and partitions.....	36
5.1.1	Recovering your system after a crash.....	36
5.1.2	Recovering partitions and disks	44
5.1.3	About recovery of dynamic/GPT disks and volumes.....	45
5.1.4	Arranging boot order in BIOS	47
5.1.5	Recovering files and folders	48
5.1.6	Searching backup content	49
5.2	Recovery options	49
5.2.1	Disk recovery mode	50
5.2.2	Pre/Post commands for recovery	50
5.2.3	Validation option.....	50
5.2.4	Computer restart.....	51
5.2.5	File recovery options.....	51
5.2.6	Overwrite file options	51
5.2.7	Performance of recovery operation	51
5.2.8	Notifications for recovery operation	52
6	Antivirus and antimalware protection	54
6.1	Active protection	54
6.1.1	Configuring Active Protection	55
6.2	Managing files in Quarantine	56
6.3	Configuring Protection exclusions	56
7	Disk cloning and migration	57
7.1	General information	57
7.1.1	Clone Disk wizard	57
7.1.2	Manual partitioning	59
7.1.3	Excluding items from cloning	60
7.2	Preparing for migration	61
7.2.1	What to do if Acronis True Image for BIWIN does not recognize your SSD	62
7.2.2	Migrating to SSD using the backup and recovery method.....	63
8	Tools	64
8.1	Creating bootable rescue media.....	64
8.1.1	Acronis Media Builder.....	64
8.1.2	Making sure that your rescue media can be used when needed	67
8.2	Security and Privacy Tools	70
8.2.1	Acronis DriveCleanser	71
8.2.2	Hard Disk Wiping methods.....	74
8.3	Adding a new hard disk.....	75
8.3.1	Selecting a hard disk.....	76
8.3.2	Selecting initialization method	77
8.3.3	Creating new partitions	77

8.4	Mounting an image.....	79
8.5	Unmounting an image	80
9	Troubleshooting	81
9.1	Acronis System Report.....	81
9.2	How to collect crash dumps	82
10	Glossary of Terms	84

1 Introduction

1.1 What is Acronis True Image for BIWIN?

Acronis True Image for BIWIN is an integrated software suite that ensures the security of all of the information on your PC. Backups allow you to recover your computer system should a disaster occur, such as losing data, accidentally deleting critical files or folders, or suffering a complete hard disk crash.

Key features:

- Rescue bootable media (p. 64)
- Hard disk cloning (p. 57)
- Security and privacy tools (p. 64)

Getting started

Learn how to protect your computer with two simple steps: "Protecting your system (p. 10)".

1.2 System requirements and supported media

1.2.1 Minimum system requirements

Acronis True Image for BIWIN requires the following hardware:

- BIWIN device.
- Intel CORE 2 Duo (2GHz) processor or equivalent
The CPU must support SSE instructions.
- 2 GB RAM
- 7 GB of free space on the system hard disk
- CD-RW/DVD-RW drive or USB drive for bootable media creation
 - Required free space for Linux is about 660 MB.
 - Required free space for Windows is about 700 MB.
- Screen resolution is 1024 x 768
- Mouse or other pointing device (recommended)

1.2.2 Supported operating systems

Acronis True Image for BIWIN has been tested on the following operating systems:

- Windows XP SP3
- Windows 7 SP1 (all editions)
- Windows 8 (all editions)
- Windows 8.1 (all editions)
- Windows 10 (all editions, including the October 2020 Update)
- Windows Home Server 2011

Note

- *Beta builds are not supported.*
 - *Windows Embedded, IoT editions, Windows 10 LTSC, and Windows 10 LTSC are not supported*
-

Acronis True Image for BIWIN also lets you create a bootable CD-R/DVD-R or USB drive that can back up and recover a disk/partition on a computer running any Intel- or AMD- based PC operating system, including Linux®. Note that the Intel-based Apple Macintosh is not supported.

1.2.3 Supported file systems

- NTFS
- Ext2/Ext3/Ext4
- ReiserFS(3) *
- Linux SWAP *
- HFS+**/HFSX**
- FAT16/32/exFAT**

* File systems are supported only for disk or partition backup/recovery operations.

** Disk recovery, partition recovery, and cloning operations are supported without resizing.

1.2.4 Supported storage media

- Hard disk drives*
- Solid State Drives (SSD)
- Networked storage devices
- FTP servers**
- CD-R/RW, DVD-R/RW, DVD+R (including double-layer DVD+R), DVD+RW, DVD-RAM, BD-R, BD-RE
- USB 1.1 / 2.0 / 3.0, USB-C, eSATA, FireWire (IEEE-1394), SCSI, and PC card storage devices

* Limitations on operations with dynamic and GPT disks:

- Creation of Acronis Secure Zone on dynamic disks is not supported.
- Recovery of a dynamic volume as a dynamic volume with manual resizing is not supported.
- Try&Decide® cannot be used for protecting dynamic disks.
- "Clone disk" operation is not supported for dynamic disks.

** An FTP server must allow passive mode file transfers. Acronis True Image for BIWIN splits a backup into files with a size of 2GB when backing up directly to an FTP server.

The firewall settings of the source computer should have Ports 20 and 21 opened for the TCP and UDP protocols to function. The **Routing and Remote Access** Windows service should be disabled.

1.3 Installing Acronis True Image for BIWIN

Installing Acronis True Image for BIWIN

To install Acronis True Image for BIWIN:

1. Run the setup file.
2. Read the terms of the license agreement.
3. If you accept the terms of the document, click **Install**.

Acronis True Image for BIWIN will be installed on your system partition (usually C:).

4. When the installation is complete, click **Start application**.

Recovering from an Acronis True Image for BIWIN error

If Acronis True Image for BIWIN ceased running or produced errors, its files might be corrupted. To repair this problem, you first have to recover the program. To do this, run Acronis True Image for BIWIN installer again. It will detect Acronis True Image for BIWIN on your computer and will ask you if you want to repair or remove it.

Removing Acronis True Image for BIWIN

To remove Acronis True Image for BIWIN components:

1. Open the list of installed programs and applications.
 - Select **Start -> Settings -> Control panel -> Add or remove programs**.
 - If you use Windows Vista, select **Start -> Control panel -> Programs and Features**.
 - If you use Windows 7, select **Start -> Control Panel -> Uninstall a program**.
 - If you use Windows 8 or Windows 10, click the Settings icon, then select **Control Panel -> Uninstall a program**.
2. Select the component to be removed.
3. Depending on your operating system, click **Remove** or **Uninstall**.
4. Follow the instructions on the screen.

You may have to reboot your computer afterwards to complete the task.

1.4 Upgrading Acronis True Image for BIWIN

To purchase Acronis True Image or Acronis True Image Cloud:

1. Start Acronis True Image for BIWIN.
2. On the sidebar, click **Account**, and then click **Upgrade**. The built-in store opens.
3. Select the license that you want to buy, and then click **Buy now**.
4. Provide your payment information.

Built-in store

Acronis True Image for BIWIN provides an in-app store.

To access the in-app store, go to the **Account** tab, and then click **Upgrade**. You will see the in-app store and all available purchase options.

1.4.1 Acronis True Image advanced features

Advanced features of Acronis True Image are unavailable in your product edition. You can get these features by upgrading your edition to Acronis True Image. After upgrade, the following features will be available for you:

- **Online Backup**
Online Backup allows you to store your files and disks on Acronis Cloud. Your data will be protected even if your computer is lost, stolen, or destroyed, and your data can be entirely recovered onto a new device, if needed.
- **File backup**

Instead of backing up entire partitions and disks, you can back up specific files and folders, both to a local storage and Acronis Cloud.

- **Cloud archiving**

Data archiving is a tool that allows you to move your big or rarely used files to Acronis Cloud. Every time you run this tool, it analyzes the data in the selected folder and suggests uploading the found files to Acronis Cloud. You can select the files and folders that you want to archive. After uploading, the local copies of these files will be deleted. Afterwards, when you need to open or change an archived file, you can download it back to your local storage device or access and manage it right in Acronis Cloud.

- **Local archiving**

When you archive your old, large, or rarely used files, Acronis Cloud is not the only possible destination. You can also select local storage, including NAS, an external hard drive, or a USB flash drive. Your local archives are placed into Acronis Archive, which can be accessed in File Explorer under Favorites, along with your cloud archive.

- **Family data protection**

Family data protection is a unified cross-platform solution that allows you to track and control the protection status of all computers, smartphones, and tablets sharing the same Acronis account. Since users of these devices must be signed in to the same account, usually they are members of the same family. In general, each of them can use this feature, but there is often a family member who is more experienced in technology than the others. So, it's reasonable to make that person responsible for protection of the family data. To track and control the protection status of your family's devices, use the web-based Online Dashboard, which is accessible from any computer connected to the Internet.

- **Data synchronization**

You can have the same data - documents, photos, videos, etc. - on all of your computers. Your data is within easy reach anywhere and anytime. No more emailing files to yourself or carrying an USB drive all the time.

You can create as many syncs as you need and store your synced files and versions of those files on Acronis Cloud. This lets you roll back to a previous file version whenever you need it. You can also access the Cloud using a web browser, without having to install the application.

- **Acronis Survival Kit**

To recover your computer in case of a failure, you need to have two crucial components—a backup of your system disk and a bootable rescue media. Acronis Survival Kit is an external hard disk drive that contains both components so that you could have a single device that has everything that you need to recover your computer.

- **Acronis Universal Restore**

Acronis Universal Restore allows you to create a bootable system clone on different hardware. Use this utility when recovering your system disk to a computer with a dissimilar processor, different motherboard or a different mass storage device than in the system you originally backed up. This may be useful, for example, after replacing a failed motherboard or when deciding to migrate the system from one computer to another.

- **Acronis True Image for mobile devices**

Acronis True Image for mobile devices allows you to back up your mobile data to Acronis Cloud or local storage, and then recover it in case of loss or corruption. You can install Acronis True Image on any mobile devices that runs either iOS (iPhone, iPad, iPod) or the Android (mobile phones and tablets) operating systems.

- **Try&Decide**

When you turn Try&Decide on, your computer is in the Try mode. After that you can perform any potentially dangerous operations without worrying that you might damage your operating system, programs or data. When you turn Try&Decide off, you decide if you want to apply the changes to your computer or you want to discard them.

- **Acronis Secure Zone**

The Acronis Secure Zone is a special secure partition that you can create on your computer for storing backups.

- **System Clean-up**

The System Clean-up wizard enables you to securely remove all traces of your PC actions, including user names, passwords, and other personal information.

See the full feature list at <http://acronis.com/promotion/biwin>.

1.5 Technical Support

Customer support for Acronis True Image for BIWIN users is provided by BIWIN at <https://biwintech.com/>.

2 Getting started

In this section

User interface language	10
Protecting your system	10
Backing up all data on your PC.....	12
Cloning your hard drive.....	13
Recovering your computer	14

2.1 User interface language

Acronis True Image for BIWIN is available in two localizations: English and Chinese. By default, the language is set in accordance with your Windows display language.

To change the user interface language:

1. Start Acronis True Image for BIWIN.
2. In the **Settings** section, select a preferred language from the list.

2.2 Protecting your system

To protect your system:

1. Back up your computer (p. 10).
2. Create bootable media (p. 11).

It is recommended to test the rescue media as described in Making sure that your rescue media can be used when needed.

2.2.1 Step 1. Backing up your computer

When should I back up my computer?

Create a new backup version after every significant event in your system.

Examples of these events include:

- You bought a new computer.
- You reinstalled Windows on your computer.
- You configured all system settings (for example, time, date, language) and installed all necessary programs on your new computer.
- Important system update.

To ensure you save a healthy state of a disk, it is a good idea to scan it for viruses before backing it up. Please use antivirus software for this purpose. Note this operation often takes a significant amount of time.

How do I create a backup of my computer?

You have two options to protect your system:

- **Entire PC backup (recommended)**

Acronis True Image backs up all your internal hard drives in disk mode. The backup contains the operating system, installed programs, system settings, and all your personal data including your photos, music, and documents. Refer to *Backing up all data on your PC* (p. 12) for details.

- **System disk backup**

You can choose to back up your system partition or the entire system drive. Refer to *Backing up disks and partitions* (p. 23) for details.

To back up your computer:

1. Start Acronis True Image for BIWIN.
2. On the sidebar, click **Backup**.

If this is your first backup, you will see the backup configuration screen. If you already have some backups in the backup list, then first click **Add backup**, and then click **Create new backup**.

3. Click the **Backup source** icon, and then select **Entire PC**.

If you want to back up your system disk only, then click **Disks and partitions**, and then select your system partition (usually C:) and the System Reserved partition (if any).

4. Click the **Backup destination** icon, and then select a storage place for the backup (see recommendation below).
5. Click **Back up now**.

Result: A new backup box appears in the **My backups** list. To create a new version of the backup in future, select the backup box from the list, and then click **Back up now**.

2.2.2 Step 2. Creating bootable rescue media

What is bootable media?

Bootable media is a product, such as a CD-R/RW or a USB flash drive, from which you can run Acronis True Image when Windows cannot start. You can make a media bootable by using Acronis Media Builder.

How do I create bootable media?

1. Insert a CD-R/RW or plug in a USB flash drive.
2. Start Acronis True Image for BIWIN.
3. On the sidebar, click **Tools**, and then click **Rescue Media Builder**.
4. On the first step, select **Acronis bootable rescue media**.
5. Select the device to use to create the bootable media.
6. Click **Proceed**.

How do I use bootable media?

Use bootable media to recover your computer when Windows cannot start.

1. Connect the bootable media to your computer (insert the CD or plug in the USB drive).
2. Arrange the boot order in BIOS so that your rescue media device (CD or USB drive) is the first device to be booted.

Refer to *Arranging boot order in BIOS* (p. 47) for details.

3. Boot your computer from the rescue media and select **Acronis True Image for BIWIN**.

Result: Once Acronis True Image is loaded, you can use it to recover your computer.

Refer to *Acronis Media Builder* (p. 64) for details.

2.3 Backing up all data on your PC

What is an Entire PC backup?

An Entire PC backup is the easiest way to back up the full contents of your computer. We recommend that you choose this option when you are not sure which data that you need to protect. If you want to back up your system partition only, refer to Backing up disks and partitions (p. 23) for details.

When you select Entire PC as a backup type, Acronis True Image backs up all your internal hard drives in disk mode. The backup contains the operating system, installed programs, system settings, and all your personal data including your photos, music, and documents.

The recovery from an Entire PC backup is also simplified. You only need to choose the date to which you want to revert your data. Acronis True Image recovers all data from the backup to the original location. Note that you cannot select specific disks or partitions to recover and you cannot change the default destination. If you need to avoid these limitations, we recommend that you back up your data with an ordinary disk-level backup method. Refer to Backing up disks and partitions (p. 23) for details.

If an Entire PC backup contains dynamic disks, you recover your data in partition mode. This means that you can select partitions to recover and change recovery destination. Refer to About recovery of dynamic/GPT disks and volumes (p. 45) for details.

How do I create an Entire PC backup?

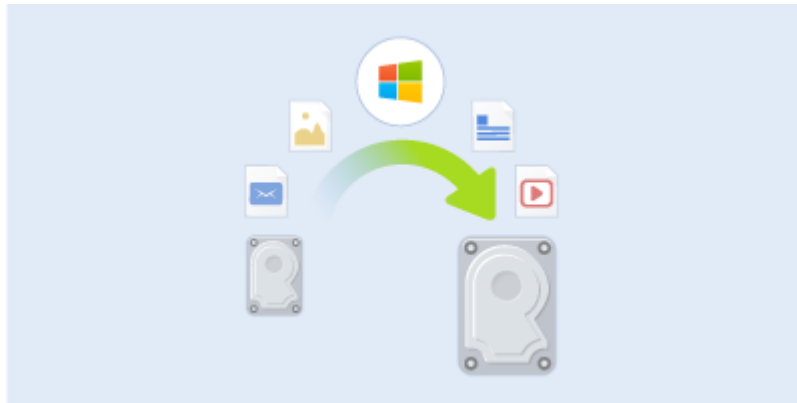
To back up the entire contents of your computer:

1. Start Acronis True Image for BIWIN.
2. On the sidebar, click **Backup**.
3. Click **Add backup**, and then click **Create new backup**.
4. Click the **Backup source** icon, and then select **Entire PC**.
5. Click the **Backup destination** icon, and then select a destination for the backup.
6. [optional step] Click **Options** to set the options for the backup, including Schedule, Scheme (p. 24), and Password protection. For more information see Backup options (p. 24).
7. Click **Back up now**.

2.4 Cloning your hard drive

Why do I need it?

When you see that the free space on your hard drive is not enough for your data, you might want to buy a new, larger hard drive and transfer all your data to the new drive. The usual copy operation does not make your new hard drive identical to the old one. For example, if you open Windows Explorer and copy all files and folders to the new hard drive, Windows will not start from the new hard drive. The Clone disk utility allows you to duplicate all your data and make Windows bootable on your new hard drive.



Before you start

We recommend that you install the target (new) drive where you plan to use it and the source drive in another location, for example, in an external USB enclosure. This is especially important for laptops.

Warning! Your old and new hard drives must work in the same controller mode (for example, IDE or AHCI). Otherwise, your computer will not start from the new hard drive.

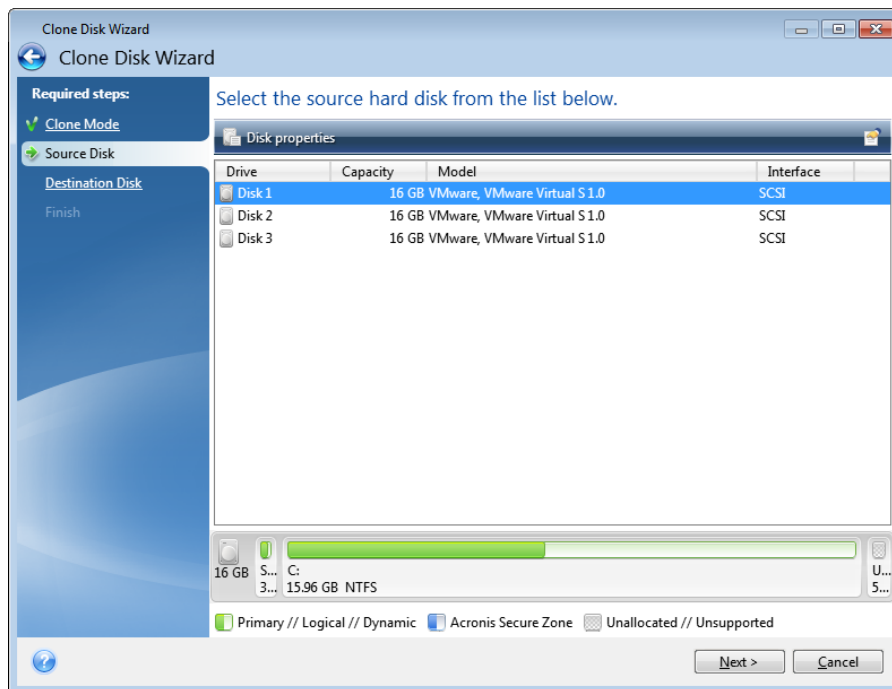
Using the Clone disk utility

To clone a disk:

1. On the sidebar, click **Tools**, and then click **Clone disk**.
2. On the **Clone Mode** step, we recommend that you choose the **Automatic** transfer mode. In this case, the partitions will be proportionally resized to fit your new hard drive. The **Manual** mode provides more flexibility. Refer to Clone Disk wizard (p. 57) for more details about the manual mode.

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 this case, the next steps will be bypassed and you will be taken to the cloning Summary screen.

3. On the **Source Disk** step, select the disk that you want to clone.



4. On the **Destination Disk** step, select the destination disk for the cloned data.

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

5. On the **Finish** step, ensure that the configured settings suit your needs, and then click **Proceed**.

By default, Acronis True Image for BIWIN shuts down the computer after the clone process finishes. This enables you to change the position of master/subordinate jumpers and remove one of the hard drives.

2.5 Recovering your computer

Please be aware that recovery of a system disk is an important operation. Before you start, we recommend that you read the detailed descriptions in the following Help topics:

- Trying to determine the crash cause (p. 36)
- Preparing for recovery (p. 36)
- Recovering your system to the same disk (p. 37)

Let's consider two different cases:

1. Windows works incorrectly, but you can start Acronis True Image for BIWIN.
2. Windows cannot start (for example, you turn on your computer and see something unusual on your screen).

Case 1. How to recover computer if Windows works incorrectly?

1. Start Acronis True Image for BIWIN.
2. On the sidebar, click **Backup**.
3. From the backup list, select the backup that contains your system disk.
4. Depending on the backup type, click **Recover PC** or **Recover disks**.
5. In the opened window, select the backup version (the data state from a specific date and time).

6. Select the system partition and the System Reserved partition (if any) to be recovered.
7. Click **Recover now**.

To complete the operation, Acronis True Image for BIWIN must restart your system.

Case 2. How to recover computer if Windows cannot start?

1. Connect Acronis bootable media to your computer, and then run the special standalone version of Acronis True Image for BIWIN.

Refer to Step 2 Creating bootable rescue media (p. 11) and Arranging boot order in BIOS (p. 47) for details.

2. On the Welcome screen, select **My disks** below **Recover**.
3. Select the system disk backup to be used for recovery. Right-click the backup and choose **Recover**.

When the backup is not displayed, click **Browse** and manually specify the path to the backup.

4. At the **Recovery method** step, select **Recover whole disks and partitions**.
5. Select the system partition (usually C) on the **What to recover** screen. Note that you may distinguish the system partition by the Pri, Act flags. Select the System Reserved partition (if any), as well.
6. You may leave all settings of the partitions without changes and click **Finish**.
7. Check the summary of operations, and then click **Proceed**.
8. When the operation finishes, exit the standalone version of Acronis True Image for BIWIN, remove the rescue media (if any), and boot from the recovered system partition. After making sure that you have recovered Windows to the state you need, restore the original boot order.

3 Basic concepts

In this section

Basic concepts.....	16
The difference between file backups and disk/partition images	18
Full, incremental and differential backups	18
FAQ about backup, recovery and cloning	19
FTP connection.....	20
Authentication settings.....	20
Backup file naming.....	21
Wizards.....	21

3.1 Basic concepts

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

Note: Certain features and functionalities may be unavailable in the True Image edition that you use.

Backup and recovery

Backup refers to the making copies of data so that these additional copies may be used to **recover** 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 recover small numbers of files after they have been accidentally deleted or corrupted.

Acronis True Image for BIWIN does both by creating disk (or partition) images and file-level backups respectively.

Backup versions

Backup versions are the file or files created during each backup operation. If you do not use consolidation feature, the amount of versions created is always equal to the amount of times the backup is executed or to the amount of stored points in time.

So, a version represents a point in time to which the system or data can be restored. To put it another way, backup versions represent full and incremental backups - see Full and incremental backups (p. 18).

The backup versions are similar to file versions. The file versions concept is familiar to those who use a Windows Vista and Windows 7 feature called "Previous versions of files". This feature allows you to restore a file as it existed on a particular date and time. A backup version allows you to recover your data in a similar way.

This could be useful when trying to find damaged or deleted files. Simply browse through the backup versions in the Acronis Backup Explorer until you find the backup version containing the required files. Additionally, you can recover different saved versions of the found files.

Disk cloning

This operation migrates or copies the entire contents of one disk drive to another disk drive. This may be necessary, for example, when installing a larger capacity disk. The result is 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.

Acronis True Image for BIWIN does not provide for cloning a single partition. You can only clone the entire drive.

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 validation

The backup validation feature allows you to confirm that your data can be recovered. As mentioned above, the program adds checksum values to the data blocks being backed up. During backup validation, Acronis True Image for BIWIN opens the backup file, recalculates 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.

Consolidation

Consolidation allows you to delete backups which you no longer need from a backup chain.

A chain to be consolidated can consist of a full backup and one or more incremental backups.

If necessary, you can delete the base full backup from the chain. The program will create a new full backup in place of the oldest remaining backup. Consolidation keeps whichever backups you choose and deletes any backups that are not selected.

Because consolidation may require significant time and system resources (including disk space), we recommend using it sparingly. In many cases, starting a new backup chain and then deleting the old one will be a better choice.

Disaster recovery

Recovering from a disaster usually requires a rescue media and a backup of the system partition.

Acronis True Image for BIWIN provides for recovery from a disaster caused by system data corruption, viruses, malware, or other causes.

If the operating system fails to boot, Acronis True Image for BIWIN will recover the system partition. You can create a rescue media by using the Media Builder tool.

Scheduling

For your backups to be really helpful, they must be as "up-to-date" as possible. This means that you should run backups on a regular basis. Although creating an Acronis True Image for BIWIN backup is quite easy, on occasion, you may forget to do a backup.

With the scheduler, you do not have to remember. You can schedule automatic backups ahead of time. Your data will be backed up as long as there is sufficient storage space.

Understanding these terms and concepts will be helpful when using the program's features.

3.2 The difference between file backups and disk/partition images

When you back up files and folders, only the files and folder tree are compressed and stored.

Disk/partition backups are different from file and folder backups. Acronis True Image stores an exact snapshot of the disk or partition. This procedure is called "creating a disk image", or "creating a disk backup" and the resulting backup is often called "a disk/partition image" or "a disk/partition backup".

A disk/partition backup contains all the data stored on the disk or partition:

1. Zero track of the hard disk with the master boot record (MBR) (applicable to MBR disk backups only).
2. One or more partitions, including:
 1. Boot code.
 2. File system meta data, including service files, file allocation table (FAT) and partition boot record.
 3. File system data, including operating system (system files, registry, drivers), user data and software applications.
3. System Reserved partition, if any.
4. EFI system partition, if any (applicable to GPT disk backups only).

By default Acronis True Image stores only the hard disk sectors that contain data. Furthermore, Acronis True Image does not back up 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.

You can change this default method by turning on the sector-by-sector mode. In this case Acronis True Image copies all hard disk sectors, and not only those that contain data.

3.3 Full, incremental and differential backups

Note: *Incremental and differential backups are not available in this product edition.*

In general, True Image offers three backup methods:

- 1) **Full:** contains all of the data at the moment of the backup creation. It forms a base for further incremental or differential backups. It can also be used as a standalone backup.
- 2) **Incremental:** Only those files will be included which have been changed since the LAST backup.
- 3) **Differential:** Only those files will be included which have been changed since the last FULL backup.

Acronis True Image for BIWIN, however, supports only the full method:

"Full" - 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.

To choose a desired backup method, you usually need to configure a custom backup scheme. For more information see Custom schemes (p. 25).

3.4 FAQ about backup, recovery and cloning

- **I have a 150GB system partition, but the occupied space on that partition is only 80GB. What will Acronis True Image for BIWIN include in a backup?** - By default, Acronis True Image copies only the hard disk sectors that contain data, so it will include only 80GB in a backup. You can also choose the sector-by-sector mode. Note that such a backup mode is required only in special cases. For more information see Image creation mode (p. 27). While creating a sector-by-sector backup, the program copies both used and unused hard disk sectors and the backup file will usually be significantly larger.
- **Will my system disk backup include drivers, documents, pictures, etc.?** - Yes, such a backup will contain the drivers, as well as the contents of the My documents folder and its subfolders, if you kept the default location of the My documents folder. If you have just a single hard disk in your PC, such a backup will contain all of the operating system, applications and data.
- **I have an old hard disk drive which is almost full in my notebook. I purchased a new bigger HDD. How can I transfer Windows, programs and data to the new disk?** - You can either clone the old hard disk on the new one or back up the old hard disk and then recover the backup to a new one. The optimum method usually depends on your old hard disk partitions layout.
- **I want to migrate my old system hard disk to an SSD. Can this be done with Acronis True Image?** - Yes, Acronis True Image for BIWIN provides such a function. For procedure details, see Migrating your system from an HDD to an SSD (p. 61)
- **What is the best way to migrate the system to a new disk: cloning or backup and recovery?** - The backup and recovery method provides more flexibility. In any case, we strongly recommend to make a backup of your old hard disk even if you decide to use cloning. It could be your data saver if something goes wrong with your original hard disk during cloning. For example, there were cases when users chose the wrong disk as the target and thus wiped their system disk. In addition, you can make more than one backup to create redundancy and increase security.
- **What should I back up: a partition or the whole disk?** - In most cases, it is better to back up the whole disk. However, there may be some cases when a partition backup is advisable. For example, your notebook has a single hard disk with two partitions: system (disk letter C) and the data (disk letter D). The system partition stores your working documents in the My documents folder with subfolders. The data partition stores your videos, pictures, and music files. Such files are already compressed and backing them up using Acronis True Image would not give you significant reduction of the backup file size. In this case, it may be better to use a local sync for the data partition files and a separate backup for the system partition. However, we also recommend creating at least one whole disk backup if your backup storage has enough space.
- **Could you tell me how to clone: in Windows or after booting from the rescue media?** Even when you start cloning in Windows, the computer will reboot into the Linux environment the same as when booting from the rescue media. Because of this, it is better to clone under rescue media. For example, there may be a case when your hard disk drives are detected in Windows and not detected in Linux. If this is the case, the cloning operation will fail after reboot. When booting from the rescue media, you can make sure that Acronis True Image detects both the source and target disks before starting the cloning operation.
- **Can I clone or back up and recover a dual boot machine?** Yes, this is possible in most cases. If your systems are installed in separate partitions of the same physical hard disk drive, cloning or recovery usually proceeds without any problems. If the systems are on different physical hard disk drives, there may be some problems with bootability after recovery.
- **Does Acronis True Image support RAID?** - Acronis True Image supports hardware RAID arrays of all popular types. Support of software RAID configurations on dynamic disks is also provided. Acronis Bootable Rescue Media supports most of the popular hardware RAID controllers. If the

standard Acronis rescue media does not "see" the RAID as a single volume, the media does not have the appropriate drivers.

3.5 FTP connection

Acronis True Image for BIWIN allows you to store your backups on FTP servers.

To create a new FTP connection, when selecting a backup storage click **FTP connection**, and in the opened window provide:

- Path to the FTP server, for example: *my.server.com*
- Port
- User name
- Password

To check your settings, click the **Test connection** button. The computer will try to connect to the specified FTP server. If the test connection has been established, click the **Connect** button to add the FTP connection.

The created FTP connection will appear in the folder tree. Select the connection and browse for the backup storage that you want to use.

Please, be aware that the mere opening of an FTP server's root folder does not bring you to your home directory.

For data to be recovered directly from an FTP server, the backup must consist of files no greater than 2GB each.

Because of this, Acronis True Image for BIWIN splits a backup into files with a size of 2GB when backing up directly to an FTP server. If you back up to a hard disk with the aim of transferring the backup to an FTP later, you may split the backup into files of 2GB each by setting the desired file size in the backup options.

An FTP server must allow passive mode file transfers.

*The firewall settings of the source computer should have Ports 20 and 21 opened for the TPC and UDP protocols to function. The **Routing and Remote Access** Windows service should be disabled.*

3.6 Authentication settings

If you are connecting to a networked computer, in most cases you will need to provide the necessary credentials for accessing the network share. For example, this is possible when you select a backup storage. The **Authentication Settings** window appears automatically when you select a networked computer name.

If necessary, specify the user name and password, and then click **Test connection**. When the test is successfully passed, click **Connect**.

Troubleshooting

When you create a network share that you plan to use as a backup storage, please ensure that at least one of the following conditions is met:

- Windows account has a password on the computer where the shared folder is located.
- Password-protected sharing is turned off in Windows.

For example, in Windows 7, you can find this setting at **Control Panel** —> **Network and Internet** —> **Network and Sharing Center** —> **Advanced sharing settings** —> Turn off password protected sharing.

Otherwise, you will not be able to connect to the shared folder.

3.7 Backup file naming

A backup file name has the following attributes:

- Backup name.
- Backup method (full, inc, diff: full, incremental, differential).
- Number of backup chain (in the form of b#).
- Number of backup version (in the form of s#).
- Number of volume (in the form of v#).

For example this attribute changes when you split a backup into several files. Refer to Backup splitting (p. 28) for details.

Thus a backup name may look the following way:

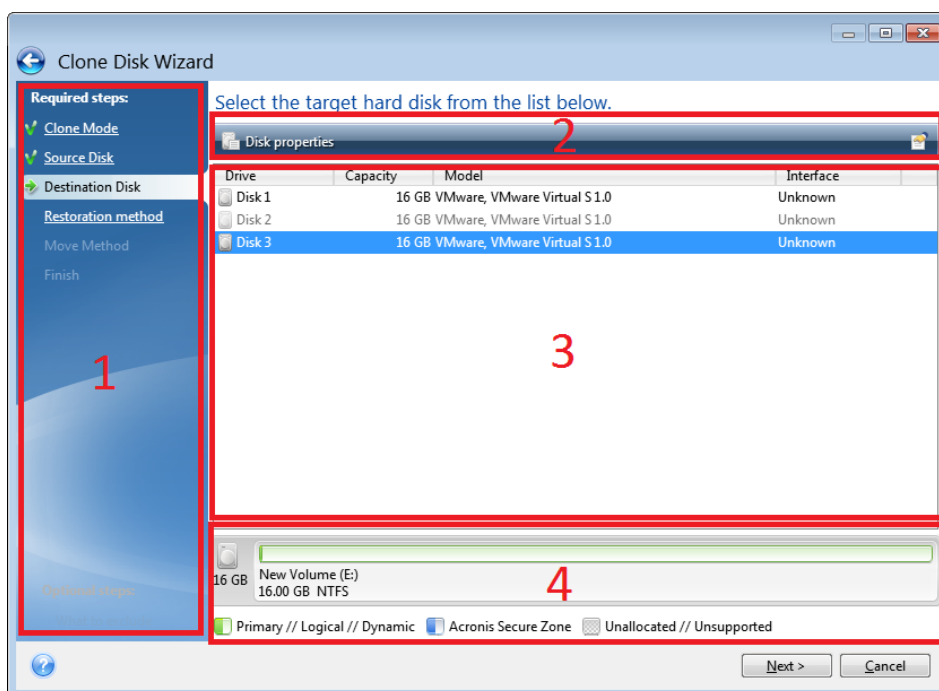
1. **my_documents_full_b1_s1_v1.tib**
2. **my_documents_full_b2_s1_v1.tib**
3. **my_documents_inc_b2_s2_v1.tib**
4. **my_documents_inc_b2_s3_v1.tib**

If you are creating a new backup, and there is already a file with the same name, the program does not delete the old file, but adds to the new file the "-number" suffix, for example, **my_documents_inc_b2_s2_v1-2.tib**.





3.8 Wizards

When you use the available Acronis True Image tools and utilities, the program will in many cases employ wizards to guide you through the operations.

For example, see the screen shot below.



A wizard window usually consists of the following areas:

1. This is the list of steps to complete the operation. A green checkmark appears next to a complete step. The green arrow indicates the current step. When complete all the steps, the program displays the Summary screen in the **Finish** step. Check the summary and click **Proceed** to start the operation.
2. This toolbar contains buttons to manage objects you select in area 3.
For example:
 -  **Details** - displays the window that provides detailed information about the selected backup.
 -  **Properties** - displays the selected item properties window.
 -  **Create new partition** - displays the window where you can configure a new partition settings.
 -  **Columns** - allows you to choose which table columns to display and in which order.
3. This is the main area where you select items and change settings.
4. This area displays additional information about the item you select in area 3.

4 Backing up data

Acronis True Image for BIWIN includes a wealth of sophisticated backup capabilities that would please even an IT professional. They allow you to back up your disks and partitions. You can choose a backup feature that suits you most or use them all. The sections below describe the backup features in more detail.

In this section

Backing up disks and partitions.....	23
Backup options.....	24
Operations with backups	33

4.1 Backing up disks and partitions

As opposed to file backups, disk and partition backups contain all the data stored on the disk or partition. This backup type is usually used to create an exact copy of a system partition of the whole system disk. Such backup allows you to recover your computer when Windows works incorrectly or cannot start.

To back up partitions or disks:

1. Start Acronis True Image.
2. On the sidebar, click **Backup**.
3. Click **Add backup**, and then click **Create new backup**.
4. [Optional] To rename the backup, click the arrow next to the backup name, click **Rename**, and then enter a new name.
5. Click the **Backup source** icon, and then select **Disks and partitions**.
6. In the opened window, select the check boxes next to the partitions and disks that you want to back up, and then click **OK**.

To view hidden partitions, click **Full partition list**.

To back up dynamic disks you can use only the partition mode.

7. Click the **Backup destination** icon, and then select a destination for backup:
 - **Your external drive**—When an external drive is plugged into your computer, you can select it from the list.
 - **NAS**—Select an NAS from the list of found NAS devices.
 - **Browse**—Select a destination from the folder tree.

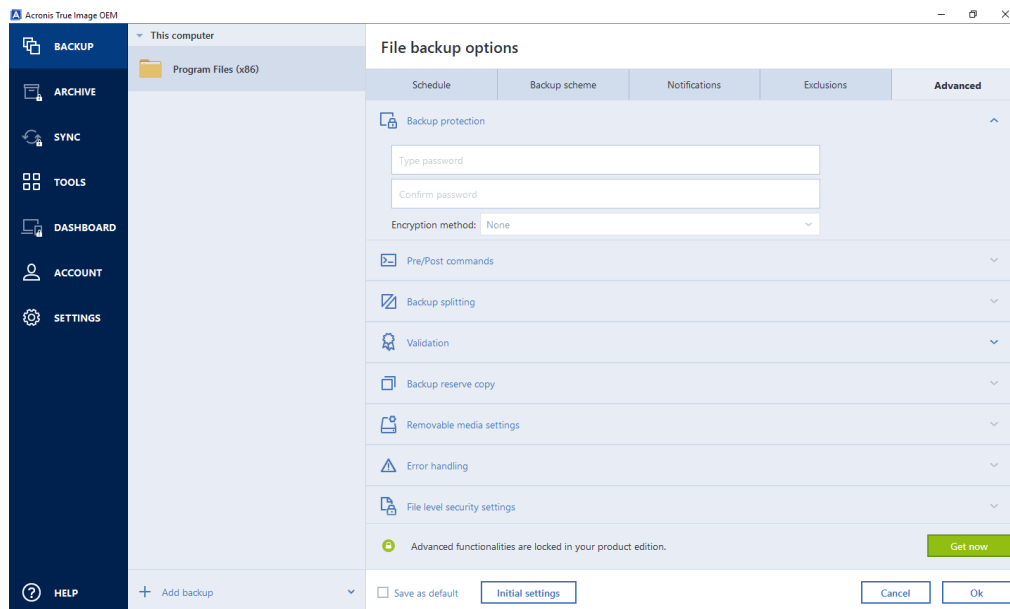
If possible, avoid storing your system partition backups on dynamic disks, because the system partition is recovered in the Linux environment. Linux and Windows work with dynamic disks differently. This may result in problems during recovery.

8. [optional step] Click **Options** to set the options for the backup, including Schedule, Scheme (p. 24), and Password protection. For more information see Backup options (p. 24).
9. Perform one of the following:
 - To run the backup immediately, click **Back up now**.
 - To run the backup later or on a schedule, click the arrow to the right of the **Back up now** button, and then click **Later**.

4.2 Backup options

In the **Disk Backup Options** window you can configure options for a disk/partition backup process. To open the options window, click the appropriate link.

After you have installed the application, all options are set to the initial values. You can change them for your current backup operation only or for all backups that will be created in future. Select the **Save the settings as default** check box to apply the modified settings to all further backup operations by default.



Note that options of each backup type are fully independent, and you should configure them separately.

If you want to reset all the modified options to the values that were set after the product installation initially, click the **Reset to initial settings** button.

In this section

Backup schemes.....	24
Notifications for backup operation.....	27
Image creation mode.....	27
Pre/Post commands for backup.....	28
Backup splitting.....	28
Backup validation option.....	29
Backup reserve copy.....	29
Removable media settings.....	30
Backup comment.....	30
Error handling.....	30
Computer shutdown.....	31
Performance of backup operation.....	31

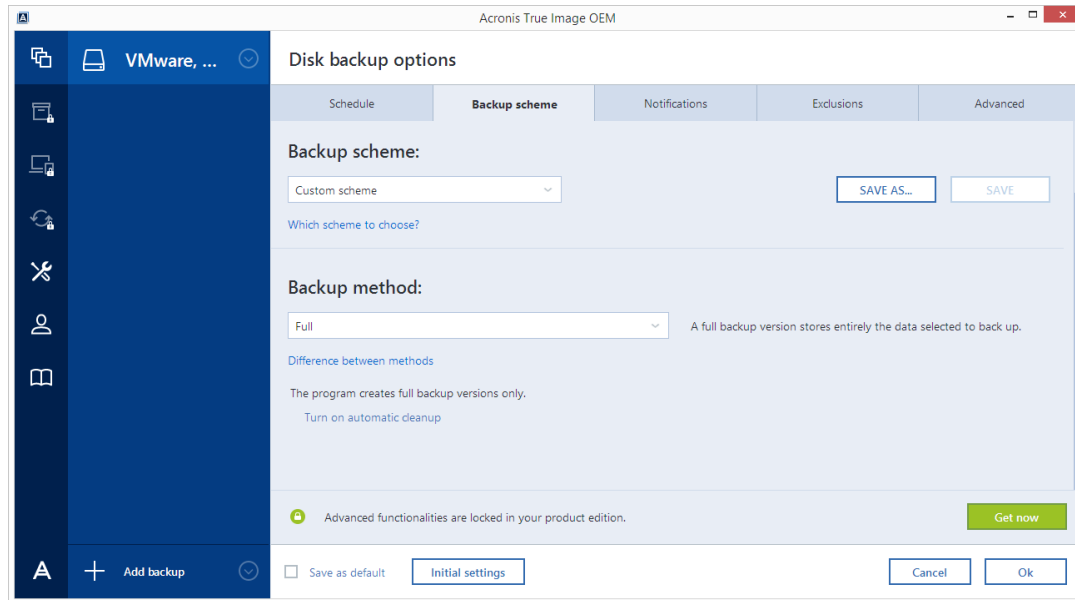
4.2.1 Backup schemes

Note: Certain features and functionalities may be unavailable in the True Image edition that you use.

Backup schemes along with the scheduler help you to set up your backup strategy. The schemes allow you to optimize backup storage space usage, improve data storage reliability, and automatically delete the obsolete backup versions.

Backup scheme defines the following parameters:

- Sequence of the backup versions created using different methods
- Version cleanup rules



Acronis True Image for BIWIN allows you to choose the following backup schemes:

- **Single version** (p. 25) - select this scheme if you want to use the smallest backup storage.
- **Custom** (p. 25) - select this item if you want to set up a backup scheme manually.

4.2.1.1 Single version scheme

The program creates a full backup version and overwrites it every time when you run backup manually.

Result: you have a single up-to-date full backup version.

Required storage space: minimal.

4.2.1.2 Custom schemes

With Acronis True Image for BIWIN you also can create your own backup schemes. Schemes can be based on the pre-defined backup schemes. You can make changes in a selected pre-defined scheme to suit your needs and then save the changed scheme as a new one.

You cannot overwrite existing pre-defined backup schemes.

In addition, you can create custom schemes from scratch based on full backup method. To do this, under **Backup method**, select **Full**.

Automatic cleanup rules

To delete obsolete backup versions automatically, you can set one of the following cleanup rules:

- **Delete versions older than [defined period]** (available for full method only) - Select this option to limit the age of backup versions. All versions that are older than the specified period will be automatically deleted.
- **Delete version chains older than [defined period]** (available for incremental and differential methods only) - Select this option to limit the age of backup version chains. The oldest version chain will be deleted only when the most recent backup version of this chain is older than the specified period.
- **Store no more than [n] recent versions** (available for full method only) - Select this option to limit the maximum number of backup versions. When the number of versions exceeds the specified value, the oldest backup version will be automatically deleted.
- **Store no more than [n] recent version chains** (available for incremental and differential methods only) - Select this option to limit the maximum number of backup version chains. When the number of version chains exceeds the specified value, the oldest backup version chain will be automatically deleted.
- **Keep size of the backup no more than [defined size]** - Select this option to limit the maximum size of the backup. After creating a new backup version, the program checks whether the total backup size exceeds the specified value. If it's true, the oldest backup version will be deleted.

The first backup version option

Often the first version of any backup is one of the most valuable versions. This is true because it stores the initial data state (for example, your system partition with recently installed Windows) or some other stable data state (for example, data after a successful virus check).

Do not delete the first version of the backup - Select this check box to keep the initial data state. The program will create two initial full backup versions. The first version will be excluded from the automatic cleanup, and will be stored until you delete it manually.

If you select incremental or differential method, the first backup chain will start from the second full backup version. And only the third version of the backup will be incremental or differential one.

Note that when the check box is selected, the **Store no more than [n] recent versions** check box will change to **Store no more than 1+[n] recent versions**.

Managing custom backup schemes

If you change anything in an existing backup scheme, you can save the changed scheme as a new one. In this case you need to specify a new name for that backup scheme.

- You can overwrite existing custom schemes.
- You cannot overwrite existing pre-defined backup schemes.
- In a scheme name, you can use any symbols allowed by OS for naming files. The maximum length of a backup scheme name is 255 symbols.
- You can create not more than 16 custom backup schemes.

After creating a custom backup scheme, you can use it as any other existing backup scheme while configuring a backup.

You can also use a custom backup scheme without saving it. In this case, it will be available only for the backup where it was created and you will be unable to use it for other backups.

If you do not need a custom backup scheme anymore, you can delete it. To delete the scheme, select it in the backup schemes list, click **Delete**, and then click **Delete scheme** in the confirmation window.

The pre-defined backup schemes cannot be deleted.

4.2.2 Notifications for backup operation

Sometimes a backup or recovery procedure can last an hour or longer. Acronis True Image for BIWIN can notify you when it is finished via email. The program can also duplicate messages issued during the operation or send you the full operation log after operation completion.

By default all notifications are disabled.

Free disk space threshold

You may want to be notified when the free space on the backup storage becomes less than the specified threshold value. If after starting a backup Acronis True Image for BIWIN finds out that the free space in the selected backup location is already less than the specified value, the program will not begin the actual backup process and 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 for the backup or to cancel the backup.

If the free space becomes less than the specified value while the backup is being run, the program will display the same message and you will have to make the same decisions.

To set the free disk space threshold:

- Select the **Show notification message on insufficient free disk space** check box
- In the **Size** box, type or select a threshold value and select a unit of measure

Acronis True Image for BIWIN can monitor free space on the following storage devices:

- Local hard drives
- USB cards and drives
- Network shares (SMB)

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

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

4.2.3 Image creation mode

You can use these parameters to create an exact copy of your whole partitions or hard disks, and not only the sectors that contain data. For example, this can be useful when you want to back up a partition or disk containing an operating system that is not supported by Acronis True Image. Please note that this mode increases processing time and usually results in a larger image file.

- To create a sector-by-sector image, select the **Back up sector-by-sector** check box.
- To include all unallocated disk space into the backup, select the **Back up unallocated space** check box.

This check box is available only when the **Back up sector-by-sector** check box is selected.

4.2.4 Pre/Post commands for backup

You can specify commands (or even batch files) that will be automatically executed before and after the backup procedure.

For example, you may want to start/stop certain Windows processes, or check your data before starting backup.

To specify commands (batch files):

- Select a command to be executed before the backup process starts in the **Pre-command** field. To create a new command or select a new batch file, click the **Edit** button.
- Select a command to be executed after the backup process ends in the **Post-command** field. To create a new command or select a new batch file, click the **Edit** button.

Please do not try to execute interactive commands, i.e. commands that require user input (for example, "pause"). These are not supported.

4.2.4.1 Edit user command for backup

You can specify user commands to be executed before or after the backup procedure:

- In the **Command** field, type-in a command or select it from the list. Click ... to select a batch file.
- In the **Working directory** field, type-in a path for command execution or select it from the list of previously entered paths.
- In the **Arguments** field enter or select command execution arguments from the list.

Disabling the **Do not perform operations until the command's execution is complete** parameter (enabled for Pre commands by default), will permit the backup process to run concurrently with your command execution.

The **Abort the operation if the user command fails** (enabled by default) parameter will abort the operation if any errors occur in command execution.

You can test a command you entered by clicking the **Test command** button.

4.2.5 Backup splitting

Acronis True Image for BIWIN cannot split already existing backups. Backups can be split only when being created.

Large backups can be split into several files that together make up the original backup. A backup can also be split for burning to removable media.

The default setting - **Automatic**. With this setting, Acronis True Image for BIWIN will act as follows.

When backing up to a hard disk:

- If the selected disk has enough space and its file system allows the estimated file size, the program will create a single backup file.
- If the storage disk has enough space, but its file system does not allow the estimated file size, the program will automatically split the image into several files.
- If you do not have enough space to store the image on your hard disk, the program will warn you and wait for your decision as to how you plan to fix the problem. You can try to free some additional space and continue or select another disk.

When backing up to a CD-R/RW, DVD-R/RW, DVD+R/RW, BD-R/RE:

- Acronis True Image for BIWIN will ask you to insert a new disk when the previous one is full.

Alternatively, you may select the desired file size from the drop-down list. The backup will then be split into multiple files of the specified size. This is useful when you store a backup to a hard disk in order to burn the backup to CD-R/RW, DVD-R/RW, DVD+R/RW or BD-R/RE later on.

Creating images directly on CD-R/RW, DVD-R/RW, DVD+R/RW, BD-R/RE might take considerably more time than it would on a hard disk.

4.2.6 Backup validation option

Note: *Certain features and functionalities may be unavailable in the product edition that you use.*

Location: **Options > Advanced > Validation**

You can specify the following settings:

- **Validate backup each time after it is completed** - Select to check the integrity of the backup version immediately after backup. We recommend that you enable this option when you back up your critical data or system disk.
 - **Validate the latest diverse backup only** - A quick validation of the last backup slice.
 - **Validate entire backup**
- **Validate backup on schedule** - Select to schedule validation of your backups to ensure that they remain "healthy".
 - **The latest diverse backup version when it is completed**
 - **Entire backup when it is completed**

The default settings are as follows:

- **Frequency:** once a month.
- **Day:** the date when the backup was started.
- **Time:** the moment of backup start plus 15 minutes.

You can also configure start of the validation manually from the backup context menu.

To do this, right-click the backup and choose:

- **Validate all versions**
- **Validate the latest version**

You can change the default settings and specify your own schedule.

4.2.7 Backup reserve copy

You can create reserve copies of your backups and save them on the file system or a network drive.

To make a reserve copy:

- Select the **Create a reserve copy of my backups** check box
- Click **Set location...** and specify a location for the backup copies

All backup options (such as backup compression, backup splitting, etc.) will be inherited from the source backup.

A reserve copy always contains all the data selected for backup, that is, when creating a reserve copy the program always makes a full backup of the source data.

Also remember that you will pay for the enhanced convenience and increased security of your data by the time required for performing the backup because normal backup and reserve copying are performed one at a time and not simultaneously.

4.2.8 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.

Acronis True Image for BIWIN does not support creating bootable media if a flash drive is formatted in NTFS or exFAT. The drive must have a FAT16 or FAT32 file system.

The following settings are available:

- **Place Acronis True Image for BIWIN on media**
Acronis True Image for BIWIN - includes support of USB, PC Card (formerly PCMCIA) and SCSI interfaces along with the storage devices connected via them, and therefore is strongly recommended.
- **Place Acronis System Report on media**
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 for BIWIN from the bootable media. The generated system report can be saved to a USB flash drive.
- **Ask for first media while creating backups 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. Therefore, you should disable the prompt when scheduling a backup to removable media. Then, if the removable media is available (for example, CD-R/RW inserted) the backup can run unattended.

If you have other Acronis products installed on your computer, the bootable versions of these programs' components will be offered as well.

4.2.9 Backup comment

This option allows you to add comments to the backup. Backup comments may help you to find the necessary backup later, when recovering data by using bootable media.

If a backup does not have comments, type your comment in the comments area. When a comment already exists, you can edit it after clicking **Edit**.

4.2.10 Error handling

When the program encountered an error while performing backup, it stops the backup process and displays a message, waiting for a response on how to handle the error. If you set an error handling policy, the program will not stop the backup process, but will simply handle the error according to the set rules and continue working.

You can set the following error handling policy:

- **Do not show messages and dialogs while processing (silent mode)** - Enable this setting to ignore errors during backup operations. This is useful when you cannot control the backup process. You can view the detailed log of all operations after the backup process finishes.
- **Ignore bad sectors** - This option is available only for disk and partition backups. It lets you successfully complete a backup even if there are bad sectors on the hard disk.

We recommend that you select this check box when your hard drive is failing, for example:

- Hard drive is making clicking or grinding noises during operation.
- The S.M.A.R.T. system has detected hard drive issues and recommends that you back up the drive as soon as possible.

When you leave this check box cleared, the backup may fail because of possible bad sectors on the drive.

- **Repeat attempt if a backup fails** - This option allows you to automatically repeat a backup attempt if the backup fails for some reason. You can specify number of attempts and time interval between attempts. Note that if the error interrupting the backup persists, then the backup will not be created.

This option is not available, when you back up your data to a USB flash drive or USB hard drive.

4.2.11 Computer shutdown

Location: **Options > Advanced > Computer shutdown**

You can configure the following options:

- **Stop all current operations when I shut down the computer**
When you turn off your computer while Acronis True Image for BIWIN is performing a long operation, for example a disk backup to the cloud, this operation prevents the computer from shutdown. When this check box is selected, Acronis True Image for BIWIN automatically stops all its current operations before shutdown. This may take about two minutes. The next time you run Acronis True Image for BIWIN, it will restart the stopped backups.
- **Shut down the computer after the backup is complete**
If you know that the backup process you are configuring may take a long time, you may select the **Shut down the computer after the backup is complete** check box. In this case, you will not have to wait until the operation completion. The program will perform the backup and turn off your computer automatically.

This option is also useful when you schedule your backups. For example, you may want to perform backups every weekday in the evening to save all your work. Schedule the backup and select the check box. After that you may leave your computer when you finish your work knowing that the critical data will be backed up and the computer will be turned off.

4.2.12 Performance of backup operation

Location: **Options > Advanced > Performance**

Compression level

You can choose the compression level for a backup:

- **None** - the data will be copied without any compression, which may significantly increase the backup file size.
- **Normal** - the recommended data compression level (set by default).

- **High** - higher backup file compression level, takes more time to create a backup.
- **Maximum** - maximum backup compression, but takes a long time to create a backup.

The optimal data compression level depends on the type of files stored in the backup. For example, even maximum compression will not significantly reduce the backup size, if the backup contains essentially compressed files, like .jpg, .pdf or .mp3.

You cannot set or change the compression level for a pre-existing backup.

Operation priority

Changing the priority of a backup or recovery process can make it run faster or slower (depending on whether you raise or lower the priority), but it can also adversely affect the performance of other running programs. The priority of any process running in a system, determines the amount of CPU usage and system resources allocated to that process. Decreasing the operation priority will free more resources for other CPU tasks. Increasing backup or recovery priority may speed up the process by taking resources from the other currently running processes. The effect will depend on total CPU usage and other factors.

You can set up the operation priority:

- **Low** (enabled by default) - the backup or recovery process will run slower, but the performance of other programs will be increased.
- **Normal** - the backup or recovery process will have the equal priority with other processes.
- **High** - the backup or recovery process will run faster, but the performance of other programs will be reduced. Be aware that selecting this option may result in 100% CPU usage by Acronis True Image for BIWIN.

Network connection transfer rate

When you back up data to network drives, or FTP, you can change the connection speed used by Acronis True Image for BIWIN. Set the connection speed that will allow you to use Internet and network resources without annoying slowdowns.

To set up the connection speed, select one of the following options:

- **Maximum**
The data transfer rate is maximum within a system configuration.
- **Limit to**
You can specify a maximum value for data upload speed.

Snapshot for backup

This option is for advanced users only. Do not change the default setting if you are not sure which option to choose.

During a disk or partition backup process, which often takes a long time, some of the backed-up files may be in use, locked, or being modified in one way or another. For example, you may work on a document and save it from time to time. If Acronis True Image for BIWIN backed up files one by one, your open file would likely be changed since the backup start, and then saved in the backup to a different point in time. Therefore, the data in the backup would be inconsistent. To eliminate it, Acronis True Image for BIWIN creates a so-called snapshot that fixes the data to back up to a particular point in time. This is done before the backup starts and guarantees that the data is in consistent state.

Select a backup snapshot type from the list:

- **No snapshot**

A snapshot will not be created. The files will be backed up one by one as an ordinary copy operation.

- **VSS**

Warning! This is the only recommended option for backing up your system. Your computer may not start after recovery from a backup created with a different snapshot type.

This option is default for disk-level and the Entire PC backups, and guarantees data consistency in the backup.

- **Acronis snapshot**

A snapshot will be created with the Acronis driver used in previous versions of Acronis True Image.

- **VSS without writers**

This option is default for file-level backups.

VSS writers are special VSS components for notifying applications that a snapshot is going to be created, so that the applications prepare their data for the snapshot. The writers are needed for applications that perform large number of file operations and require data consistency, for example databases. Because such applications are not installed on home computers, there is no need to use writers. In addition, this reduces the time required for file-level backups.

4.3 Operations with backups

4.3.1 Backup operations menu

The backup operations menu provides quick access to additional operations that can be performed with the selected backup.

The backup operations menu can contain the following items:

- **Rename** - allows you to set a new name for a backup in the list. The backup files will not be renamed.
- **Validate the latest version** - starts quick validation of the last backup slice.
- **Validate all versions** - starts validation of all backup slices.
- **Clean up versions** - allows you to delete backup versions you no longer need.
- **Clone settings** - creates a new empty backup box with the settings of the initial backup and named **(1) [the initial backup name]**. Change the settings, save them, and then click **Back up now** on the cloned backup box.
- **Move** - click to move all the backup files to another location. The subsequent backup versions will be saved to the new location.
If you change the backup destination by editing the backup settings, only new backup versions will be saved to the new location. The earlier backup versions will remain in the old location.
- **Delete** - depending on a backup type, this command completely deletes the backup from its location or allows you to choose whether you want to delete the backup completely or the backup box only. When you delete a backup box, the backup files remain in the location, and you will be able to add the backup to the list later. Note that when you delete a backup completely, the deletion cannot be undone.
- **Open location** - opens the folder containing the backup files.

- **Search files** - allows you to find a specific file or folder in a backup by entering its name into the search field.
- **Convert to VHD** (for disk-level backups) - allows you to convert a selected Acronis backup version (.tib file) to virtual hard disks (.vhd(x) files). The initial backup version will not be modified.

4.3.2 Validating backups

The validation procedure checks whether you will be able to recover data from a backup.

Validating backups in Windows

To validate an entire backup:

1. Start Acronis True Image for BIWIN, and then click **Backup** on the sidebar.
2. From the backup list, right-click the required backup and choose **Validate all versions** or **Validate the latest version**.

Validating backups in a stand-alone version of Acronis True Image (bootable media)

To validate a specific backup version or an entire backup:

1. On the **Recovery** tab, find the backup that contains the version that you want to validate. If the backup is not listed, click **Browse for backup**, and then specify the path to the backup. Acronis True Image adds this backup to the list.
2. Right-click the backup or a specific version, and then click **Validate Archive**. This opens the **Validate Wizard**.
3. Click **Proceed**.

4.3.3 Backing up to various places

Acronis True Image for BIWIN offers you flexibility in choosing destinations for your backups. You can save full backup versions to different places including a network share, CD/DVD, USB stick, as well as any local internal or external hard drive.

You can save backup versions to different destinations by changing the backup destination when editing the settings of a selected backup. For example, after you save the initial full backup to an external USB hard drive, you can change the backup destination to a USB stick by editing the backup settings.

One more useful aspect of this feature is the ability to split backups "on-the-fly". Suppose you perform a backup to a hard disk and in the middle of the backup process Acronis True Image for BIWIN finds out that the disk to which you are backing up, does not have sufficient free space for completing the backup. The program displays a message warning you that the disk is full.

To complete the backup, you may either try to free up some space on the disk and click **Retry** or select another storage device. To choose the latter option, click **Browse...** in the confirmation window. The **Browse for Destination** window appears.

The left pane shows the storage locations available on your computer. After you select a suitable location, assign a name for the file that will contain the remaining data being backed up. You can enter the name manually (for example, "tail_end.tib") or use the file name generator (a button to the right of the line). Then click **OK** and Acronis True Image for BIWIN will complete the backup.

If backup versions belonging to the same backup "chain" have been saved to different destinations, Acronis True Image for BIWIN may prompt you for the locations of previous backup versions during

data recovery. This may occur when the selected backup version does not contain the files you want to recover (or contains only a part of them). This may also happen when you recover a backup that was split on-the-fly.

4.3.4 Adding an existing backup to the list

You may have Acronis True Image backups created by a previous product version or copied from another computer. Every time you start Acronis True Image for BIWIN, it scans your computer for such backups and adds them to the backup list automatically.

If you have backups that are not shown in the list, you can add them manually.

To add backups manually:

1. In the **Backup** section, click **Add backup**, and then click **Add existing backup**. Program opens a window where you can browse for backups on your computer.
2. Select a backup version (a .tib file), and then click **Add**.
The entire backup will be added to the list.

4.3.5 Deleting backups and backup versions

You may want to delete backups and backup versions you no longer need. Acronis True Image for BIWIN stores information on the backups in a metadata information database.

Therefore, deleting unneeded backup files in Windows Explorer will not delete information about these backups from the database, and Acronis True Image for BIWIN 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 versions by using the tools provided by Acronis True Image for BIWIN.

To delete an entire backup:

Find the corresponding backup box on the **Backup and recovery** tab of Acronis True Image for BIWIN. Click the gear icon to open the Operations menu and then click **Delete**.

When you delete an entire backup, all its versions will be deleted as well.

To delete a specific backup version:

1. On the **Backup and recovery** tab, find the corresponding backup box, click **Explore and recover**.
2. In Backup explorer, right-click on the time line the version you want to delete, and then click **Delete version**.

5 Recovering data

In this section

Recovering disks and partitions	36
Recovery options.....	49

5.1 Recovering disks and partitions

5.1.1 Recovering your system after a crash

When your computer fails to boot, it is advisable to at first try to find the cause using the suggestions given in Trying to determine the crash cause (p. 36). If the crash is caused by corruption of the operating system, use a backup to recover your system. Make the preparations described in Preparing for recovery (p. 36) and then proceed with recovering your system (p. 37).

5.1.1.1 Trying to determine the crash cause

A system crash can be due to two basic factors:

- **Hardware failure**

In this scenario, it is better to let your service center handle the repairs. However, you may want to perform some routine tests. Check the cables, connectors, power of external devices, etc. Then, restart the computer. If there is a hardware problem, the Power-On Self Test (POST) will inform you about the failure.

If the POST does not reveal a hardware failure, enter BIOS and check whether it recognizes your system hard disk drive. To enter BIOS, press the required key combination (**Del**, **F1**, **Ctrl+Alt+Esc**, **Ctrl+Esc**, or some other, depending on your BIOS) during the POST sequence. Usually the message with the required key combination is displayed during the startup test. Pressing this combination takes you to the setup menu. Go to the hard disk autodetection utility which usually comes under "Standard CMOS Setup" or "Advanced CMOS setup". If the utility does not detect the system drive, it has failed and you need to replace the drive.

- **Operating system corruption (Windows cannot start up)**

If the POST correctly detects your system hard disk drive, then the cause of the crash is probably a virus, malware or corruption of a system file required for booting. In this case, recover the system using a backup of your system disk or system partition. Refer to Recovering your system (p. 37) for details.

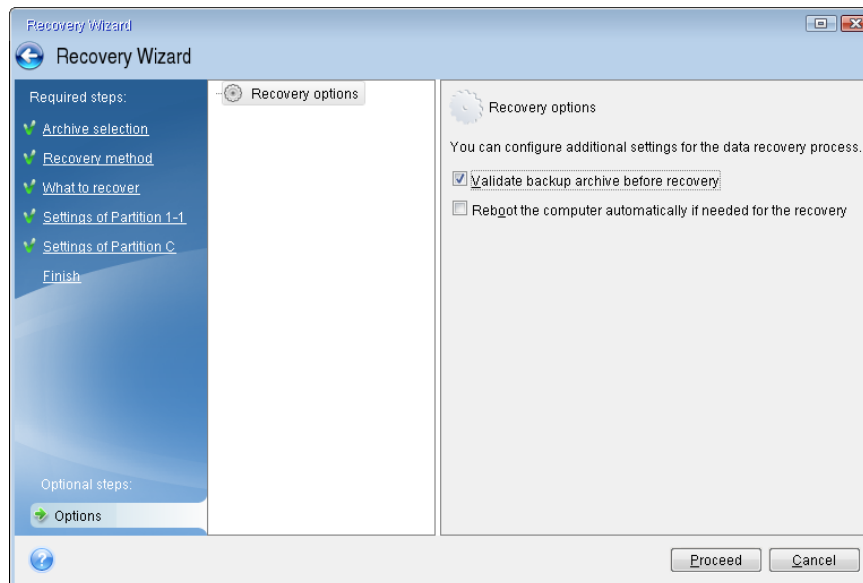
5.1.1.2 Preparing for recovery

We recommend that you perform the following actions before recovery:

- Scan the computer for viruses if you suspect that the crash occurred due to a virus or malware attack.
- Under bootable media, try a test recovery to a spare hard drive, if you have one.
- Validate the image under bootable media. A backup that can be read during validation in Windows, **may not always be readable in a Linux environment.**

Under bootable media, there are two ways to validate a backup:

- To validate a backup manually, on the **Recovery** tab, right-click a backup and select **Validate Archive**.
- To validate a backup automatically before recovery, on the **Options** step of the **Recovery Wizard**, select the **Validate backup archive before recovery** check box.



- Assign unique names (labels) to all partitions on your hard drives. This will make finding the disk containing your backups easier.

When you use the Acronis True Image for BIWIN rescue media, it creates disk drive letters that might differ from the way Windows identifies drives. For example, the D: disk identified in the standalone Acronis True Image for BIWIN might correspond to the E: disk in Windows.

5.1.1.3 Recovering your system to the same disk

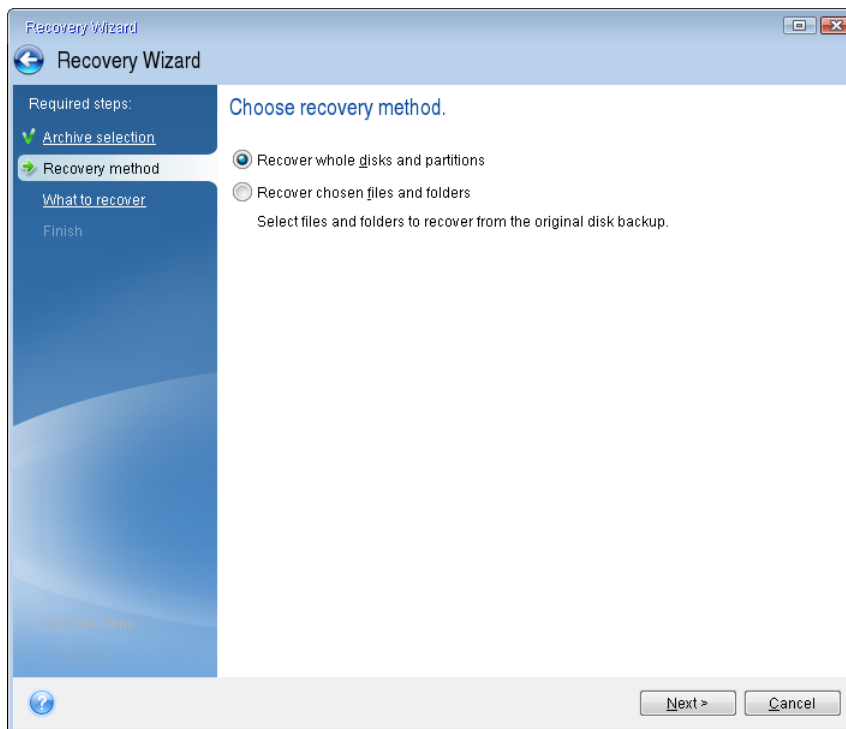
Before you start, we recommend that you complete the procedures described in Preparing for recovery (p. 36).

To recover your system:

1. Attach the external drive if it contains the backup to be used for recovery and make sure that the drive is powered on.
2. Arrange the boot order in BIOS so as to make your rescue media device (CD, DVD or USB stick) the first boot device. See Arranging boot order in BIOS (p. 47).
3. Boot from the rescue media and select **Acronis True Image for BIWIN**.
4. On the **Home** screen, select **My disks** below **Recover**.
5. Select the system disk or partition backup to be used for recovery.

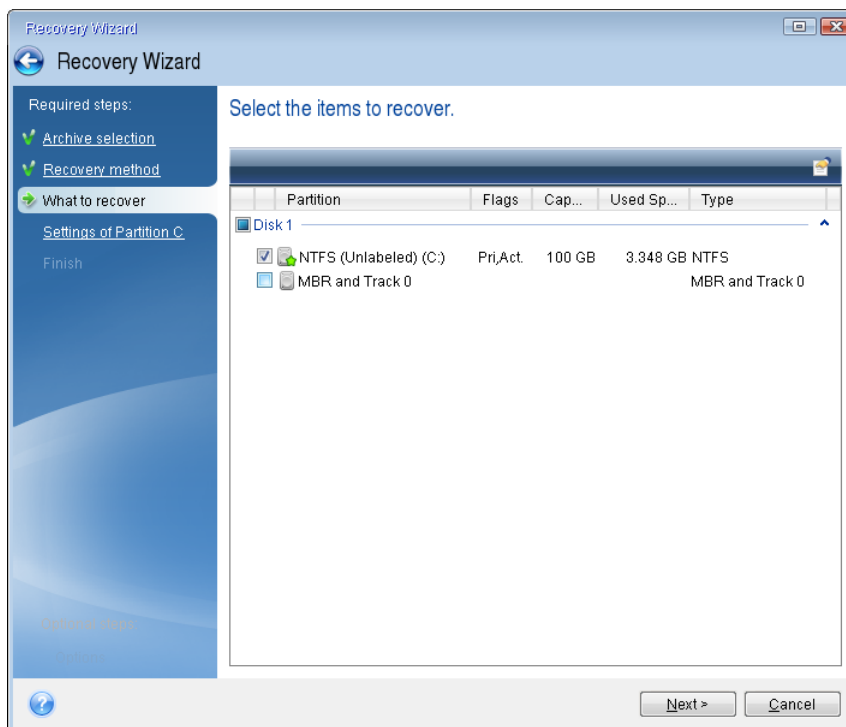
When the backup is not displayed, click **Browse** and specify path to the backup manually.

6. Select **Recover whole disks and partitions** at the **Recovery method** step.



7. 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.

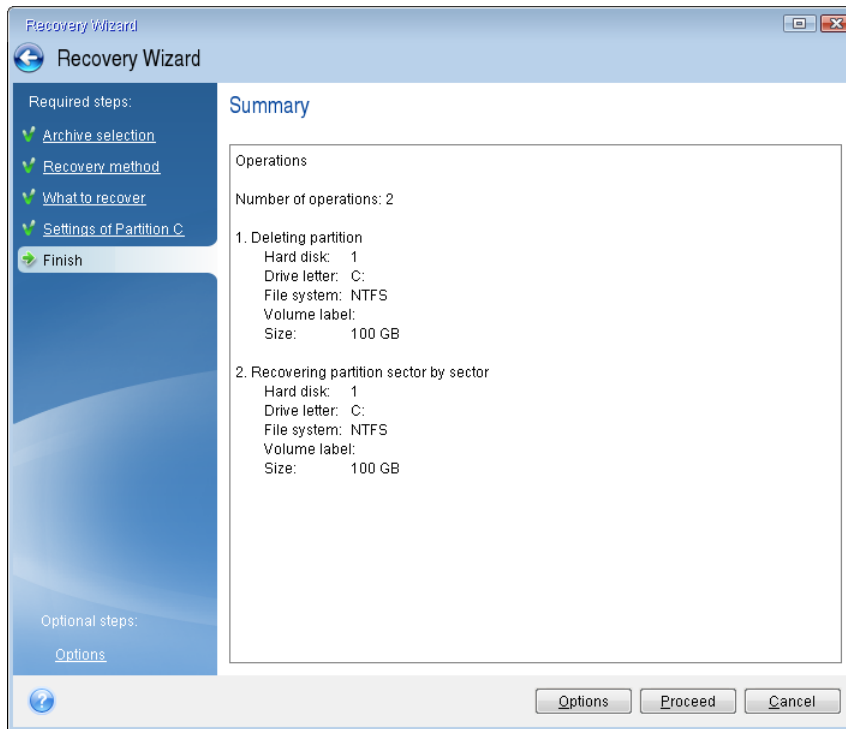
*In case of Windows 7 the System Reserved partition will have the **Pri, Act** flags. You will need to select for recovery both the System Reserved partition and the System partition.*



8. 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 as required

before clicking **Next**. Changing the settings will be needed when recovering to the new hard disk of a different capacity.

- 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. Having checked the summary click **Proceed**.



- When the operation finishes, exit the standalone version of Acronis True Image, remove the rescue media and boot from the recovered system partition. After making sure that you have recovered Windows to the state you need, restore the original boot order.

5.1.1.4 Recovering your system to a new disk under bootable media

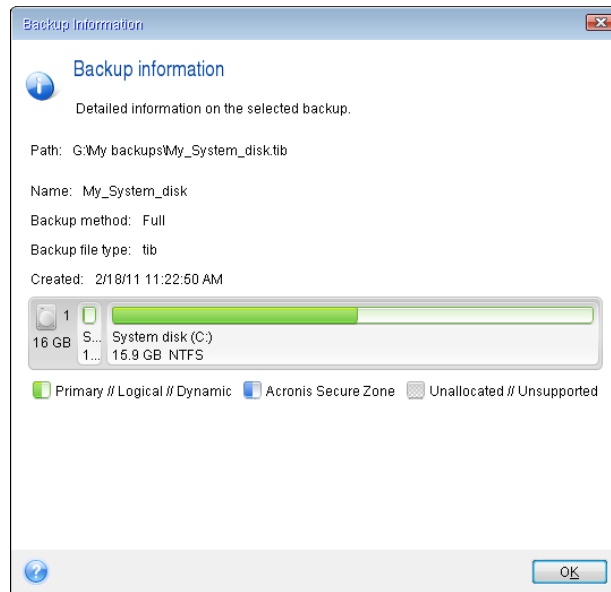
Before you start, we recommend that you complete the preparations described in Preparing for recovery (p. 36). You do not need to format the new disk, as this will be done in the process of recovery.

Warning! Your old and new hard drives must work in the same controller mode (for example, IDE or AHCI). Otherwise, your computer will not start from the new hard drive.

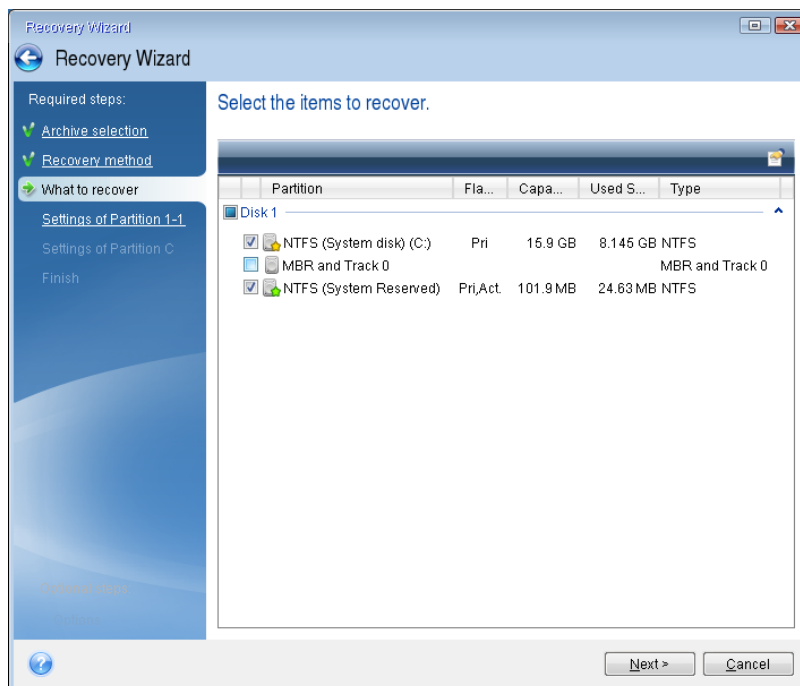
To recover your system to a new disk:

- Install the new hard drive to the same position in the computer and use the same cable and connector that was used for the original drive. If this is not possible, install the new drive to where it will be used.
- Attach the external drive if it contains the backup to be used for recovery and make sure that the drive is powered on.
- Arrange the boot order in BIOS so as to make your rescue media device (CD, DVD or USB stick) the first boot device. See Arranging boot order in BIOS (p. 47).
- Boot from the rescue media and select **Acronis True Image for BIWIN**.
- On the **Home** screen, select **My disks** below **Recover**.

6. Select the system disk or partition backup to be used for recovery. When the backup is not displayed, click **Browse** and specify path to the backup manually.
7. If you have a hidden partition (for example, the System Reserved partition or a partition created by the PC manufacturer), click **Details** on the wizard's toolbar. Please remember the location and size of the hidden partition, because these parameters need to be the same on your new disk.



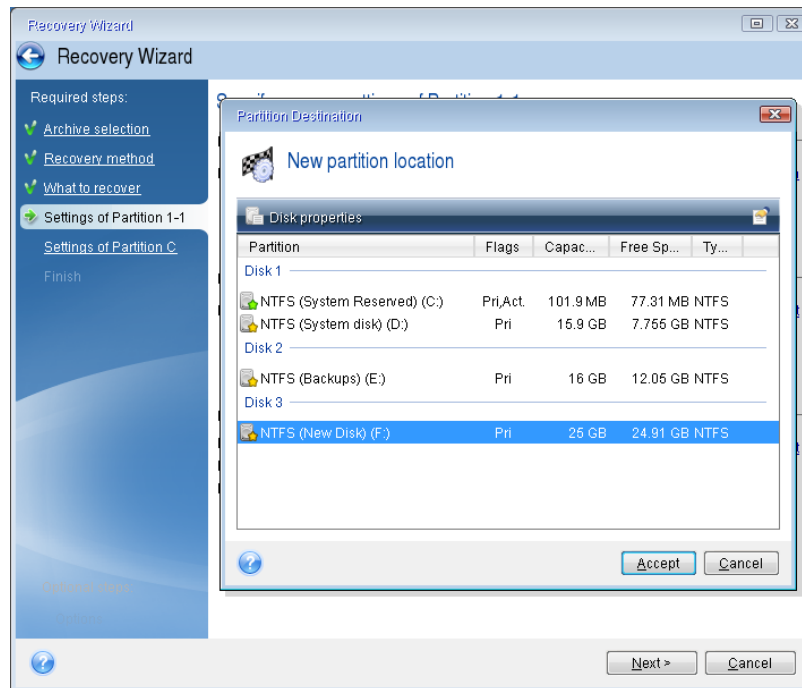
8. Select **Recover whole disks and partitions** at the **Recovery method** step.
9. On the **What to recover** step, select the boxes of the partitions to be recovered. Do not select the **MBR and Track 0** box.



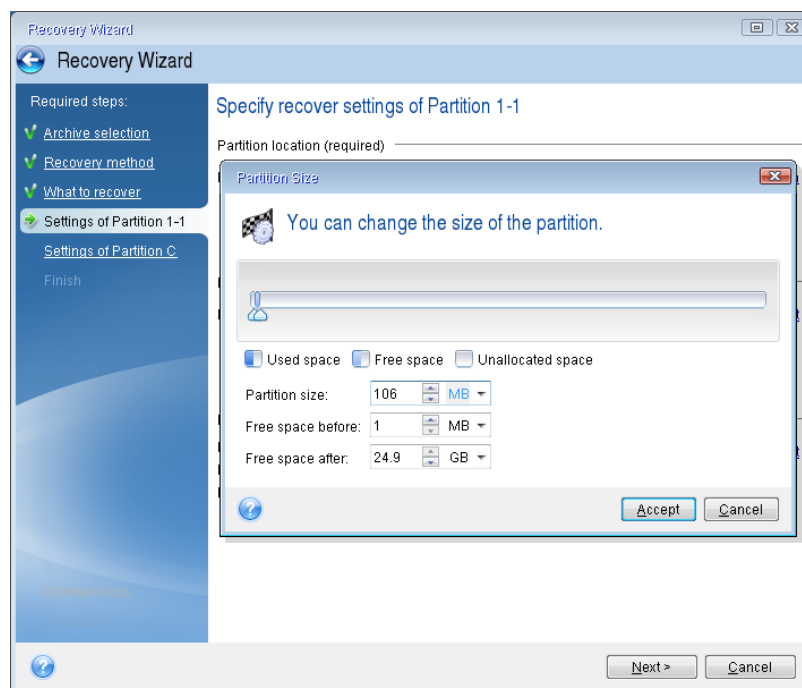
Selecting partitions leads to appearance of the relevant steps "Settings of partition ...". Note that these steps start with partitions which do not have an assigned disk letter (as usually is the case with hidden partitions). The partitions then take an ascending order of partition disk letters. This order cannot be changed. The order may differ from the physical order of the partitions on the hard disk.

10. On the Settings of the hidden partition step (usually named Settings of Partition 1-1), specify the following settings:

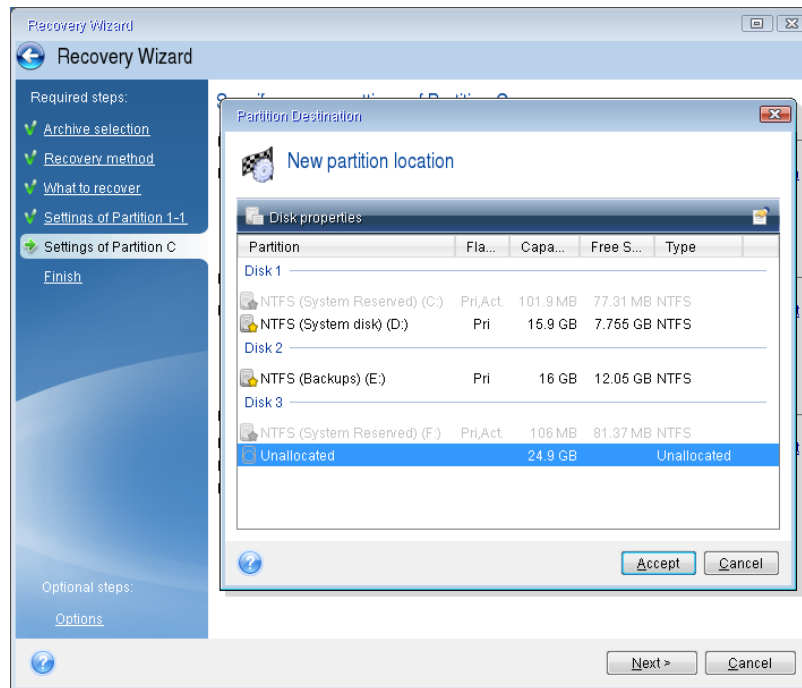
- **Location.** Click **New location**, select your new disk by either its assigned name or capacity, and then click **Accept**.



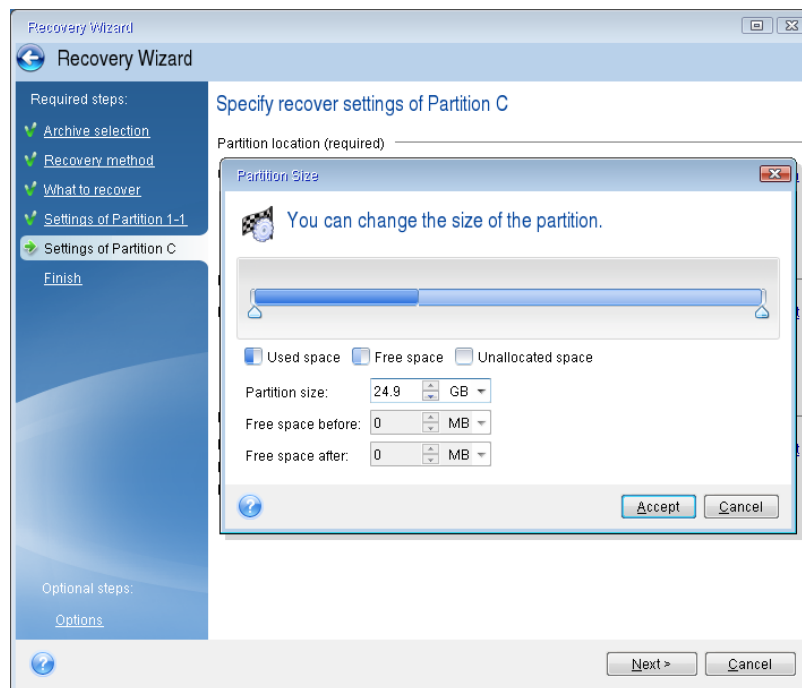
- **Type.** Check the partition type and change it, if necessary. Ensure that the System Reserved partition (if any) is primary and marked as active.
- **Size.** Click **Change default** in the Partition size area. By default the partition occupies the entire new disk. Enter the correct size in the Partition size field (you can see this value on the **What to recover** step). Then drag this partition to the same location that you saw in the Backup Information window, if necessary. Click **Accept**.



11. On the **Settings of Partition C** step, specify the settings for the second partition, which in this case is your system partition.
 - Click **New location**, and then select unallocated space on the destination disk that will receive the partition.



- Change the partition type, if necessary. The system partition must be primary.
- 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**.



12. Carefully read the summary of operations to be performed and then click **Proceed**.

If your original disk contains a hidden partition created by the PC manufacturer, please proceed to MBR recovery. You need to recover the MBR because the PC manufacturer could change the generic Windows MBR or a sector on track 0 to provide access to the hidden partition.

1. Select the same backup again. 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.
2. At the next step, select the destination disk as the target for MBR recovery. You can also recover the disk signature. Refer to *Selecting target disk for MBR recovery* (p. 43) for details.
Click **Next** and then **Proceed**. After MBR recovery is complete, exit the standalone version of Acronis True Image.

When the recovery is complete

Before you boot the computer, please disconnect the old drive (if any). If Windows "sees" both the new and old drive during the boot, this will result in problems booting Windows. If you upgrade the old drive to a larger capacity new one, disconnect the old drive before the first boot.

Remove the rescue media and 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 order.

Selecting target disk for MBR recovery

In this window you should select a hard disk for recovering the Master Boot Record (MBR) along with track 0.

Recover disk signature check box

If you have selected MBR recovery at the **Content selection** step, the **Recover disk signature** check box will be in the bottom left corner. Disk signature is a part of a hard disk MBR. It is used for uniquely identifying the disk media.

We recommend that you select the **Recover disk signature** check box due to the following reasons:

- Acronis True Image for BIWIN 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.
- Some installed applications use a disk signature for licensing and other purposes.
- If you use Windows Restore Points, they will be lost when the disk signature is not recovered.
- Recovering a disk signature allows recovering VSS snapshots used by Windows Vista and Windows 7's "Previous Versions" feature.

We recommend that you clear the **Recover disk signature** check box when:

- You use an image backup not for disaster recovery but for cloning your Windows hard drive to another one.

In this case, Acronis True Image for BIWIN generates a new disk signature for the recovered hard drive, even if you recover to the same drive.

Having selected a hard disk drive and specified whether to recover the disk signature, click **Next** to continue.

5.1.2 Recovering partitions and disks

To recover partitions or disks:

1. Start Acronis True Image for BIWIN.
2. In the **Backup** section, select the backup which contains the partitions or disks you want to recover, and then click **Recover disks**.
3. In the **Backup version** list, select the backup version you want to recover by its backup date and time.
4. Select the disks to recover.

If you need to recover separate partitions, click **Recover specific partitions**, and then select the partitions to recover.

5. In the recovery destination field below the partition name, select the destination partition. Unsuitable partitions are marked by red lettering. Note that all data on the destination partition will be lost because it is replaced by the recovered data and file system.

*To recover to the original partition, at least 5 % of the partition space must be free. Otherwise, the **Recover now** button will be unavailable.*

6. [optional step] To set up additional parameters for the disk recovery process, click **Options**.
7. After you finish with your selections, click **Recover now** to start recovery.

5.1.2.1 Partition properties

When you recover partitions to a basic disk, you can change properties of these partitions. To open the **Partition Properties** window, click **Properties** next to the selected target partition.

The screenshot shows the 'Manage Partition' dialog box. It has a title bar with a close button (X). The main area contains several fields: 'Letter' (G), 'Label' (New Volume), and 'Type' (Primary). Below these is a progress bar. Further down, it shows 'Used: 1.2 GB', 'Partition size: 9.0 GB', and 'Unallocated space: Place after partition 7.0 GB'. At the bottom, there is an information message: 'You can create partitions on the unallocated space, by using Acronis Disk Director. Learn more about Acronis Disk Director'. An 'Ok' button is located at the bottom right.

You can change the following partition properties:

- **Letter**
- **Label**
- **Type**
You can make the partition primary, primary active, or logical.
- **Size**

You can resize the partition by dragging the right-side border with your mouse, on the horizontal bar on the screen. To assign the partition a specific size, enter the appropriate number into the **Partition size** field. You can also select the position of unallocated space—before or after the partition.

5.1.3 About recovery of dynamic/GPT disks and volumes

Recovery of dynamic volumes

You can recover dynamic volumes to the following locations on the local hard drives:

- **Dynamic volume.**

Manual resizing of dynamic volumes during recovery to dynamic disks is not supported. If you need to resize a dynamic volume during recovery, it should be recovered to a basic disk.

- **Original location (to the same dynamic volume).**

The target volume type does not change.

- **Another dynamic disk or volume.**

The target volume type does not change. For example, when recovering a dynamic striped volume over a dynamic spanned volume the target volume remains spanned.

- **Unallocated space of the dynamic group.**

The recovered volume type will be the same as it was in the backup.

- **Basic volume or disk.**

The target volume remains basic.

- **Bare-metal recovery.**

When performing a so called "bare-metal recovery" of dynamic volumes to a new unformatted disk, the recovered volumes become basic. If you want the recovered volumes to remain dynamic, the target disks should be prepared as dynamic (partitioned and formatted). This can be done using third-party tools, for example, Windows Disk Management snap-in.

Recovery of basic volumes and disks

- When recovering a basic volume to an unallocated space of the dynamic group, the recovered volume becomes dynamic.
- When recovering a basic disk to a dynamic disk of a dynamic group consisting of two disks, the recovered disk remains basic. The dynamic disk to which the recovery is performed becomes "missing" and a spanned/striped dynamic volume on the second disk becomes "failed".

Partition style after recovery

The target disk's partition style depends on whether your computer supports UEFI and on whether your system is BIOS-booted or UEFI-booted. See the following table:

	My system is BIOS-booted (Windows or Acronis Bootable Media)	My system is UEFI-booted (Windows or Acronis Bootable Media)
My source disk is MBR and my OS does not support UEFI	The operation will not affect neither partition layout nor bootability of the disk: partition style will remain MBR, the destination disk will be bootable in BIOS.	After operation completion, the partition style will be converted to GPT style, but the operating system will fail booting from UEFI, since your operating system does not support it.
My source disk is MBR and my OS supports UEFI	The operation will not affect neither partition layout nor bootability of the disk: partition style will remain MBR, the destination disk will be bootable in BIOS.	The destination partition will be converted to GPT style that will make the destination disk bootable in UEFI. See Example of recovery to UEFI system (p. 46).
My source disk is GPT and my OS supports UEFI	After operation completion, the partition style will remain GPT, the system will fail booting on BIOS, because your operating system cannot support booting from GPT on BIOS.	After operation completion, the partition style will remain GPT, the operating system will be bootable on UEFI.

Example of recovery procedure

See Example of recovery to a UEFI system (p. 46).

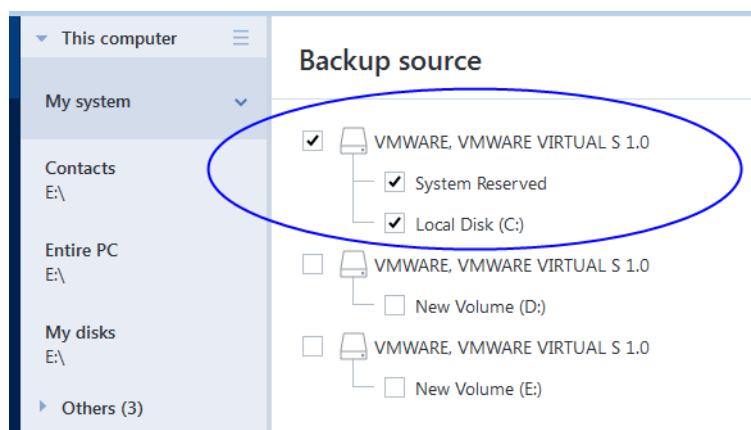
5.1.3.1 Example of recovery to a UEFI system

Here is an example for transferring a system with the following conditions:

- The source disk is MBR and the OS supports UEFI.
- The target system is UEFI-booted.
- Your old and new hard drives work in the same controller mode (for example, IDE or AHCI).

Before you start the procedure, please ensure that you have:

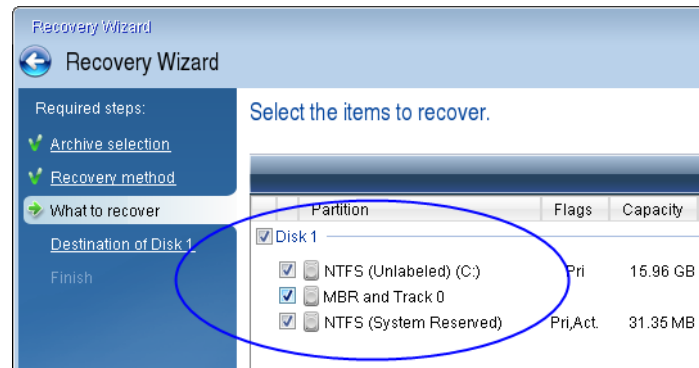
- **Acronis bootable media.**
Refer to Creating Acronis bootable media (p. 11) for details.
- **Backup of your system disk created in disk mode.**
To create this backup, switch to disk mode, and then select the hard drive that contains your system partition. Refer to Backing up disks and partitions (p. 23) for details.



To transfer your system from an MBR disk to a UEFI-booted computer:

1. Boot from the Acronis bootable media in UEFI mode and select Acronis True Image.
2. Run the **Recovery wizard** and follow the instructions described in Recovering your system (p. 37).
3. On the **What to recover** step, select the check box next to the disk name to select the entire system disk.

In the example below, you need to select the **Disk 1** check box:



4. On the **Finish** step, click **Proceed**.

When the operation finishes, the destination disk is converted to GPT style so that it is bootable in UEFI.

After the recovery, please ensure that you boot your computer in UEFI mode. You may need to change the boot mode of your system disk in the user interface of the UEFI boot manager.

5.1.4 Arranging boot order in BIOS

To boot your computer from Acronis bootable rescue media, you need to arrange boot order in BIOS so the media is the first booting device.

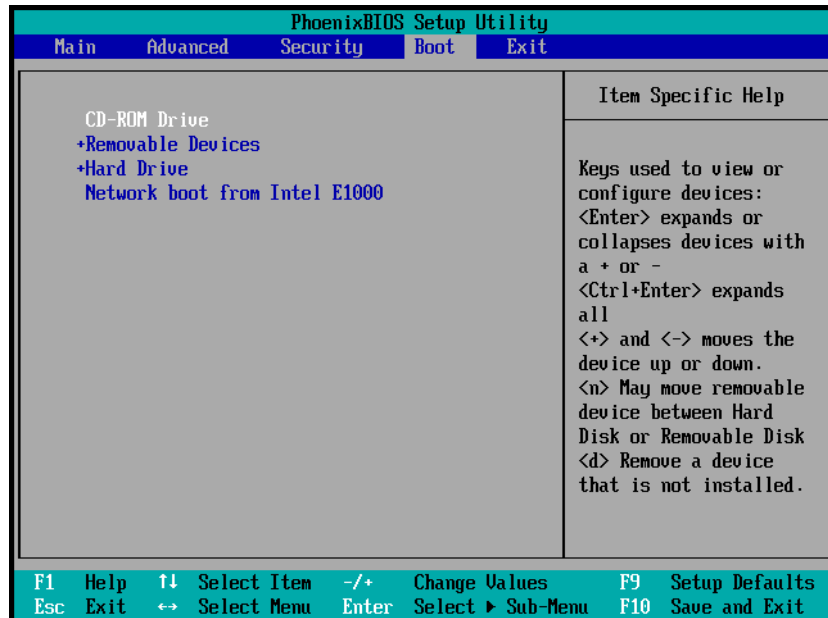
To boot from Acronis bootable media:

1. If you use a USB flash drive as a bootable media, plug it into the USB port.
2. Turn your computer on. During the Power-On Self Test (POST), you will see the key combination that you need to press in order to enter BIOS.
3. Press the key combination (such as, **Del**, **F1**, **Ctrl+Alt+Esc**, **Ctrl+Esc**). BIOS setup utility will open. Note that BIOS may differ in appearance, sets of items, names, etc.

*Some motherboards have a so called boot menu opened by pressing a certain key or key combination, for instance, **F12**. The boot menu allows selecting the boot device from a list of bootable devices without changing the BIOS setup.*

4. If you use a CD or DVD as a bootable media, insert it in the CD or DVD drive.
5. Make your rescue media (CD, DVD or USB drive) device the first booting device:
 1. Navigate to the Boot order setting by using the arrow keys on your keyboard.

- Place the pointer on the device of your bootable media and make it the first item in the list. You can usually use the Plus Sign and the Minus Sign keys to change the order.



- Exit BIOS and save the changes that you made. The computer will boot from Acronis bootable media.

If the computer fails to boot from the first device, it tries to boot from the second device in the list, and so on.

5.1.5 Recovering files and folders

You can recover files and folders both from file-level and disk-level backups.

To recover files and folders:

- Start Acronis True Image for BIWIN.
- On the sidebar, click **Backup**.
- From the backup list, select the backup which contains the files or folders that you want to recover.
- On the right panel, click **Recover files**.
- Select backup version (data state on specific date and time).
- Select the files and folders that you want to recover, and then click **Next**.
- Select a destination on your computer to where you want to recover selected files/folders. You can recover data to its original location or choose a new one, if necessary. To choose a new location, click the **Browse** button.
- When needed, set the options for the recovery process (recovery process priority, file-level security settings, etc.). To set the options, click **Options**. The options you set here will be applied only to the current recovery operation.
- To start the recovery process, click the **Recover now** button.
You can stop the recovery by clicking **Cancel**. Please keep in mind that the aborted recovery may still cause changes in the destination folder.

Recovering files in Windows Explorer

To recover files and folders directly from Windows Explorer:

1. Double-click the corresponding .tib file, and then browse to the file or folder that you want to recover.
2. Copy the file or folder to a hard disk.

Note: The copied files lose the "Compressed" and "Encrypted" attribute. If you need to keep these attributes, it is recommended to recover the backup.

5.1.6 Searching backup content

While recovering data from local backups, you can search for specific files and folders stored in the selected backup.

To search for files and folders:

1. Start recovering data as described in Recovering partitions and disks (p. 44) or Recovering files and folders (p. 48).
2. When selecting files and folders to recover, enter the file or folder name into the **Search** field. The program shows search results.
You can also use the common Windows wildcard characters: * and ?. For example, to find all files with extension **.exe**, enter ***.exe**. To find all .exe files with names consisting of five symbols and starting with "my", enter **My????.exe**.
3. By default, Acronis True Image for BIWIN searches the folder selected on the previous step. To include the entire backup in the search, click the down arrow, and then click **in entire backup**. To return to the previous step, delete the search text, and then click the cross icon.
4. After the search is complete, select the files that you want to recover, and then click **Next**.

Note: Pay attention to the Version column. The files and folders that belong to different backup versions cannot be recovered at the same time.

5.2 Recovery options

In the **Disk Recovery Options** you can configure options for a disk/partition and file recovery processes respectively. After you installed the application, all options are set to the initial values. You can change them for your current recovery operation only or for all further recovery operations as well. Select the **Save the settings as default** check box to apply the modified settings to all further recovery operations by default.

If you want to reset all the modified options to their initial values that were set after the product installation, click the **Reset to initial settings** button.

In this section

Disk recovery mode	50
Pre/Post commands for recovery	50
Validation option.....	50
Computer restart	51
File recovery options.....	51
Overwrite file options	51
Performance of recovery operation	51
Notifications for recovery operation	52

5.2.1 Disk recovery mode

With this option you can select the disk recovery mode for image backups.

- **Recover sector-by-sector** - select this check box if you want to recover both used and unused sectors of disks or partitions. This option will be effective only when you choose to recover a sector-by-sector backup.

5.2.2 Pre/Post commands for recovery

You can specify commands (or even batch files) that will be automatically executed before and after the recovery procedure.

For example, you may want to start/stop certain Windows processes, or check your data for viruses before recovery.

To specify commands (batch files):

- Select a command to be executed before the recovery process starts in the **Pre-command** field. To create a new command or select a new batch file, click the **Edit** button.
- Select a command to be executed after the recovery process ends in the **Post-command** field. To create a new command or select a new batch file, click the **Edit** button.

Please do not try to execute interactive commands, i.e. commands that require user input (for example, "pause"). These are not supported.

5.2.2.1 Edit user command for recovery

You can specify user commands to be executed before or after recovery:

- In the **Command** field type-in a command or select it from the list. Click ... to select a batch file.
- In the **Working directory** field type-in a path for command execution or select it from the list of previously entered paths.
- In the **Arguments** field enter or select command execution arguments from the list.

Disabling the **Do not perform operations until the command execution is complete** parameter (enabled by default), will permit the recovery process to run concurrently with your command execution.

The **Abort the operation if the user command fails** (enabled by default) parameter will abort the operation if any errors occur in command execution.

You can test the command you entered by clicking the **Test command** button.

5.2.3 Validation option

- **Validate backup before recovery**—Enable this option to check the backup integrity before recovery.
- **Check the file system after recovery**—Enable this option to check the file system integrity on the recovered partition.

Only FAT16/32 and NTFS file systems can be checked.

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.

5.2.4 Computer restart

If you want the computer to reboot automatically when it is required for recovery, select the **Restart the computer automatically if needed for the recovery** check box. This may be used when a partition locked by the operating system has to be recovered.

5.2.5 File recovery options

You can select the following file recovery options:

- **Recover files with their original security settings** - if the file security settings were preserved during backup, 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 backups.
- **Set current date and time for recovered files** - you can choose whether to recover the file date and time from the backup or assign the files the current date and time. By default the file date and time from the backup will be assigned.

5.2.6 Overwrite file options

Choose what to do if the program finds a file in the target folder with the same name as in the backup.

This option is available only while restoring data from file-level backups.

Selecting the **Overwrite existing files** check box will give the files from the backup unconditional priority over the files on the hard disk, though, by default, the more recent files and folders are protected against overwriting. If you want to overwrite those files and folders too, clear the appropriate check box.

If you do not need to overwrite some files:

- Select/clear the **Hidden files and folders** check box to enable/disable overwriting of all hidden files and folders.
- Select/clear the **System files and folders** check box to enable/disable overwriting of all system files and folders.
- Select/clear the **More recent files and folders** check box to enable/disable overwriting of new files and folders.
- Click **Add specific files and folders** to manage the list of custom files and folders that you do not want to overwrite.
 - To disable overwriting of specific files, click the **Add...** button to create an exclusion criterion.
 - While specifying the criteria, you can use the common Windows wildcard characters. For example, to preserve all files with extension **.exe**, you can add ***.exe**. Adding **My???.exe** will preserve all **.exe** files with names consisting of five symbols and starting with "my".

To delete a criterion, for example, added by mistake, click the Delete icon to the right of the criterion.

5.2.7 Performance of recovery operation

On the **Performance** tab you can configure the following settings:

Operation priority

Changing the priority of a backup or recovery process can make it run faster or slower (depending on whether you raise or lower the priority), but it can also adversely affect the performance of other running programs. The priority of any process running in a system, determines the amount of CPU usage and system resources allocated to that process. Decreasing the operation priority will free more resources for other CPU tasks. Increasing backup or recovery priority may speed up the process by taking resources from the other currently running processes. The effect will depend on total CPU usage and other factors.

You can set up the operation priority:

- **Low** (enabled by default) - the backup or recovery process will run slower, but the performance of other programs will be increased.
- **Normal** - the backup or recovery process will have the equal priority with other processes.
- **High** - the backup or recovery process will run faster, but the performance of other programs will be reduced. Be aware that selecting this option may result in 100% CPU usage by Acronis True Image for BIWIN.

5.2.8 Notifications for recovery operation

Sometimes a backup or recovery procedure can last an hour or longer. Acronis True Image for BIWIN can notify you when it is finished via e-mail. The program can also duplicate messages issued during the operation or send you the full operation log after operation completion.

By default all notifications are disabled.

Free disk space threshold

You may want to be notified when the free space on the backup storage becomes less than the specified threshold value. If after starting a backup Acronis True Image for BIWIN finds out that the free space in the selected backup location is already less than the specified value, the program will not begin the actual backup process and 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 for the backup or to cancel the backup.

If the free space becomes less than the specified value while the backup is being run, the program will display the same message and you will have to make the same decisions.

To set the free disk space threshold:

- Select the **Show notification message on insufficient free disk space** check box
- In the **Size** box, type or select a threshold value and select a unit of measure

Acronis True Image for BIWIN can monitor free space on the following storage devices:

- Local hard drives
- USB cards and drives
- Network shares (SMB)

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

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

E-mail notification

You can specify an email account that will be used to send you email notifications.

To configure the email notifications:

1. Select the **Send e-mail notifications about the operation state** check box.
2. Configure email settings:
 - Enter the email address in the **To** field. You can enter several email addresses in a semicolon-delimited format.
 - Enter the outgoing mail server (SMTP) in the **Outgoing mail server (SMTP)** field.
 - Set the port of the outgoing mail server. By default the port is set to 25.
 - If required, select the **SMTP authentication** check box, and then enter the user name and password in the corresponding fields.
3. To check whether your settings are correct, click the **Send test message** button.

If the test message sending fails, then perform the following:

1. Click **Show extended settings**.
2. Configure additional email settings:
 - Enter the e-mail sender address in the **From** field. If you are not sure what address to specify, then type any address you like in a standard format, for example *aaa@bbb.com*.
 - Change the message subject in the **Subject** field, if necessary.
 - Select the **Log on to incoming mail server** check box.
 - Enter the incoming mail server (POP3) in the **POP3 server** field.
 - Set the port of the incoming mail server. By default the port is set to 110.
3. Click the **Send test message** button again.

Additional notification settings:

- To send a notification concerning process completion, select the **Send notification upon operation's successful completion** check box.
- To send a notification concerning process failure, select the **Send notification upon operation failure** check box.
- To send a notification with operation messages, select the **Send notification when user interaction is required** check box.
- To send a notification with full log of operations, select the **Add full log to the notification** check box.

6 Antivirus and antimalware protection

- Active Protection runs constantly in the background to protect your machines in real time while you work as usual.

Note You can turn the protection on or off in the True Image UI only. You cannot stop the process manually through Task Manager or any other external tool.

The Protection dashboard

The Protection dashboard contains statistical data on the **Active protection** processes, provides control over the protection status, and access to the settings.

To access the Protection dashboard, click **Protection** on the Acronis True Image for BIWIN sidebar.

On the **Overview** tab of the dashboard, you can:

- View statistics about the active protection status.
- View the number of detected issues, quarantined, and excluded items.
- Stop the entire protection for a predefined period of time (30 minutes, 1 hour, 4 hours, until restart). To do this, click **Turn off protection** and choose the period.

On the **Activity** tab of the dashboard, you can view a log of the changes that you applied to your protection status and settings.

In this section

Active protection.....	54
Managing files in Quarantine.....	56
Configuring Protection exclusions	56

6.1 Active protection

Active Protection constantly checks your computer for ransomware and other malicious threats. In addition to your files, Acronis Active Protection protects the Acronis True Image application files, your backups, archives, and the Master Boot Records of your hard drives.

Antiransomware protection

Ransomware encrypts files and demands a ransom for the encryption key. Cryptomining malware performs mathematical calculations in the background, thus stealing the processing power and network traffic of your machine.

When the **Antiransomware Protection** service is on, it monitors in real time the processes running on your computer. When it detects a third-party process that tries to encrypt your files or mine cryptocurrency, the service informs you about it and asks if you want to allow the process to continue or to block the process.

To allow the process to continue the activity, click **Trust**. If you are not sure if the process is safe and legal, we recommend that you click **Quarantine**. After this, the process will be added to **Quarantine** and blocked from any activities.

After blocking a process, we recommend that you check if your files have been encrypted or corrupted in any way. If they are, click **Recover modified files**. Acronis True Image for BIWIN will search the following locations for the latest file versions to recover.

- Temporary file copies that were preliminarily created during the process verification
- Local backups
- Cloud backups

If Acronis True Image for BIWIN finds a good temporary copy, the file is restored from that copy. If temporary file copies are not suitable for restore, Acronis True Image for BIWIN searches for backup copies locally and in the cloud, compares the creation dates of the copies found in both locations, and restores your file from the latest available non-corrupt copy.

Note *Acronis True Image for BIWIN does not support file recovery from password-protected backups.*

To configure Acronis True Image for BIWIN to automatically recover files after blocking a process, select the **Automatically recover files after blocking a process** check box in the Active Protection settings. See Configuring Active Protection (p. 55).

Related topics

Configuring Active Protection 55

6.1.1 Configuring Active Protection

1. Click **Protection** on Acronis True Image for BIWIN the side bar, then click **Settings**, and go to the **Active Protection** tab.
2. Switch on the **Antiransomware Protection** toggle to protect your computer from potentially harmful applications and processes that run in the background.
3. Select the options that you want to enable.

- **Automatically recover files after blocking a process** – Though a process was blocked, there is still a possibility that your files were modified. If this check box is selected, Acronis True Image for BIWIN recovers the files as follows.

Acronis True Image for BIWIN searches the following locations for the latest file versions to recover.

- Temporary file copies that were preliminarily created during the process verification
- Local backups
- Cloud backups

If Acronis True Image for BIWIN finds a good temporary copy, the file is restored from that copy. If temporary file copies are not suitable for restore, Acronis True Image for BIWIN searches for backup copies locally and in the cloud, compares the creation dates of the copies found in both locations, and restores your file from the latest available unmodified copy.

Note *Acronis True Image for BIWIN does not support file recovery from password-protected backups.*

- **Protect backup files from ransomware** – Acronis True Image for BIWIN will protect its own processes and your backups and archives from ransomware.
 - **Protect network shares and NAS** – Acronis True Image for BIWIN will monitor and protect the network shares and NAS devices you have access to. You can also specify a recovery location for files affected by a ransomware attack.
 - **Protect your computer from illicit cryptomining** – Select this check box to defend your computer from cryptomining malware.
4. Click **OK**.

6.2 Managing files in Quarantine

Based on your settings, Active protection can move blocked files to quarantine. Quarantine is a special storage that is used to isolate infected and suspected files from your computer and data. When you place an application file in quarantine, the risk of potential harmful actions from the blocked application is minimized.

By default, files are kept for 30 days in quarantine and then deleted from your PC. You can review the files in quarantine and decide whether to keep or delete them before that period expires. You can also change the default period to keep files in quarantine.

To restore or delete files from quarantine:

1. On the **Protection** dashboard, click **Quarantine**.
2. In the Quarantine list, select an item.
 - To return the item to its original location, click **Restore**.
 - To delete an item, click **Delete from PC**.
3. Click **Close**.

To setup the period for automatic deletion of files from the quarantine:

1. On the **Protection** dashboard, click **Settings**, and click the **Advanced** tab.
2. In the **Quarantine** section, locate the **Delete quarantined items from this PC after** spin-box, and select the number of days to keep items in quarantine.
3. Click **OK**.

6.3 Configuring Protection exclusions

Active protection uses the definitions from the Protection database to determine potential threats. If you trust some executable files and folders, you can add them to the Protection exclusions list, so Acronis True Image for BIWIN will skip them during scanning.

To add a file or folder to the Protection exclusions list:

1. On the **Protection** dashboard click **Protection exclusions**.
2. From the **Add exclusion** menu, select what you want to exclude.
 - **Add file** – to exclude executable or other files from scanning.
 - **Add folder** – to exclude folders from scanning.
3. Browse for the item that you want to exclude and click **Open**.
4. Add another item to exclude or click **Save** to update the list.

To remove files or folders from the Protection exclusions list:

1. On the **Protection** dashboard click **Protection exclusions**.
2. In the list of protection exclusions, select the check boxes for the items that you want to remove and click **Remove**.
3. Click **Save** to update the list.

To configure protection exclusions for Web filtering, see *Configuring Active Protection* (p. 55).

7 Disk cloning and migration

This operation copies the entire contents of one disk drive to another disk drive. This may be necessary, for example, when you want to clone your operating system, applications, and data to a new, larger capacity disk. You can do it two ways:

- Use the Clone disk utility (p. 57).
- Back up your old disk drive, and then recover it to the new one (p. 39).


In this section

General information.....	57
Preparing for migration.....	61

7.1 General information

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 new disk in the computer. If your computer doesn't have a bay for another hard disk, you can temporarily install it in place of your CD drive. 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.

 *Warning! If you clone a disk with Windows to an external USB hard drive, you will not be able to boot from it. Windows does not support booting from external USB hard drives. Please clone to internal SSD or HDD instead.*

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.

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.

We strongly recommend that you create a backup of the entire original disk as a safety precaution. It could be your data saver if something goes wrong with your original hard disk during cloning. For information on how to create such a backup see [Backing up partitions and disks](#) (p. 23). After creating the backup, make sure that you validate it.

To clone a disk:

- Click **Clone disk** on the **Tools and utilities** tab of the Home screen.
- Follow the **Disk Clone Wizard** steps.

7.1.1 Clone Disk wizard

Before you start, we recommend that you read general information about Disk cloning utility (p. 57).

To clone a disk:

1. On the sidebar, click **Tools**, and then click **Clone disk**.
2. On the **Clone Mode** step, choose a transfer mode.

- **Automatic**—Recommended in most cases.
- **Manual**—Manual mode will provide more data transfer flexibility. 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.

3. On the **Source Disk** step, select the disk that you want to clone.

Acronis True Image for BIWIN does not support cloning of dynamic disks.

4. On the **Destination Disk** step, select the destination disk for the cloned data.
If the selected destination disk contains partitions, you will need to confirm deletion of the partitions. Note that the real data destruction will be performed only when you click **Proceed** on the last step of the wizard.

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

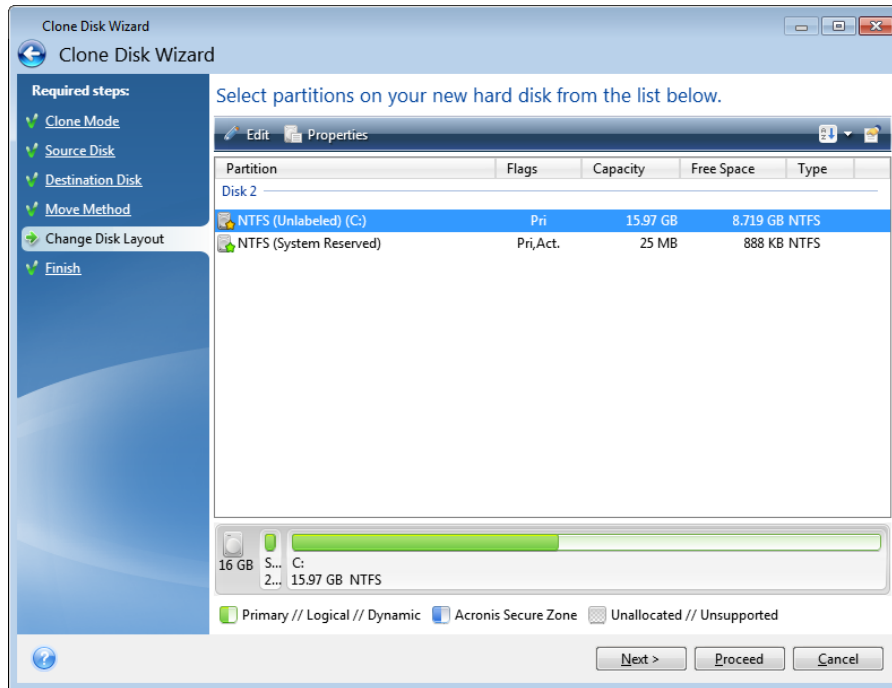
5. [This step is only available if the source disk has an OS installed]. On the **Disk Usage** step, select how you are going to use the clone.
 - **To replace a disk on this machine**—the system disk data will be copied, and the clone will be bootable. Use this clone for replacing the system disk with a new one on this PC.
 - **To use on another machine**—the system disk data will be copied, and the clone will be bootable. Use this clone to transfer all the data to another PC on a bootable disk.
 - **To use as a data disk**—the disk data will be copied. Use this clone as a non-bootable data drive.
6. [This step is only available in the manual cloning mode]. On the **Move method** step, choose a data move method.
 - **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.
 - **Proportional**—the new disk space will be proportionally distributed between cloned partitions.
 - **Manual**—you will specify a new size and other parameters yourself.
7. [This step is only available in the manual cloning mode]. On the **Change disk layout** step, you can edit settings of the partitions that will be created on the destination disk. Refer to Manual partitioning (p. 59) for details.
8. [Optional step] On the **What to exclude** step, you can specify files and folders that you do not want to clone. Refer to Excluding items from cloning (p. 60) for details.
9. On the **Finish** step, ensure that the configured settings suit your needs, and then click **Proceed**.

If the cloning operation is stopped for some reason, you will have to configure and start the procedure again. You will not lose your data, because Acronis True Image does not alter the original disk and data stored on it during cloning.

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. By default, Acronis True Image for BIWIN shuts down the computer after the clone process finishes. This enables you to change the position of master/subordinate jumpers and remove one of the hard drives.

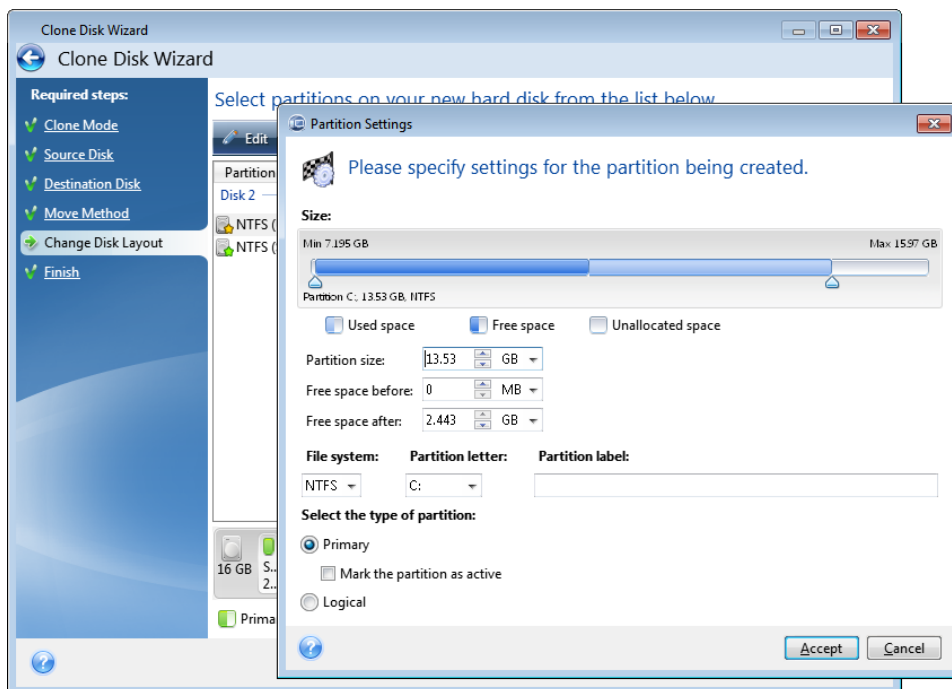
7.1.2 Manual partitioning

The manual transfer method enables you to resize partitions on the new disk. By default, the program resizes them proportionally.



To edit a partition:

1. Select the partition, and then click **Edit**. This will open the Partition Settings window.




2. Specify the following settings for the partition:
 - Size and position
 - File system

- Partition type (available only for MBR disks)
- Partition letter and label

Refer to Partition settings (p. 78) for details.

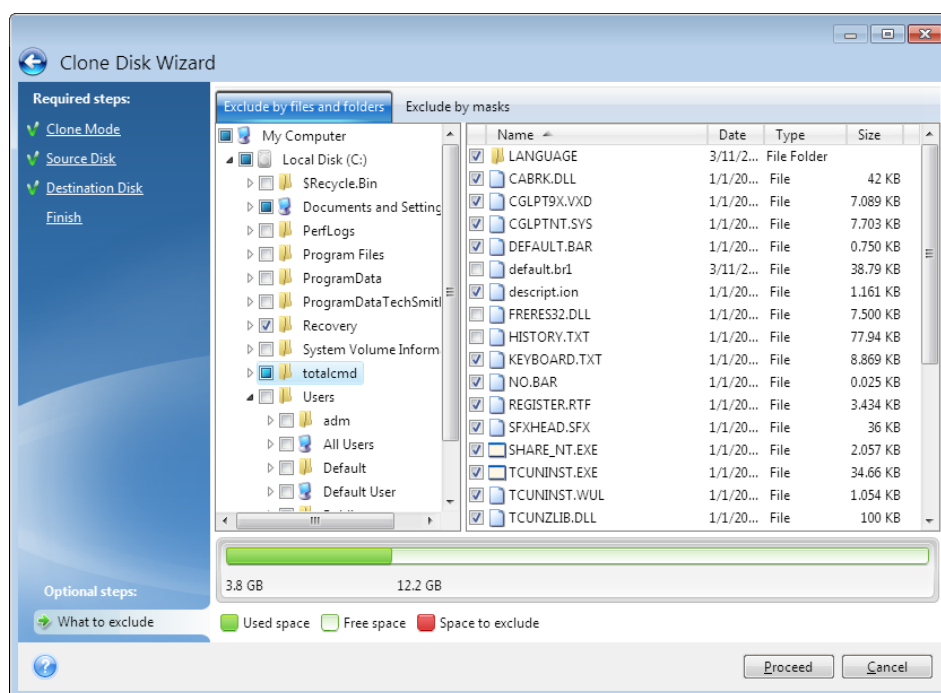
3. Click **Accept**.

 **Be careful!** Clicking any previous wizard step on the sidebar in this window will reset all size and location changes that you've selected, so you will have to specify them again.

7.1.3 Excluding items from cloning

If you do not want to clone specific files from a source disk (for example, when your target disk is smaller than the source one), you can opt to exclude them in the **What to exclude** step.

We do not recommend excluding hidden and system files when cloning your system partition.



You have two ways to exclude files and folders:

- **Exclude by files and folders** - this tab allows you to select specific files and folders from the folder tree.
- **Exclude by masks** - this tab allows you to exclude a group of files by mask or an individual file by name or path.

To add an exclusion criterion, click **Add**, type a file name, a path or a mask, and then click **OK**. You can add as many files and masks as you like.

Examples of exclusion criteria:

- You can enter explicit file names:
 - *file.ext* - all such files will be excluded from cloning.
 - *C:\file.ext* - the file.ext file on the C: disk will be excluded.
- You can use wildcard characters (* and ?):
 - **.ext* - all files with a .ext extension will be excluded.

- *??name.ext* - all files with a .ext extension, having six letters in their names (starting with any two symbols (??) and ending with *name*), will be excluded.
- You can enter path to a folder:
 - *C:\my pictures - my pictures* folder on the C: disk will be excluded.

You can edit and remove exclusion criteria using the corresponding buttons on the right pane.

7.2 Preparing for migration

Solid state disks have become quite common. Many users decide to replace their system hard disk with an SSD to enhance the disk system performance. Such a replacement may raise a number of questions.

First of all, make sure that Acronis True Image for BIWIN detects your new SSD both in Windows and under the Acronis rescue media. If there is a problem, see [What to do if Acronis True Image for BIWIN does not recognize your SSD](#) (p. 62).

SSD size

Because SSDs are still somewhat expensive, the size of your new SSD will usually be less than that of your old hard disk. This may cause a problem if your hard disk contains the operating system, programs and data.

We presuppose that before purchasing the SSD you estimated the approximate space occupied by your operating system and applications and that you selected an SSD that has a reasonable reserve capacity.

If the occupied space on your old hard disk exceeds the size of your SSD, you will need to free up space on the system disk to make migration possible.

SSD alignment

Another question concerns the alignment of SSDs. To get the optimum performance from an SSD and to prolong its life, the partition offset must meet certain criteria. In most cases you do not need to check or manually fix the alignment, the program will do it automatically.

In any event, we recommend that you perform one of the following:

- Create the backup you are going to use for migration in disk mode. In other words, back up the source disk entirely, not just the system partition.
- Make sure the destination SSD does not contain partitions (the disk space is unallocated). Note that if your SSD is new and has never been used before, it does not contain partitions.

Which migration method to choose

If your system disk consists of a single partition (not counting the hidden System Reserved partition existing in many installations of Windows 7), you can try to migrate to the SSD using the Clone tool. For more information see [Cloning a hard disk](#) (p. 57).

However, we recommend to use the backup and recovery method in most cases. This method provides more flexibility and control over migration. See [Migrating to an SSD using the backup and recovery method](#) (p. 63).

7.2.1 What to do if Acronis True Image for BIWIN does not recognize your SSD

Sometimes Acronis True Image for BIWIN may not recognize an SSD.

In such a case, check whether the SSD is recognized in BIOS.

If the BIOS of your computer does not show the SSD, verify that the power and data cables are properly connected. You may also try to update the BIOS and SATA drivers. If these suggestions do not help, contact the Support of your SSD manufacturer.

If the BIOS of your computer does show the SSD, you can try the following procedure:

Depending on your operating system, type **cmd** in the Search field or in the Run field, and then press **Enter**.

At the command line prompt type:

diskpart

list disk The screen will show the disks connected to your computer. Find out the disk number for your SSD. Use its size as the reference.

select disk N Here N is the disk number of your SSD.

clean This operation removes all information from the SSD and overwrites the MBR with the default one.

exit

exit

Start Acronis True Image for BIWIN and check whether it detects the SSD. If it detects the SSD, use the Add new disk tool to create a single partition on the disk occupying the entire disk space. When creating a partition, check that the free space before partition is 1 MB. For more information, see Adding a new hard disk (p. 75).

The next step is to check whether your Acronis bootable media recognizes the SSD.

1. Boot from the Acronis bootable media.
2. Select **Tools & Utilities -> Add New Disk** in the main menu and the **Disk selection** screen will show the information about all hard disks in your system. Use this for checking whether the SSD is detected in the recovery environment.
3. If the screen shows your SSD, just click **Cancel**.

If the bootable media does not recognize the SSD and the SSD controller mode is AHCI, you can try to change the mode to IDE (or ATA in some BIOS brands) and see whether this solves the problem.

Attention! Do not start Windows after changing the mode; it may result in serious system problems. You must return the mode to AHCI before starting Windows.

If after changing the mode the bootable media detects the SSD, you may use the following procedure for recovery or cloning under bootable media:

1. Shut down the computer.
2. Boot to BIOS, change the mode from AHCI to IDE (or ATA in some BIOS brands).
3. Boot from Acronis bootable media.

4. Recover or clone the disk.
5. Boot to BIOS and change IDE back to AHCI.
6. Start Windows.

What to do if the above suggestions do not help

You can try to create a WinPE-based media. This may provide the necessary drivers. For more information, see *Creating Acronis bootable media* (p. 65).

7.2.2 Migrating to SSD using the backup and recovery method

You can use the following procedure for all supported operating systems. First, let's consider a simple case: your system disk consists of a single partition. Note that for Windows 7, the system disk usually has a hidden System Reserved partition.

We recommend that you migrate your system to an empty SSD that does not contain partitions (the disk space is unallocated). Note that if your SSD is new and has never been used before, it does not contain partitions.

To migrate your system to an SSD:

1. Start Acronis True Image for BIWIN.
2. Create Acronis rescue media, if you do not have it yet. To do this, in the **Tools** section, click **Create bootable media** and follow the instructions on the screen.
3. Back up your entire system drive (in the disk backup mode) to a hard disk other than your system hard disk and the SSD.
4. Switch off the computer and remove your system hard disk.
5. Mount the SSD into the slot where the hard disk was.

For some SSD brands you may need to insert the SSD into a PCI Express slot.

6. Boot from your Acronis rescue media.
7. Validate the backup to make sure that it can be used for recovery. To do this, click **Recovery** on the left pane and select the backup. Right-click, select **Validate Archive** in the shortcut menu and then click **Proceed**.
8. After the validation finishes, right-click the backup and select **Recover** in the shortcut menu.
9. Choose **Recover whole disks and partitions** at the Recovery method step and then click **Next**.
10. Select the system disk at the What to recover step.
11. Click **New location** and then select the SSD as the new location for your system disk, then click **Accept**.
12. At the next step click **Proceed** to start recovery.
13. After the recovery is complete, exit the standalone version of Acronis True Image for BIWIN.
14. Try to boot from the SSD and then make sure that Windows and applications work correctly.

If your system hard disk also contains a hidden recovery or diagnostic partition, as is quite often the case with notebooks, the procedure will differ. You will usually need to resize the partitions manually during recovery to the SSD. For instructions see *Recovering a disk with a hidden partition* (p. 39).

8 Tools

Acronis Tools and utilities include protection tools and mounting tools.

Protection tools

- **Acronis Startup Recovery Manager**
Allows you to start Acronis True Image for BIWIN without loading the operating system by pressing F11 at boot time before the operating system starts.
- **Rescue Media Builder** (p. 64)
Allows you to create a bootable rescue media with Acronis products (or their specified components) installed on your computer.

Image mounting

- **Mount image** (p. 79)
With this tool you can explore a previously created image. You will be able to assign temporary drive letters to the partition images and easily access these images as ordinary, logical drives.
- **Unmount image** (p. 80)
With this tool you can unmount the temporary logical drives you have created to explore an image.

8.1 Creating bootable rescue media

You can run Acronis True Image for BIWIN from an emergency boot media 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 by imaging the disk in the sector-by-sector mode. To do so, you need bootable media that has a copy of the standalone Acronis True Image for BIWIN version installed on it.

How you can obtain bootable media:

- Use the installation CD of the boxed product.
- Make a media bootable with Acronis Media Builder (p. 64):
 - Blank CD
 - Blank DVD
 - USB flash drive
Note: The data it may contain will not be modified.
 - Create an .iso image file to burn it afterwards onto a CD or DVD.

8.1.1 Acronis Media Builder

Acronis Media Builder allows you to make a USB flash drive or a blank CD/DVD bootable. In case Windows cannot start, use the bootable media to run a standalone version of Acronis True Image and recover your computer.

You can create several types of bootable media:

- **Acronis bootable rescue media**
This type is recommended for most users.

Notes

- If you use non-optical media, the media must have FAT16 or FAT32 file system.
- If Acronis Media Builder does not recognize your USB flash drive, you can try using the procedure described in an Acronis Knowledge Base article at <http://kb.acronis.com/content/1526>.
- When booting from the Rescue Media, you cannot perform backups to disks or partitions with Ext2/Ext3/Ext4, ReiserFS, and Linux SWAP file systems.
- When booting from the rescue media and using a standalone version of Acronis True Image you cannot recover files and folders encrypted with use of the encryption available in Windows XP and later operating systems. On the other hand, backups encrypted using the Acronis True Image encryption feature can be recovered.

8.1.1.1 Creating bootable media

To create bootable media:

1. Plug in a USB flash drive, or insert a blank CD or DVD.
2. Start Acronis True Image for BIWIN.
3. In the **Tools** section, click **Rescue Media Builder**.
4. Choose a media type that you want to create. Refer to Acronis Media Builder (p. 64) for details.
5. Select a destination for the media:
 - **CD**
 - **DVD**
 - **USB flash drive** (available only for Acronis bootable rescue media)
If your drive has an unsupported file system, Acronis True Image will suggest formatting it to FAT file system.

Warning! *Formatting permanently erases all data on a disk.*

 - **ISO image file**
You will need to specify the .iso file name and the destination folder.
When the .iso file is created, you can burn it onto a CD or DVD. For example, in Windows 7 and later, you can do this using a built-in burning tool. In Windows Explorer, double-click the created ISO image file, and then click **Burn**.
6. Click **Proceed**.

8.1.1.2 Bootable media startup parameters

Here, 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.). 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 the product's support team.

To add a startup parameter

- Enter a command into the **Parameters** field.
- Having specified the startup parameters, click **Next** to continue.

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.

8.1.2 Making sure that your rescue media can be used when needed

To maximize the chances of your computer's recovery, you must test that your computer can boot from the rescue media. In addition, you must check that the rescue media recognizes all your computer's devices, such as the hard drives, the mouse, the keyboard, and network adapter.

To test the rescue media

If you use external drives for storing your backups, you must attach the drives before booting from the rescue CD. Otherwise, the program might not detect them.

1. Configure your computer to enable booting from the rescue media. Then, make your rescue media device (CD-ROM/DVD-ROM drive or USB stick) the first boot device. See Arranging boot order in BIOS (p. 47).
2. If you have a rescue CD, press any key to start booting from the CD, when you see the prompt "Press any key to boot from CD". If you do not press a key within five seconds, you will need to restart the computer.
3. After the boot menu appears, choose **Acronis True Image for BIWIN**.

If your wireless mouse does not work, try to replace it with a wired one. The same recommendation applies to the keyboard.

If you do not have a spare mouse or keyboard, contact the support. They will build a custom rescue CD that will have drivers for your models of the mouse and keyboard. Please be aware that finding the appropriate drivers and making the custom rescue CD may take some time. Furthermore, this may be impossible for some models.

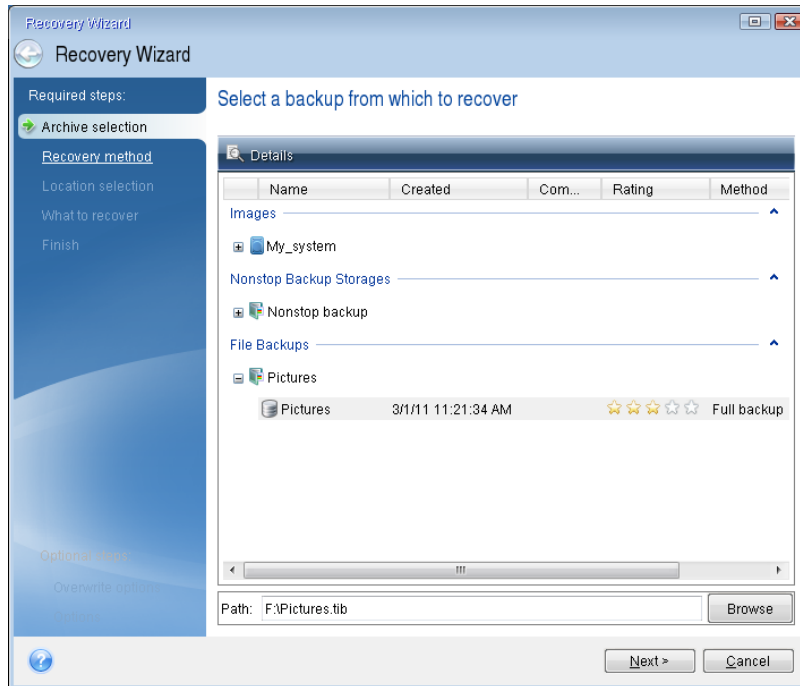
4. When the program starts, we recommend you try recovering some files from your backup. A test recovery allows you to make sure that your rescue CD can be used for recovery. In addition, you will check that the program detects all the hard drives you have in your system.

If you have a spare hard drive, we strongly recommend that you try a test recovery of your system partition to this hard drive.

How to test recovery, as well as check the drives and network adapter

1. Start Recovery Wizard by clicking **Recovery** -> **Disk Recovery** on the toolbar.

2. Select a backup at the **Archive location** step and then click **Next**.

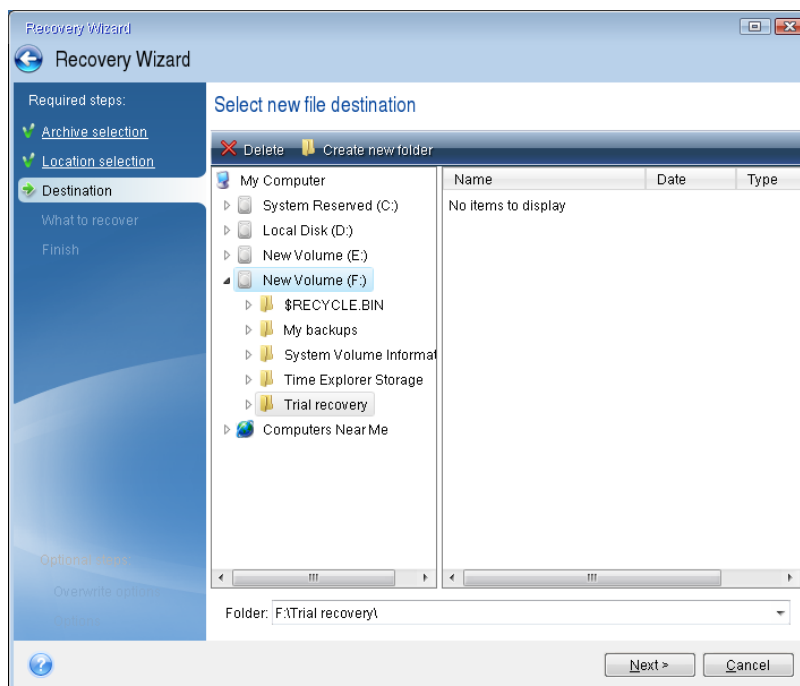


3. When recovering files with the rescue CD you are able to select only a new location for the files to be recovered. Therefore just click **Next** at the **Location selection** step.
4. After the **Destination** window opens, check that all your drives are shown under **My Computer**.

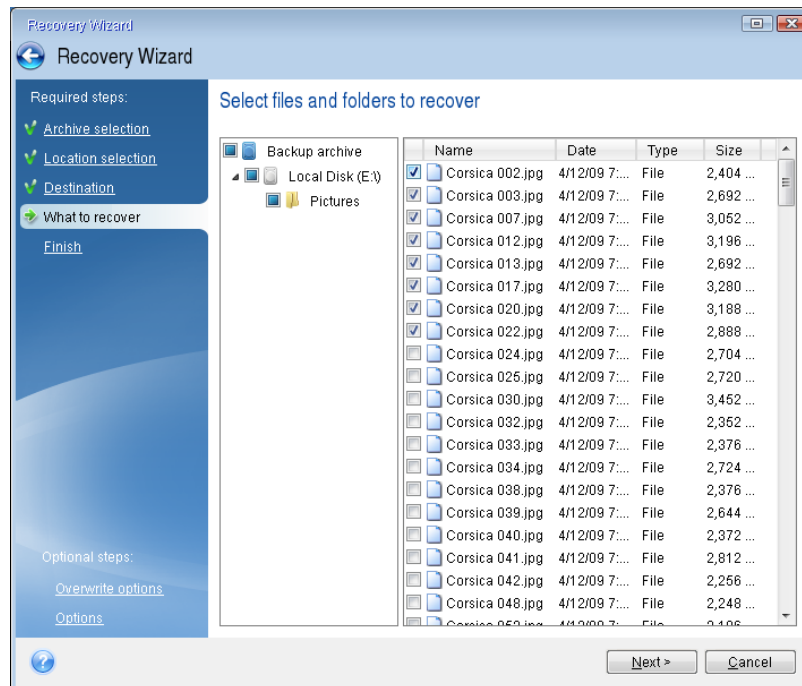
If you store your backups on the network, you should also check that you can access the network.

*If no computers are visible on the network, but the **Computers Near Me** icon is found under **My Computer**, specify network settings manually. To do this, open 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 provided with Acronis True Image for BIWIN.*



5. Select the destination for the files and then click Next.
6. Select several files for recovery by selecting their check boxes and then click **Next**.



7. Click **Proceed** on the Summary window to start recovery.
8. After the recovery finishes, exit the standalone Acronis True Image.

Now you can be reasonably sure that your rescue CD will help you when needed.

8.1.2.1 Selecting video mode when booting from the bootable media

When booting from the bootable 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 bootable media. When the boot menu appears, hover the mouse over **Acronis True Image for BIWIN** 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 for BIWIN** in the boot menu to continue booting from the bootable media. To see the available video modes, press the Enter key when the appropriate message appears.

- 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).

```

333 1024x768x16 VESA      334 1152x864x16 VESA      335 1280x960x16 VESA
336 1280x1024x16 VESA    337 1400x1050x16 VESA    338 1600x1200x16 VESA
339 1792x1344x16 VESA    33A 1856x1392x16 VESA    33B 1920x1440x16 VESA
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    34A 1366x768x8 VESA
34B 1366x768x16 VESA     34C 1366x768x32 VESA     34D 1680x1050x8 VESA
34E 1680x1050x16 VESA    34F 1680x1050x32 VESA    350 1920x1200x8 VESA
351 1920x1200x16 VESA    352 1920x1200x32 VESA    353 2048x1536x8 VESA
354 2048x1536x16 VESA    355 2048x1536x32 VESA    356 320x240x8 VESA
357 320x240x16 VESA      358 320x240x32 VESA      359 400x300x8 VESA
35A 400x300x16 VESA      35B 400x300x32 VESA      35C 512x384x8 VESA
35D 512x384x16 VESA      35E 512x384x32 VESA      35F 854x480x8 VESA
360 854x480x16 VESA      361 854x480x32 VESA      362 1280x720x8 VESA
363 1280x720x16 VESA     364 1280x720x32 VESA     365 1920x1080x8 VESA
366 1920x1080x16 VESA    367 1920x1080x32 VESA    368 1280x800x8 VESA
369 1280x800x16 VESA     36A 1280x800x32 VESA     36B 1440x900x8 VESA
36C 1440x900x16 VESA     36D 1440x900x32 VESA     36E 720x480x8 VESA
36F 720x480x16 VESA      370 720x480x32 VESA      371 720x576x8 VESA
372 720x576x16 VESA      373 720x576x32 VESA      374 800x480x8 VESA
375 800x480x16 VESA      376 800x480x32 VESA      377 1280x768x8 VESA
378 1280x768x16 VESA     379 1280x768x32 VESA
Enter a video mode or "scan" to scan for additional modes: _

```

- Wait until Acronis True Image for BIWIN 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 for BIWIN and repeat the above procedure.

After you find the optimal video mode for your hardware, you can create a new bootable 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.

8.2 Security and Privacy Tools

Acronis True Image for BIWIN contains the utility for secure destruction of data on an entire hard disk drive, and individual partitions.

When replacing your old hard drive with a new, higher-capacity one, you may accidentally leave personal and confidential information on the old disk. This information could be retrieved even if you have reformatted the disk.

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.

The data destruction methods are described in detail in Hard Disk Wiping methods (p. 74) of this guide.

In this section

Acronis DriveCleanser	71
Hard Disk Wiping methods	74

8.2.1 Acronis DriveCleanser

Acronis DriveCleanser allows you to permanently destroy all data on selected hard disks and partitions. For the destruction, you can use one of the preset algorithms or create your own. Refer to Algorithm selection (p. 72) for details.

Why do I need it?

When you format your old hard drive before throwing it away, the information is not destroyed permanently and it can still be retrieved. This is a way that your personal information can end up in the wrong hands. To prevent this, we recommend that you use Acronis DriveCleanser when you:

- Replace your old hard drive with a new one and do not plan to use the old drive any more.
- Give your old hard drive to your relative or friend.
- Sell your old hard drive.

How to use Acronis DriveCleanser


To permanently destroy data on your disk:


1. Click the **Start** button → **Acronis** (product folder) → **True Image** → **Tools and Utilities** → **DriveCleanser**.
The Acronis DriveCleanser wizard opens.
2. On the **Source selection** step, select the disks and partitions that you want to wipe. Refer to Source selection (p. 71) for details.
3. On the **Algorithm selection** step, select an algorithm that you want to use for the data destruction. Refer to Algorithm selection (p. 72) for details.
4. [optional step] You can create your own algorithm. Refer to Creating custom algorithm for details.
5. [optional step] On the **Post-wiping actions** step, choose what to do with the partitions and disk when the data destruction is complete. Refer to Post-wiping actions (p. 74) for details.
6. On the **Finish** step, ensure that the configured settings are correct. To start the process, select the **Wipe the selected partitions irreversibly** check box, and then click **Proceed**.

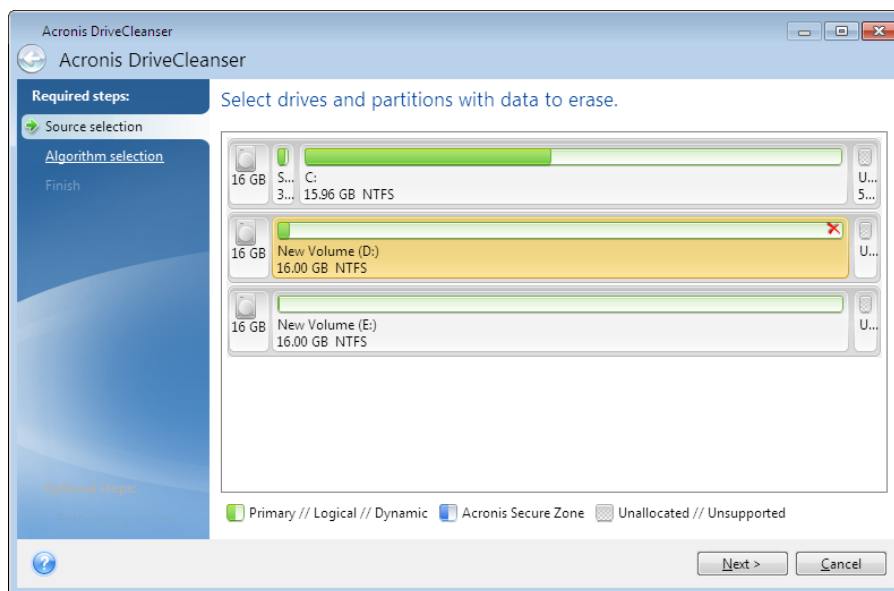
Be aware that, depending on the total size of selected partitions and the selected data destruction algorithm, the data destruction may take many hours.

8.2.1.1 Source selection

On the **Source selection** step, select partitions and disks where you want to destroy data:

- To select partitions, click the corresponding rectangles. The red mark () indicates that the partition is selected.

- To select an entire hard disk, click the disk icon ().

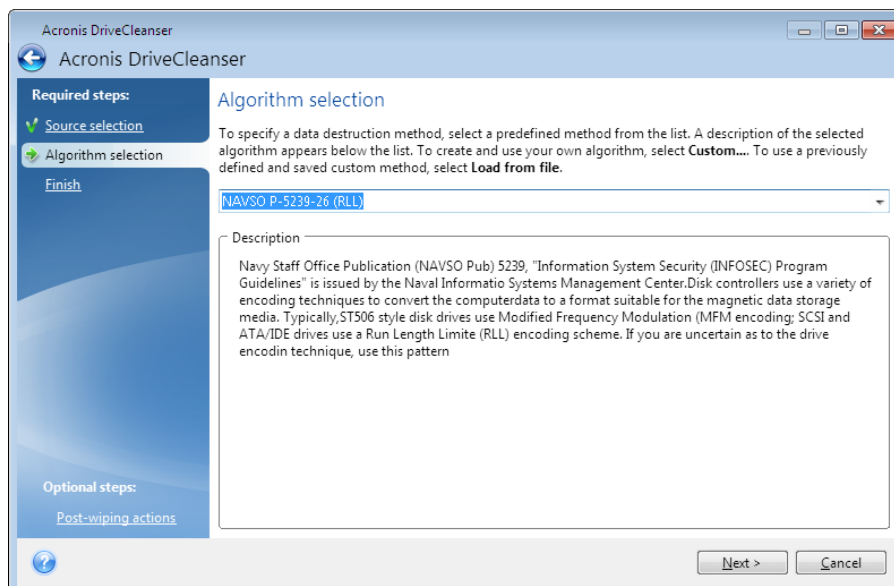


Acronis DriveCleanser cannot wipe partitions on dynamic and GPT disks, so they will not be shown.

8.2.1.2 Algorithm selection

On the **Algorithm selection** step, perform one of the following:

- To use one of the preset algorithms, select the desired algorithm. Refer to Hard Disk Wiping Methods (p. 74) for details.
- [For advanced users only] To create a custom algorithm, select **Custom**. Then continue creating on the **Algorithm definition** step. Afterwards, you will be able to save the created algorithm to a file with *.alg extension.
- To use a previously saved custom algorithm, select **Load from file** and select the file containing your algorithm.



Creating custom algorithm

Algorithm definition

The **Algorithm definition** step shows you a template of the future algorithm.

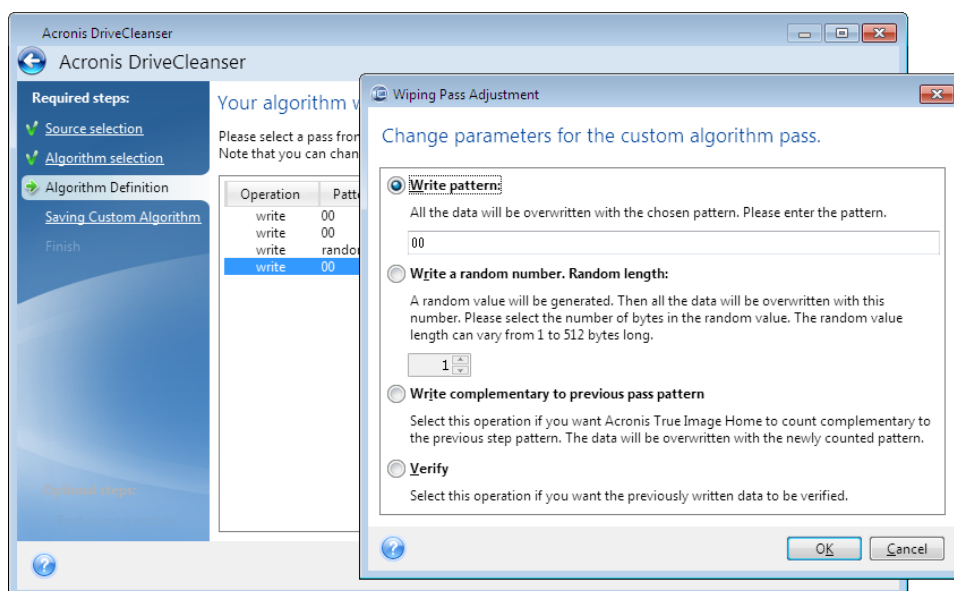
The table has the following legend:

- The first column contains the type of operation (to write a symbol to disk; and to verify written).
- The second column contains the pattern of data to be written to disk.

Each line defines an operation that will be performed during a pass. To create your algorithm, add as many lines to the table that you think will be enough for secure data destruction.

To add a new pass:

1. Click **Add**. The Wiping Pass Adjustment window opens.



2. Choose an option:

- **Write pattern**

Enter a hexadecimal value, for example, a value of this kind: 0x00, 0xAA, or 0xCD, etc. These values are 1 byte long, but they may be up to 512 bytes long. Except for such values, you may enter a random hexadecimal value of any length (up to 512 bytes).

If the binary value is represented by the 10001010 (0x8A) sequence, then the complementary binary value will be represented by the 01110101 (0x75) sequence.

- **Write a random number**

Specify the length of the random value in bytes.

- **Write complementary to previous pass pattern**

True Image adds a complementary value to the one written to disk during the previous pass.

- **Verify**

True Image verifies the values written to disk during the previous pass.

3. Click **OK**.

To edit an existing pass:

1. Select the corresponding line, and then click **Edit**.

The Wiping Pass Adjustment window opens.

Note: When you select several lines, the new settings will be applied to all of the selected passes.

2. Change the settings, and then click **OK**.

Saving algorithm to a file

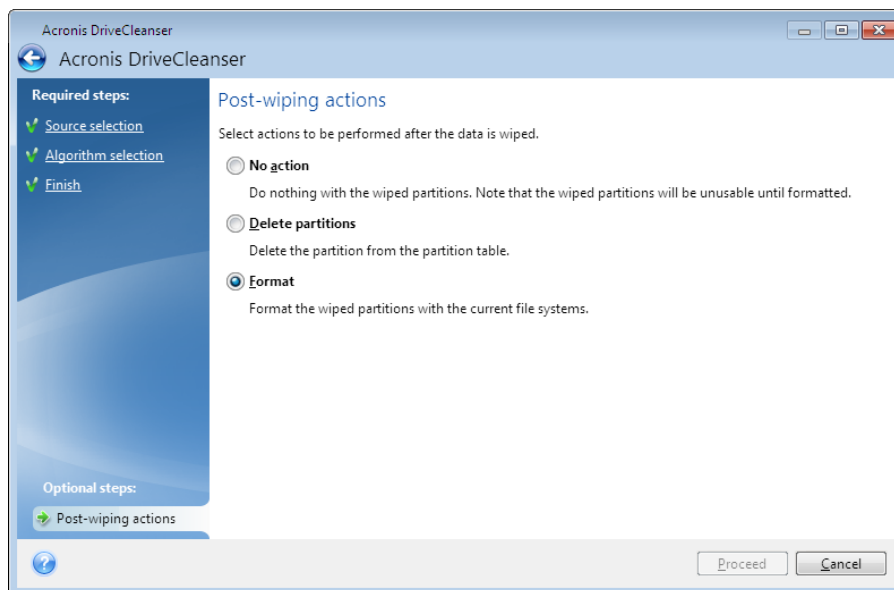
To save the created algorithm to a file in order to use this algorithm afterwards:

1. On the **Saving custom algorithm** step, select **Save to a file**, and then click **Next**.
2. In the window that opens, specify the file name and location, and then click **OK**.

8.2.1.3 Post-wiping actions

In the Post-wiping actions window, you can select actions to be performed on the partitions selected for data destruction. Acronis DriveCleanser offers you three options:

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



8.2.2 Hard Disk Wiping methods

What is the problem?

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.

Leakage mechanism

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.

Information wiping methods used by Acronis

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" at https://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html.

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.

8.3 Adding a new hard disk

If you do not have enough space for your data (e.g. family photos and videos), 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 disk drive than to clone one.

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

To add a new hard disk:

- Click the **Tools and utilities** tab and then click **Add new disk**
- Follow the Add new disk Wizard steps

If you use a 32-bit version of Windows XP, the wizard will not have the **Initialization options** step because this operating system does not support GPT disks.

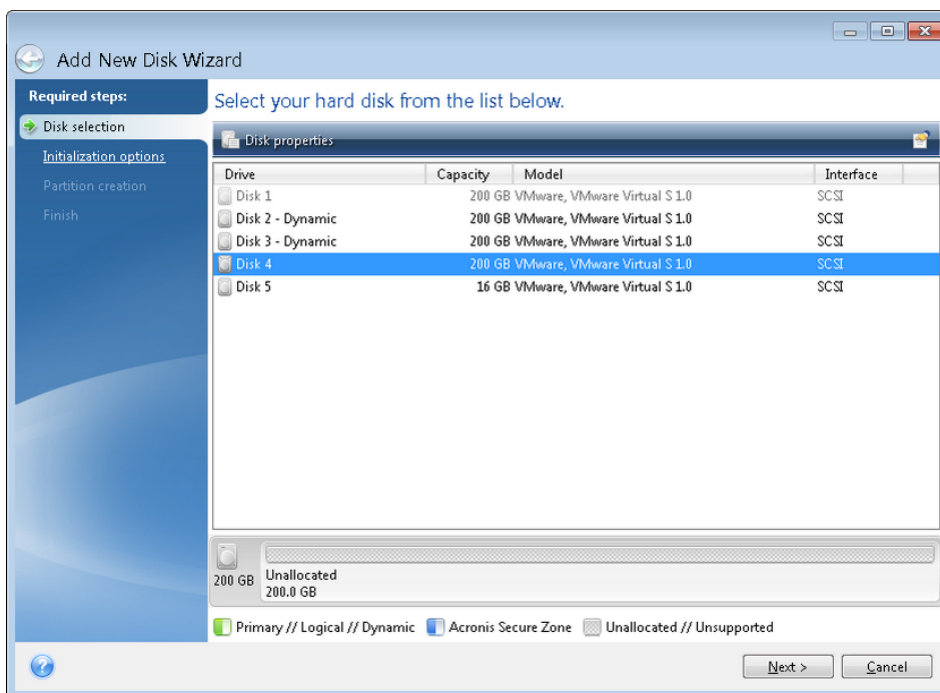
In this section

Selecting a hard disk	76
Selecting initialization method	77
Creating new partitions.....	77

8.3.1 Selecting a hard disk

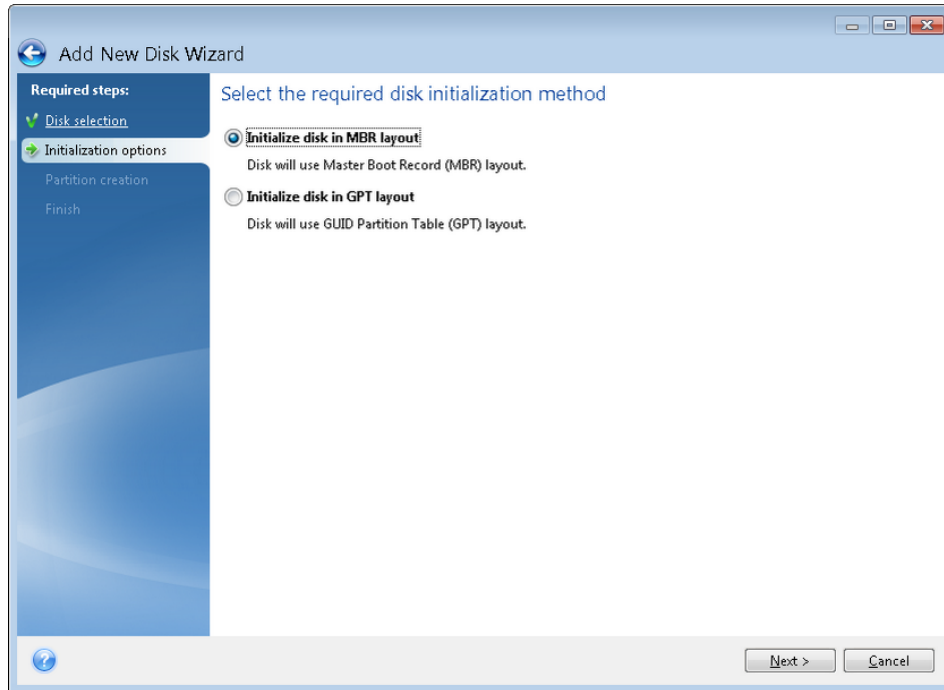
Select the disk that you have added to the computer. If you have added several disks, select one of them and click **Next** to continue. You can add the other disks later by restarting the Add New Disk Wizard.

If there are any partitions on the new disk, Acronis True Image for BIWIN will warn you that these partitions will be deleted.



8.3.2 Selecting initialization method

Acronis True Image for BIWIN supports both MBR and GPT partitioning. GUID Partition Table (GPT) is a new hard disk partitioning method providing advantages over the old MBR partitioning method. If your operating system supports GPT disks, you can select the new disk to be initialized as a GPT disk.



- To add a GPT disk, click **Initialize disk in GPT layout**.
- To add an MBR disk, click **Initialize disk in MBR layout**.

After selecting the required initialization method click **Next**.

8.3.3 Creating new partitions

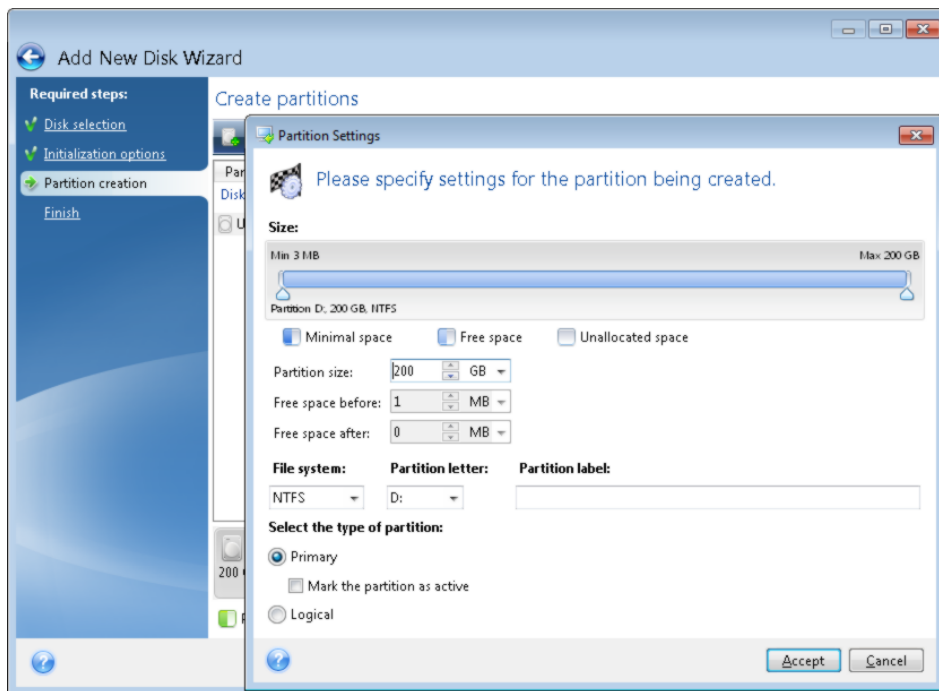
To use the space on a hard disk, it must be partitioned. Partitioning is the process of dividing the hard disk's space into logical divisions which are called partitions. Each partition may function as a separate disk with an assigned drive letter, its own file system, etc.

To create a new partition:

1. On the **Partition creation** step of the wizard, select the unallocated space, and then click **Create new partition**.
2. Specify the following settings for the partition being created:
 - Size and position
 - File system
 - Partition type (available only for MBR disks)
 - Partition letter and label

Refer to Partition settings (p. 78) for details.

3. Click **Accept**.



8.3.3.1 Partition settings

Size

To resize the partition, perform one of the following:

- Point to the partition border. When the pointer becomes a double-headed arrow, drag the pointer to enlarge or reduce the partition size.
- Type the desired partition size in the **Partition Size** field.

To relocate the partition, perform one of the following:

- Drag the partition to a new position.
- Type the desired size in either the **Free space before** or **Free space after** field.

When you create partitions, the program may reserve some unallocated space for system needs in front of the created partitions.

File System

You can either leave the partition unformatted, or choose between the following file system types:

- **NTFS** is a Windows NT, Windows 2000, Windows XP, Windows Vista, and Windows 7 native file system. Choose it if you use these operating systems. Note, that Windows 95/98/Me and DOS cannot access NTFS partitions.
- **FAT 32** is an improved 32-bit version of the FAT file system that supports volumes up to 2 TB.
- **FAT 16** is a DOS native file system. Most operating systems recognize it. However, if your disk drive is more than 4 GB, it is not possible to format it in FAT16.
- **Ext2** is a Linux native file system. It is fast enough, but it is not a journaling file system.
- **Ext3** – officially introduced with Red hat Linux version 7.2, Ext3 is a Linux journaling file system. It is forwards and backwards compatible with Linux Ext2. It has multiple journaling modes, as well as broad, cross platform compatibility in both 32-bit and 64-bit architectures.

- **Ext4** is a new Linux file system. It has improvements in comparison to ext3. It is fully backward compatible with ext2 and ext 3. However, ext3 has only partial forward compatibility with ext4.
- **ReiserFS** is a journaling file system for Linux. Generally it is more reliable and faster than Ext2. Choose it for your Linux data partition.
- **Linux Swap** is a swap partition for Linux. Choose it if you want to add more swap space using Linux.

Partition letter

Select a letter to be assigned to the partition. If you select **Auto**, the program assigns the first unused drive letter in alphabetical order.

Partition label

Partition label is a name, assigned to a partition so that you can easily recognize it. For example, a partition with an operating system could be called System, a data partition — Data, etc. Partition label is an optional attribute.

Partition type (these settings are available only for MBR disks)

You can define the new partition as primary or logical.

- **Primary** - choose this parameter if you are planning to boot from this partition. Otherwise, it is better to create a new partition as a logical drive. You can have only four primary partitions per drive, or three primary partitions and one extended partition.
Note: If you have several primary partitions, only one will be active at a time, the other primary partitions will be hidden and won't be seen by the OS.
 - **Mark the partition as active** - select this check box if you are planning to install an operating system on this partition.
- **Logical** - choose this parameter if you don't intend to install and start an operating system from the partition. A logical drive is part of a physical disk drive that has been partitioned and allocated as an independent unit, but functions as a separate drive.

8.4 Mounting an image

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

- A new disk appears in your system.
- You can view the image contents in Windows Explorer and other file managers.

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

You cannot mount a disk backup, if it is stored on an FTP server.

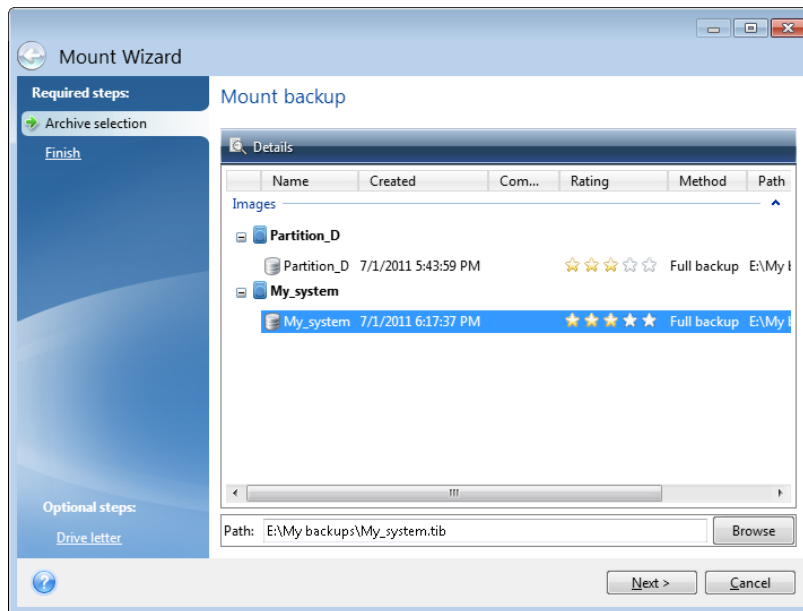
How to mount an image

1. In Windows Explorer, right-click the image file that you want to mount, and then click **Mount image**.

The Mount wizard opens.

2. Select the backup for mounting by its creation date/time. Thus, you can explore the data state at a certain moment.

Note that you cannot mount an image of the entire disk except in the case when the disk consists of one partition.



3. [optional step] On the **Drive letter** step, 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 clear the partition's check box.
4. Click **Proceed**.
5. After the image is connected, the program will run Windows Explorer, showing its contents.

8.5 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.

To unmount an image, perform one of the following:

- In Windows Explorer, right-click the disk icon and click **Unmount**.
- Restart or shut down your computer.

9 Troubleshooting

In this section

Acronis System Report.....	81
How to collect crash dumps.....	82

9.1 Acronis System Report

When you contact the product's support team, they usually need information about your system in order to resolve your problem. Sometimes getting the information is an inconvenient process and may take a long time. The Generate system report tool simplifies the procedure. It generates a system report containing all the necessary technical information and allows you to save the information to file. When it's necessary, you can attach the created file to your problem description and send it to the product's support team. This will simplify and speed up the search for a solution.

To generate a system report, perform one of the following:

- On the main program window click the question mark symbol, and select **Generate system report**.
- On the Windows **Start** menu, click **All Programs -> Acronis -> True Image -> Tools and Utilities -> Acronis System Report**.
- Press **CTRL+F7**. Note that you can use the key combination even when Acronis True Image for BIWIN is performing any other operation.

After the report is generated:

- To save the generated system report to file, click **Save** and in the opened window specify a location for the created file.
- To exit to the main program window without saving the report, click **Cancel**.
- When you create your bootable rescue media, the **Acronis System Report** tool is automatically placed on the media as a separate component. This component allows you to generate a system report when your computer cannot boot. After you boot from the media, you can generate the report without running Acronis True Image for BIWIN. Simply plug in a USB flash drive and click the **Acronis System Report** icon. The generated report is be saved on the USB flash drive.

Creating a system report from the command line prompt

1. Run Windows Command Processor (cmd.exe) as administrator.
2. Change the current directory to the Acronis True Image for BIWIN installation folder. To do so, enter:

```
cd C:\Program Files (x86)\Acronis\TrueImageHome
```

3. To create the system report file, enter:

```
SystemReport
```

File SystemReport.zip will be created in the current folder.

If you want to create the report file with a custom name, type the new name instead of <file name>:

```
SystemReport.exe /filename:<file name>
```

9.2 How to collect crash dumps

Because a crash of Acronis True Image for BIWIN or Windows can be caused by different reasons, each crash case must be investigated separately. Acronis Customer Central would appreciate if you could provide the following information:

If Acronis True Image for BIWIN crashes, please provide the following information:

1. A description of the exact sequence of steps performed before you encountered the issue.
2. A crash dump. For information on how to collect such a dump, see the Acronis Support Knowledge Base (KB) article at <https://kb.acronis.com/content/27931>.

If Acronis True Image for BIWIN causes a Windows crash:

1. A description of the exact sequence of steps performed before you encountered the issue.
2. A Windows dump file. For information on how to collect such a dump see the Acronis Support KB article at <https://kb.acronis.com/content/17639>.

If Acronis True Image for BIWIN hangs:

1. A description of the exact sequence of steps performed before you encountered the issue.
2. A userdump of the process. See the Acronis Support KB article at <https://kb.acronis.com/content/6265>.
3. The Procmon log. See the Acronis Support KB article at <https://kb.acronis.com/content/2295>.

If you cannot access the information, contact Acronis Customer Central for an FTP link for uploading files.

This information will speed up the process of finding a solution.

Copyright Statement

Copyright © Acronis International GmbH, 2003-2021. All rights reserved.

"Acronis", "Acronis Compute with Confidence", "Acronis Recovery Manager", "Acronis Secure Zone", "Acronis True Image", "Acronis Try&Decide", and the Acronis logo are trademarks of Acronis International GmbH.

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 <https://kb.acronis.com/content/7696>

Acronis patented technologies

Technologies, used in this product, are covered and protected by one or more U.S. Patent Numbers: 7,047,380; 7,246,211; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,383,327; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,836,053; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,941,510; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,074,276; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121; 8,850,060; 8,856,927; 8,996,830; 9,213,697; 9,400,886; 9,424,678; 9,436,558; 9,471,441; 9,501,234; and patent pending applications.

10 Glossary of Terms

B

Backup

1. The same as Backup operation (p. 84).
2. A set of backup versions created and managed by using backup settings. A backup can contain multiple backup versions created using full (p. 84) and incremental backup methods. Backup versions belonging to the same backup are usually stored in the same location.

Backup operation

An operation that creates a copy of the data that exists on a machine's hard disk for the purpose of recovering or reverting the data to a specified date and time.

Backup settings

A set of rules configured by a user when creating a new backup. The rules control the backup process. Later you can edit the backup settings to change or optimize the backup process.

Backup version

The result of a single backup operation (p. 84). Physically, it is a file or a set of files that contains a copy of the backed up data as of a specific date and time. Backup version of files created by Acronis True Image for BIWIN have a .tibx extension. The TIBX files resulting from consolidation of backup versions are also called backup versions.

Backup version chain

Sequence of minimum 2 backup versions (p. 84) that consist of the first full backup version and the subsequent one or more incremental versions. Backup version chain continues till the next full backup version (if any).

Bootable media

A physical media (CD, DVD, USB flash drive or other media supported by a machine BIOS as a boot device) that contains standalone version of Acronis True Image for BIWIN.

Bootable media is most often used to:

- recover an operating system that cannot start
- access and back up the data that has survived in a corrupted system
- deploy an operating system on bare metal
- back up sector-by-sector a disk that has an unsupported file system

D

Disk backup (Image)

A backup (p. 84) that contains a sector-based copy of a disk or a partition in packaged form. Normally, only sectors that contain data are copied. Acronis True Image for BIWIN provides an option to take a raw image, that is, copy all the disk sectors, which enables imaging of unsupported file systems.

F

Full backup

1. A backup method that is used to save all the data selected to back up.
2. A backup process that creates a full backup version (p. 84).

Full backup version

A self-sufficient backup version (p. 84) containing all data chosen for backup. You do not need access to any other backup version to recover the data from a full backup version.

I

Image

The same as Disk backup (p. 84).

R

Recovery

Recovery is a process of returning of a corrupted data to a previous normal state from a backup (p. 84).

V

Validation

An operation that checks whether you will be able to recover data from a particular backup version (p. 84).

When you select for validation...

- a full backup version (p. 84) - the program validates the full backup version only.
- an incremental backup version - the program validates the initial full backup version, the selected incremental backup version, and the whole chain (if any) of backup versions to the selected incremental backup version.