



# Acronis True Image WD Edition

# Table of contents

<b>1</b>	<b>Introduction .....</b>	<b>4</b>
1.1	What is Acronis True Image WD Edition? .....	4
1.2	System requirements and supported media.....	4
1.2.1	Minimum system requirements.....	4
1.2.2	Supported operating systems.....	4
1.2.3	Supported file systems .....	5
1.2.4	Supported storage media .....	5
1.3	Technical Support .....	5
<b>2</b>	<b>Basic concepts .....</b>	<b>6</b>
2.1	Acronis True Image WD Edition basic concepts .....	6
2.2	The difference between file backups and disk/partition images .....	7
2.3	Full, incremental and differential backups.....	8
2.4	Deciding where to store your backups .....	10
2.4.1	Authentication settings.....	11
2.5	Wizards.....	11
<b>3</b>	<b>Backing up data.....</b>	<b>13</b>
3.1	Backing up partitions and disks .....	13
3.2	Backup options .....	14
3.2.1	Scheduling.....	15
3.2.2	Backup schemes .....	16
3.2.3	Notifications for backup operation.....	18
3.2.4	Image creation mode.....	19
3.2.5	Backup protection .....	19
3.2.6	Pre/Post commands for backup .....	20
3.2.7	Backup splitting.....	21
3.2.8	Backup validation option .....	21
3.2.9	Backup reserve copy .....	22
3.2.10	Removable media settings .....	22
3.2.11	Backup comment.....	22
3.2.12	Error handling .....	22
3.2.13	File-level security settings for backup.....	23
3.2.14	Computer shutdown.....	23
3.2.15	Performance of backup operation.....	24
3.3	Operations with backups .....	25
3.3.1	Backup operations menu.....	25
3.3.2	Validating backups.....	26
3.3.3	Adding an existing backup to the list.....	26
<b>4</b>	<b>Recovering data .....</b>	<b>27</b>
4.1	Recovering disks and partitions.....	27
4.1.1	Recovering your system after a crash.....	27
4.1.2	Recovering partitions and disks .....	34
4.1.3	About recovery of dynamic/GPT disks and volumes .....	35
4.1.4	Arranging boot order in BIOS.....	38
4.1.5	Recovering files and folders.....	38
4.2	Recovery options .....	39

4.2.1	Disk recovery mode .....	40
4.2.2	Pre/Post commands for recovery.....	40
4.2.3	Validation option .....	41
4.2.4	Computer restart .....	41
4.2.5	File recovery options .....	41
4.2.6	Overwrite file options .....	41
4.2.7	Performance of recovery operation .....	42
4.2.8	Notifications for recovery operation .....	42
<b>5</b>	<b>Disk cloning and migration .....</b>	<b>44</b>
5.1	General information .....	44
5.1.1	Clone Disk wizard.....	44
5.1.2	Manual partitioning.....	47
5.1.3	Excluding items from cloning.....	48
5.2	Migrating your system from an HDD to an SSD.....	49
5.2.1	Preparing for migration .....	49
5.2.2	Migrating to SSD using the backup and recovery method .....	51
<b>6</b>	<b>Tools .....</b>	<b>53</b>
6.1	Adding a new hard disk.....	53
6.1.1	Selecting a hard disk .....	54
6.1.2	Selecting initialization method .....	55
6.1.3	Creating new partitions .....	55
6.2	Creating bootable rescue media .....	57
6.2.1	Acronis Media Builder .....	58
6.2.2	Making sure that your rescue media can be used when needed.....	60
6.3	Acronis Extended Capacity Manager .....	64
6.4	Acronis DriveCleanser .....	67
6.4.1	Source selection.....	67
6.4.2	Algorithm selection.....	68
6.4.3	Disk wiping summary.....	72
6.4.4	Post-wiping actions.....	72
6.5	Mounting an image.....	72
6.6	Unmounting an image .....	73
<b>7</b>	<b>Troubleshooting.....</b>	<b>74</b>
7.1	Acronis System Report.....	74
<b>8</b>	<b>Glossary of Terms.....</b>	<b>77</b>

# 1 Introduction

## In this section

What is Acronis True Image WD Edition? .....	4
System requirements and supported media .....	4
Technical Support.....	5

## 1.1 What is Acronis True Image WD Edition?

Acronis True Image WD Edition is an integrated software suite that ensures the security of all of the information on your PC. It can back up the operating system, applications, settings and all of your data, while also securely destroying any confidential data you no longer need. With this software, you can back up the entire disk drive or selected partitions.

Acronis True Image WD Edition provides you with all the essential tools 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.

You can store backups on almost any PC storage device.

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

## 1.2 System requirements and supported media

### 1.2.1 Minimum system requirements

Acronis True Image WD Edition requires the following hardware:

- Processor Pentium 1 GHz.
- 1 GB RAM.
- 1.5 GB of free space on a hard disk.
- CD-RW/DVD-RW drive or USB flash drive for bootable media creation.
- Screen resolution is 1152 x 720.
- Mouse or other pointing device (recommended).

### 1.2.2 Supported operating systems

Acronis True Image WD Edition 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 Insider Preview
- Windows Home Server 2011

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

## 1.2.3 Supported file systems

- FAT16/32
- NTFS
- Ext2/Ext3/Ext4 \*
- ReiserFS \*
- Linux SWAP \*

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

---

*\* The Ext2/Ext3/Ext4, ReiserFS, and Linux SWAP file systems are supported only for disk or partition backup/recovery operations. You cannot use Acronis True Image WD Edition for file-level operations with these file systems (file backup, recovery, search, as well as image mounting and file recovering from images). You also cannot perform backups to disks or partitions with these file systems.*

---

## 1.2.4 Supported storage media

- Hard disk drives\*
- Solid State Drives (SSD)
- Networked storage devices
- CD-R/RW, DVD-R/RW, DVD+R (including double-layer DVD+R), DVD+RW, DVD-RAM, BD-R, BD-RE
- USB 1.1 / 2.0 / 3.0, FireWire (IEEE-1394) and PC card storage devices
- REV® and other removable media

Acronis True Image WD Edition supports large hard disk drives with a capacity of more than 2TB. This support is provided even if the operating system does not have support for such hardware. For more information see Acronis Extended Capacity Manager (p. 64).

## 1.3 Technical Support

Support for Acronis True Image WD Edition users is provided by Western Digital. Please visit Support Page at [support.wdc.com](http://support.wdc.com) <http://support.wdc.com/>.

## 2 Basic concepts

### In this section

Acronis True Image WD Edition basic concepts .....	6
The difference between file backups and disk/partition images .....	7
Full, incremental and differential backups .....	8
Deciding where to store your backups .....	10
Wizards .....	11

### 2.1 Acronis True Image WD Edition basic concepts

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

#### Backup 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.

#### Backup versions

Backup versions are the file or files created during each backup operation. 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.

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.

#### 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 WD Edition 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 file format

Acronis True Image WD Edition usually saves backup data in the proprietary tib format using compression. This reduces the amount of needed storage space.

When creating a tib file, the program calculates checksum values for data blocks and adds these values to the data being backed up. These checksum values allow for the verification of data integrity.

The data from tib file backups can be recovered only through Acronis products. This may be done in Windows or in the recovery environment.

## 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 WD Edition 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.

## Disaster recovery

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

Acronis True Image WD Edition 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 WD Edition 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 a 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.

## 2.2 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 WD Edition 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 WD Edition stores only the hard disk sectors that contain data. Furthermore, Acronis True Image WD Edition 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 WD Edition copies all hard disk sectors, and not only those that contain data.

## 2.3 Full, incremental and differential backups

**Note:** Incremental and differential backups may be unavailable in the Acronis True Image WD Edition edition that you use.

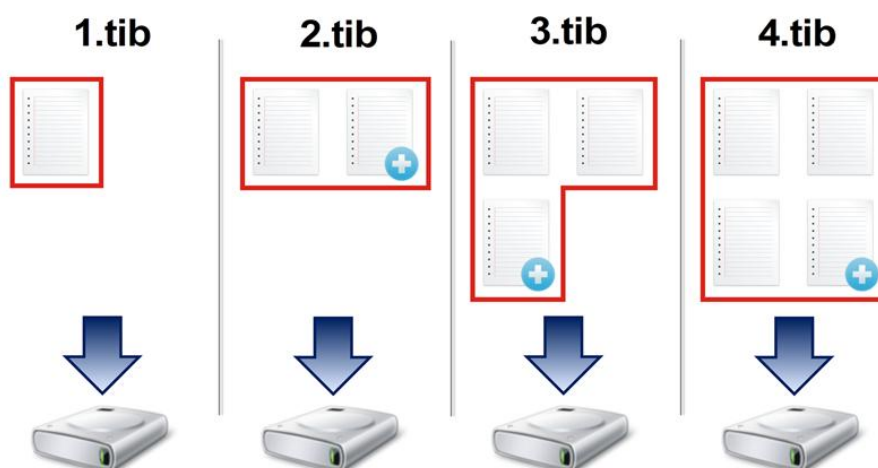
Acronis True Image WD Edition offers three backup methods:

### Full method

The result of a full method backup operation (also known as full backup version) contains all of the data at the moment of the backup creation.

**Example:** Every day, you write one page of your document and back it up using the full method. True Image saves the entire document every time you run backup.

1.tib, 2.tib, 3.tib, 4.tib - full backup versions.



### Additional information



A full backup version forms a base for further incremental or differential backups. It can also be used as a standalone backup. 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 backup versions.

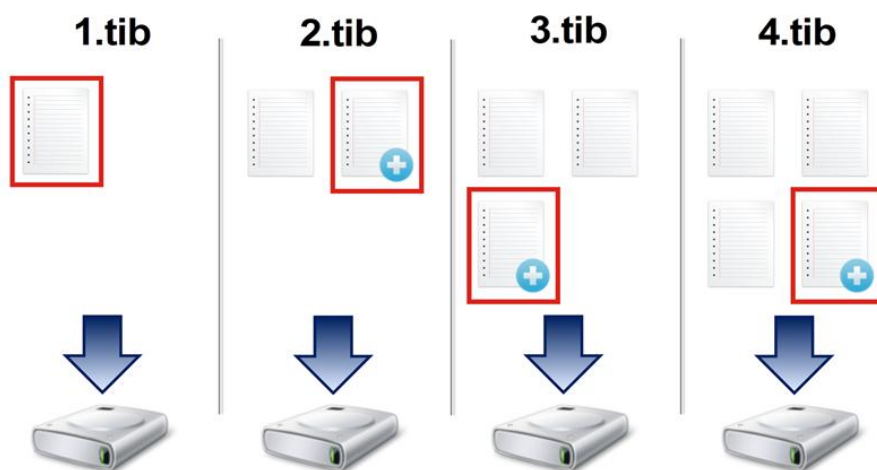
## Incremental method

The result of an incremental method backup operation (also known as incremental backup version) contains only those files which have been changed since the LAST BACKUP.

**Example:** Every day, you write one page of your document and back it up using the incremental method. True Image saves the new page every time you run backup.

**Note:** The first backup version you create always uses full method.

- 1.tib - full backup version.
- 2.tib, 3.tib, 4.tib - incremental backup versions.



## Additional information

Incremental method is the most useful when you need frequent backup versions and the ability to roll back to a specific point in time. As a rule, incremental backup versions are considerably smaller than full or differential versions.

On the other hand, incremental versions require more work for the program to provide recovery. In the example above, to recover the entire work from 4.tib file, True Image reads data from all backup versions. Therefore, if you lose an incremental backup version or it becomes corrupted, all later incremental versions are unusable.

## Differential method

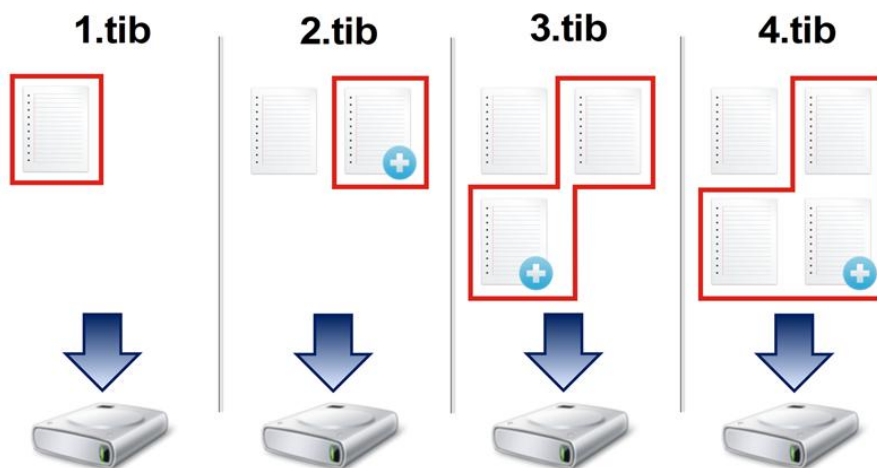
The result of a differential method backup operation (also known as differential backup version) contains only those files which have been changed since the LAST FULL BACKUP.

**Example:** Every day, you write one page of your document and back it up using the differential method. True Image saves the entire document except the first page stored in the full backup version.

**Note:** The first backup version you create always uses full method.

- 1.tib - full backup version.

- 2.tib, 3.tib, 4.tib - differential backup versions.



#### Additional information

Differential method is an intermediate between the first two approaches. It takes less time and space than "Full", but more than "Incremental". To recover data from a differential backup version, True Image needs only the differential version and the last full version. Therefore, recovery from a differential version is simpler and more reliable than recovery from an incremental one.

---

*An incremental or differential backup created after a disk is defragmented might be considerably larger than usual. This is because the defragmentation program changes file locations on the disk and the backups reflect these changes. Therefore, it is recommended that you re-create a full backup after disk defragmentation.*

---

To choose a desired backup method, you usually need to configure a custom backup scheme. For more information see Custom schemes (p. 17).

## 2.4 Deciding where to store your backups

Acronis True Image WD Edition supports quite a few of storage devices. For more information see Supported storage media (p. 5). Some of the supported storage locations are discussed below.

### Hard disk drives

Since hard disk drives are now quite inexpensive, in most cases purchasing an external hard drive for storing your backups will be an optimal solution. An external drive enhances the security of your data because you can keep it off-site (for example, at home if you back up your office computer and vice versa). You can choose various interfaces – USB, FireWire, eSATA depending on the configuration of your computer ports and the required data transfer rate. In many cases the best choice will be an external USB hard drive, especially if your computer supports USB 3.0.

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

### Home file server, NAS or NDAS

If you have a Gigabit Ethernet home network and a dedicated file server or NAS, you can store backups on the file server or NAS practically like on an internal drive.

If you decide to use an external hard drive, NAS, NDAS, etc., you will need to check whether Acronis True Image WD Edition detects the selected backup storage. You need to check this both in Windows and when booted from the rescue media.

To gain access to an NDAS enabled storage device, in many cases you will need to specify the NDAS device ID (20 characters) and the write key (5 characters). The write key allows you to use an NDAS enabled device in write mode (for example, for saving your backups). Usually the device ID and write key are printed on a sticker attached to the bottom of the NDAS device or on the inside of its enclosure. If there is no sticker, you need to contact your NDAS device vendor to obtain that information.

## Optical discs

Blank optical discs such as DVD-R, DVD+R are very cheap, so they will be the lowest cost solution for backing up your data, though the slowest one. This is especially true when backing up directly to DVDs. Furthermore, if your backup consists of several DVDs, data recovery from DVDs will require a lot of disc swapping. On the other hand, using Blu-ray discs may be a viable option.

---

*Due to the necessity of swapping discs, we strongly recommend to avoid backing up to DVDs if the number of discs is more than three. When there is no alternative to backing up to DVDs, we recommend to copy all DVDs to a folder on a hard disk and then to recover from that folder.*

---

### 2.4.1 Authentication settings

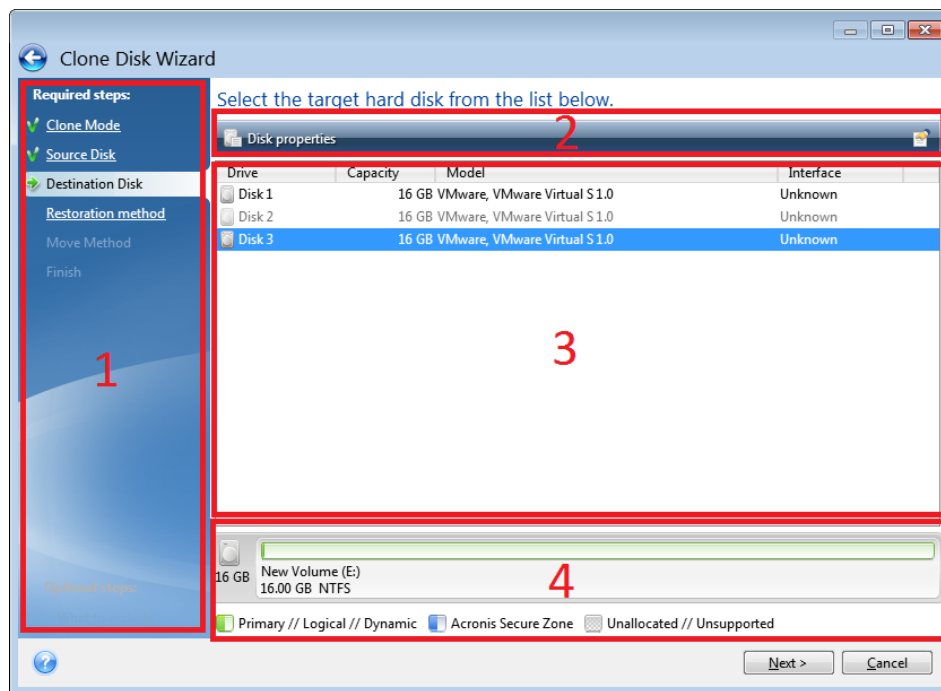
If you are connecting to a networked computer, in most cases you will need to provide the necessary credentials for accessing the network share. For example, this is possible when you select a backup storage. The **Authentication Settings** window appears automatically when you select a networked computer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

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

## 2.5 Wizards

When you use the available Acronis True Image WD Edition 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.

## 3 Backing up data

Acronis True Image WD Edition 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 partitions and disks .....	13
Backup options .....	14
Operations with backups .....	25

### 3.1 Backing up partitions and disks

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:

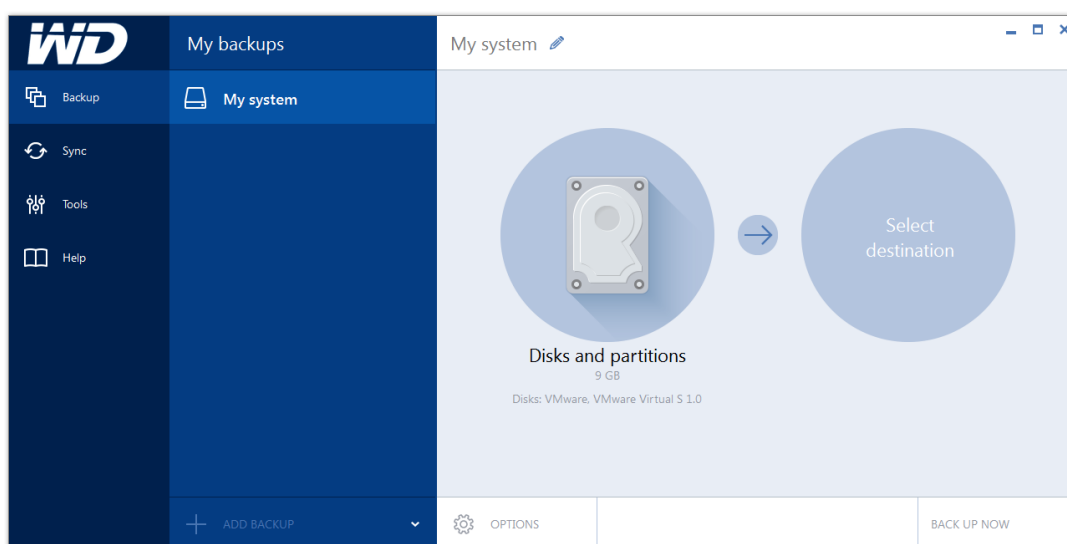
1. Start Acronis True Image WD Edition.
2. On the sidebar, click **Backup**.
3. To add a new backup, click the plus sign at the bottom of the backup list, and then type a name for the backup.
4. Click the **Backup source** icon, and then select **Disks and partitions**.
5. In the opened window, select 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.*

---



6. 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.
- **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.*

---

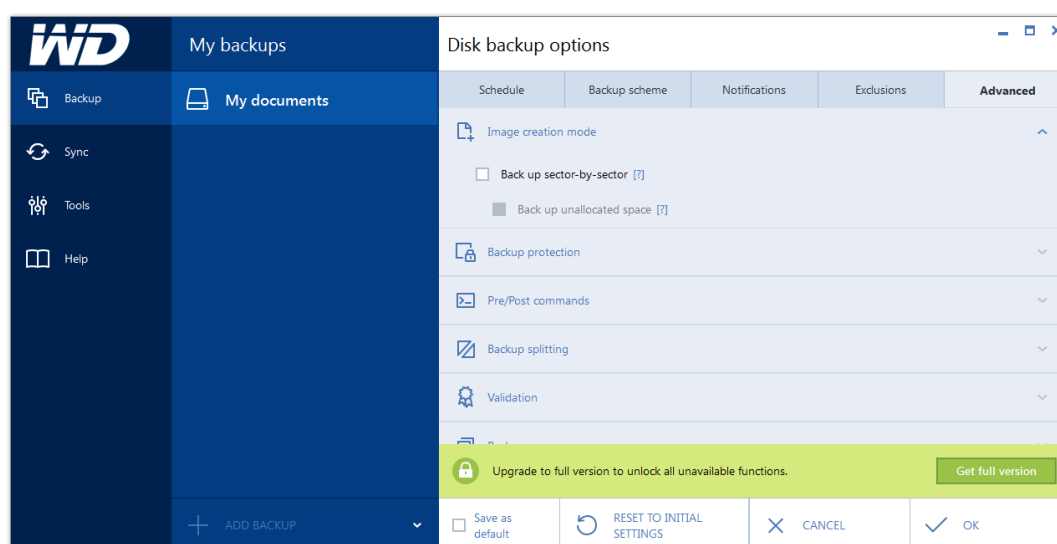
7. [optional step] Click **Options** to set the options for the backup. For more information see Backup options (p. 14).
8. Perform one of the following:
  - To run the backup immediately, click **Start backup**.
  - To run the backup later or on a schedule, click the arrow to the right of the **Start backup** button, and then click **Later**.

## 3.2 Backup options

When you create a backup, you can change additional options and fine-tune the backup process. To open the options window, select a source and destination for a backup, and then click **Options**.

Note that options of each backup type (disk-level backup, file-level backup, online backup, nonstop backup) are fully independent and you should configure them separately.

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.



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. Note that this will reset the settings for the current backup only. To reset the settings for all further backups, click **Reset to initial settings**, select the **Save the settings as default** check box, and then click **OK**.

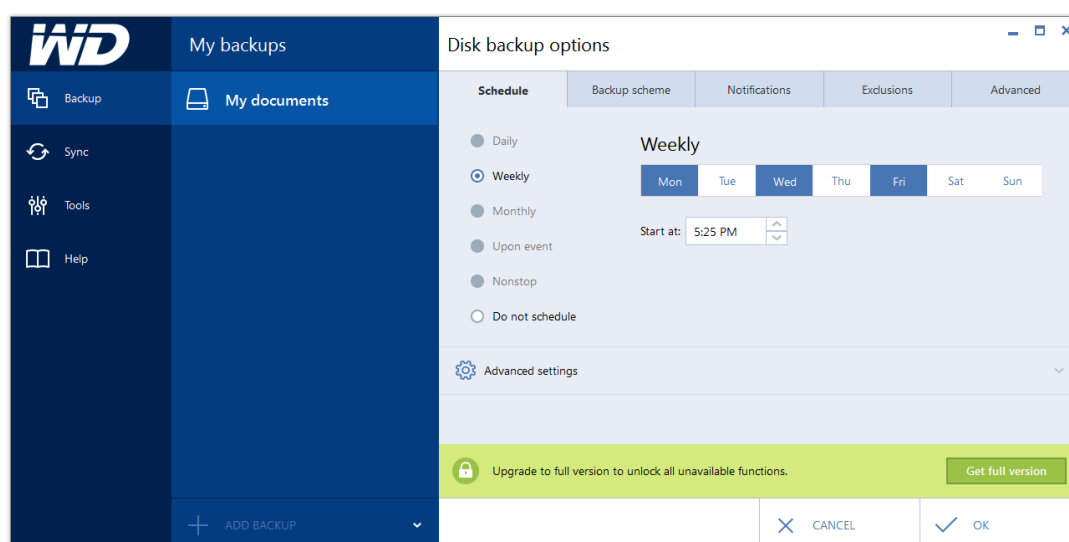
### In this section

Scheduling ..... 15

Backup schemes .....	16
Notifications for backup operation .....	18
Image creation mode.....	19
Backup protection .....	19
Pre/Post commands for backup .....	20
Backup splitting .....	21
Backup validation option .....	21
Backup reserve copy .....	22
Removable media settings.....	22
Backup comment.....	22
Error handling.....	22
File-level security settings for backup .....	23
Computer shutdown.....	23
Performance of backup operation .....	24

### 3.2.1 Scheduling

The **Schedule** tab allows you to specify the backup and validation schedule settings.



You can choose and set up one of the following backup or validation frequencies:

- **Weekly** (p. 16)—The operation will be executed once a week or several times a week on the selected days.
- **Do not schedule**—The scheduler will be turned off for the current operation. In this case the backup or validation will run only when you click **Back up now** or **Validate** respectively in the main window.

#### Advanced settings

Clicking **Advanced settings** allows you to specify the following additional settings for backup and validation:

- To postpone a scheduled operation until the next time the computer is not in use (a screen saver is displayed or computer is locked), select the **Run the backup only when the computer is idle** check box. If you schedule validation, the check box will change to **Run the validation only when the computer is idle**.

- If you want to wake up the sleeping/hibernating computer to perform the scheduled operation, select the **Wake up the sleeping/hibernating computer** check box.
- If the computer is switched off when the scheduled time comes, the operation won't be performed. You can force the missed operation to run at the next system startup. To do so, select the **Run at system startup** check box.

Additionally, you can set a time delay to start backup after the system startup. For example, to start backup 20 minutes after system startup, type *20* in the appropriate box.

- If you schedule a backup to a USB flash drive or validation of a backup that is located on a USB flash drive, one more check box appears: **Run when the current destination device is attached**. Selecting the check box will let you perform a missed operation when the USB flash drive is attached if it was disconnected at the scheduled time.
- If you want to regularly back up data located on a removable media (for example USB flash drive) or remote storage (for example network folder or NAS), we recommend that you select the **Run when the current source device is attached** check box. This is useful because an external storage device may be often unavailable at the scheduled moment of backup. In that case, if the check box is selected, the missed backup operation will start when the device is connected or attached.
- **Run the backup upon HDD alarm** (available when Acronis Drive Monitor is installed) – if enabled, the backup will run as soon as there is an alarm on Acronis Drive Monitor about a potential problem with one of the hard disks in the backup source. Acronis Drive Monitor is a hard drive health monitoring utility based on information received from hard drive S.M.A.R.T. reports, Windows logs, and its own scripts.

### 3.2.1.1 Weekly execution parameters

You can set up the following parameters for weekly operation execution:

- **Week days**  
Select the days on which to execute the operation by clicking on their names.
- **Start time**  
Set the operation's start time. Enter hours and minutes manually, or set the desired start time using the up and down buttons.

Description of the **Advanced settings** see in Scheduling (p. 15).

## 3.2.2 Backup schemes

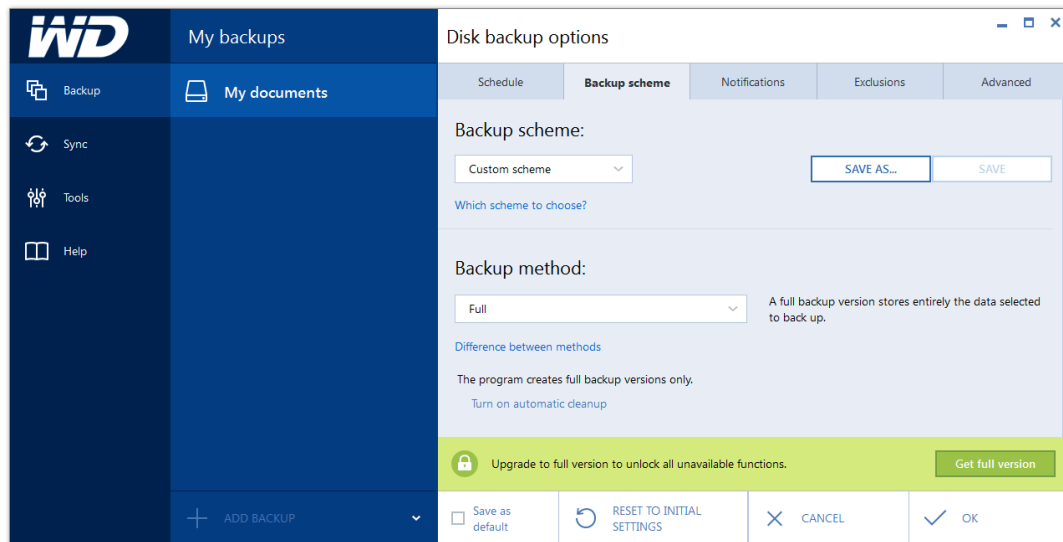
Backup schemes along with the scheduler help you to set up your backup strategy. The schemes allow you to optimize backup storage space usage, improve data storage reliability, and automatically delete the obsolete backup versions.

Backup scheme defines the following parameters:

- Backup methods that will be used to create backup versions
- Sequence of the backup versions created using different methods



- Version cleanup rules



Acronis True Image WD Edition allows you to choose the following backup schemes:

- **Single version** (p. 17) - select this scheme if you want to use the smallest backup storage.
- **Custom** (p. 17) - select this item if you want to set up a backup scheme manually.

### 3.2.2.1 Single version scheme

The program creates a full backup version and overwrites it every time according to the specified schedule or when you run backup manually.

Backup scheduler setting for disk backup: weekly.

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

Required storage space: minimal.

### 3.2.2.2 Custom schemes

With Acronis True Image WD Edition 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.*

---

So first of all select one of the backup methods in the appropriate box.

- **Full** (p. 8)  
Select this method if you want to create only full backup versions.

#### 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.

- **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.
- **Keep size of the backup no more than [defined size]** - Select this option to limit 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.

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.*

---

## 3.2.3 Notifications for backup operation

### 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 WD Edition 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 WD Edition can monitor free space on the following storage devices:

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

---

*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.*

---

## 3.2.4 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 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.

## 3.2.5 Backup protection

A backup file can be password-protected. By default, there is no password protection for backups.

---

*You cannot set or change the password for an already existing backup.*

---

#### To protect a backup:

1. Enter the password for the backup into the **Password** field. We recommend that you use a password longer than seven symbols and containing both letters (in upper and lower cases preferably) and numbers to make it more difficult to guess.

---

*A password cannot be retrieved. Please memorize the password that you specify for a backup protection.*

---

2. Retype the previously entered password into the **Confirm** field.
3. [optional step] To increase the security of your confidential data, you can encrypt the backup with strong industry-standard AES (Advanced Encryption Standard) cryptographic algorithm. AES is available with three key lengths – 128, 192 and 256 bits to balance performance and protection as desired.

The 128-bit encryption key is sufficient for most applications. The longer the key, the more secure your data. However, the 192 and 256-bit long keys significantly slow down the backup process.

If you want to use AES encryption, choose one of the following keys:

- **AES 128** - to use 128-bit encryption key
- **AES 192** - to use 192-bit encryption key

- **AES 256** - to use 256-bit encryption key

If you do not want to encrypt the backup and only want to protect a backup with a password, select **None**.

4. Having specified the backup settings, click **OK**.

## How to get access to a password-protected backup

True Image asks for the password every time you try to modify the backup:

- Recover data from the backup
- Edit settings
- Delete
- Mount
- Move

To access the backup, you must specify the correct password.

## 3.2.6 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.

### 3.2.6.1 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.

## 3.2.7 Backup splitting

---

*Acronis True Image WD Edition 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 WD Edition 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 WD Edition 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.*

---

## 3.2.8 Backup validation option

You can specify the additional validation setting: **Validate backup when it is created**.

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

### **Regular validation**

You can also schedule validation of your backups to ensure that they remain "healthy". By default regular validation is turned on with the following settings:

- Frequency: once a week
- Day: the date when the backup was started
- Time: the moment of backup start plus 15 minutes
- Advanced settings: the **Run the validation only when the computer is idle** check box is selected

You can change the default settings and specify your own schedule. For more information see Scheduling (p. 15).

## 3.2.9 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.

## 3.2.10 Removable media settings

The following settings are available:

- **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.

## 3.2.11 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**.

## 3.2.12 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 and warn you about an error with a message, 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)** (the preset is disabled) - You can enable this setting to ignore errors during backup operations. This feature was mainly designed for unattended backups when you cannot control the backup process. In this mode no

notifications will be displayed to you if errors occur during backup. Instead you can view the detailed log of all operations after the backup process finishes.

- **Ignore bad sectors** (the preset is disabled) - This option is present only for disk and partition backups. It lets you run a backup even if there are bad sectors on the hard disk. Although most disks do not have bad sectors, the possibility that they might occur increases during the course of the hard disk's lifetime. If your hard drive has started making strange noises (for example, it starts making quite loud clicking or grinding noises during operation), such noises may mean that the hard drive is failing. When the hard drive completely fails, you can lose important data, so it is high time to back up the drive as soon as possible. There may be a problem though – the failing hard drive might already have bad sectors. If the **Ignore bad sectors** check box is left unselected, a backup is aborted in case of read and/or write errors that could occur on the bad sectors. Selecting this box lets you run a backup even if there are bad sectors on the hard disk ensuring that you save as much information from the hard drive as possible.
- **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 configure this option by specifying two settings - number of attempts and time interval between attempts. According to these settings, Acronis Acronis True Image WD Edition will try to back up your data until the backup is successfully created. But if the error interrupting the backup persists, then the backup will not be created.

### 3.2.13 File-level security settings for backup

---

**Note:** This feature may be unavailable in the Acronis True Image WD Edition edition that you use.

---

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

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

These options relate only to file/folder backups.

### 3.2.14 Computer shutdown

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.

### 3.2.15 Performance of backup operation

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

#### 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.*

---

#### 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 WD Edition.

#### Network connection speed limit

When you back up data to network drives or FTP, you can reduce the influence of connection used by True Image on other network connections of your computer. Set the connection speed that will allow you to use Internet and network resources without annoying slowdowns.

To reduce connection speed:

- Select the **Limit transfer rate to** check box and specify an optimal value and an appropriate measurement unit (kilobits or megabits per second).



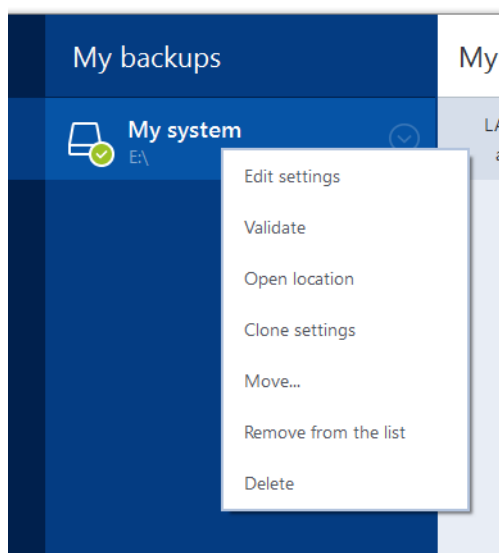
## 3.3 Operations with backups

### In this section

Backup operations menu .....	25
Validating backups.....	26
Adding an existing backup to the list.....	26

### 3.3.1 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:

- **Edit settings** - allows editing of the current backup settings.
- **Reconfigure** (for backups manually added to the backup list) - allows configuring the settings of a backup created by a previous True Image version. This item may also appear for backups created on another computer and added to the backup list without importing their settings.  
Without backup settings, you cannot refresh the backup by clicking **Back up now**. Also, you cannot edit and clone the backup settings.
- **Reconfigure** (for online backups) - allows you to bind a selected online backup to the current computer. To do this, click this item and reconfigure settings of the backup. Note that only one online backup can be active on one computer.
- **Validate** - starts backup validation.
- **Clean up** (available for nonstop backup only) - opens the **Cleanup** dialog box where you can delete the backup versions you no longer need. The backup chain will not be corrupted.
- **Open location** - opens the folder containing the backup files.
- **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.
- **Remove from the list** - removes the current backup from the backup list shown in the My backups area. This operation also turns off the scheduling of the removed backup (if a schedule was set), but it does not delete the backup files.
- **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.

### 3.3.2 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 WD Edition, and then click **Backup** on the sidebar.
2. From the backup list, select the backup to validate, click **Operations**, and then click **Validate**.

#### Validating backups in a stand-alone version of 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. 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**.

### 3.3.3 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 WD Edition, 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 Recovering data

### In this section

Recovering disks and partitions .....	27
Recovery options.....	39

## 4.1 Recovering disks and partitions

### In this section

Recovering your system after a crash.....	27
Recovering partitions and disks .....	34
About recovery of dynamic/GPT disks and volumes .....	35
Arranging boot order in BIOS .....	38
Recovering files and folders.....	38

### 4.1.1 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. 27). 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. 27) and then proceed with recovering your system.

#### 4.1.1.1 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. 28) for details.

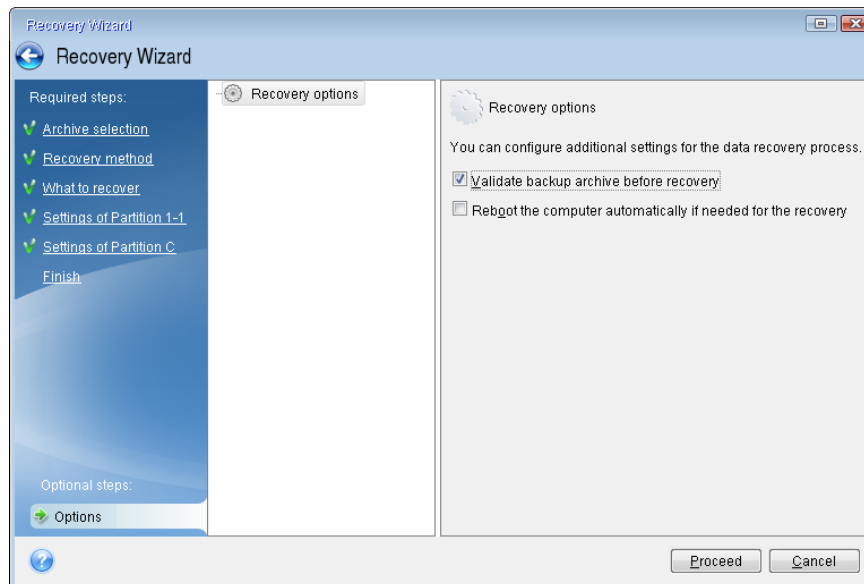
#### 4.1.1.2 Preparing for recovery

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 WD Edition 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 WD Edition might correspond to the E: disk in Windows.

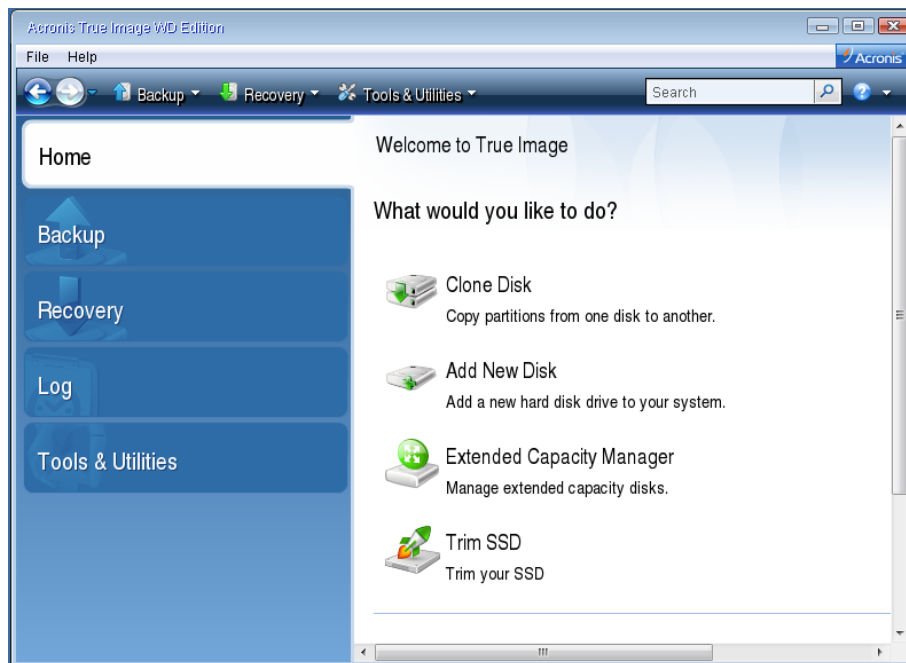
#### 4.1.1.3 Recovering your system to the same disk

Before you start, we recommend that you complete the procedures described in Preparing for recovery (p. 27).

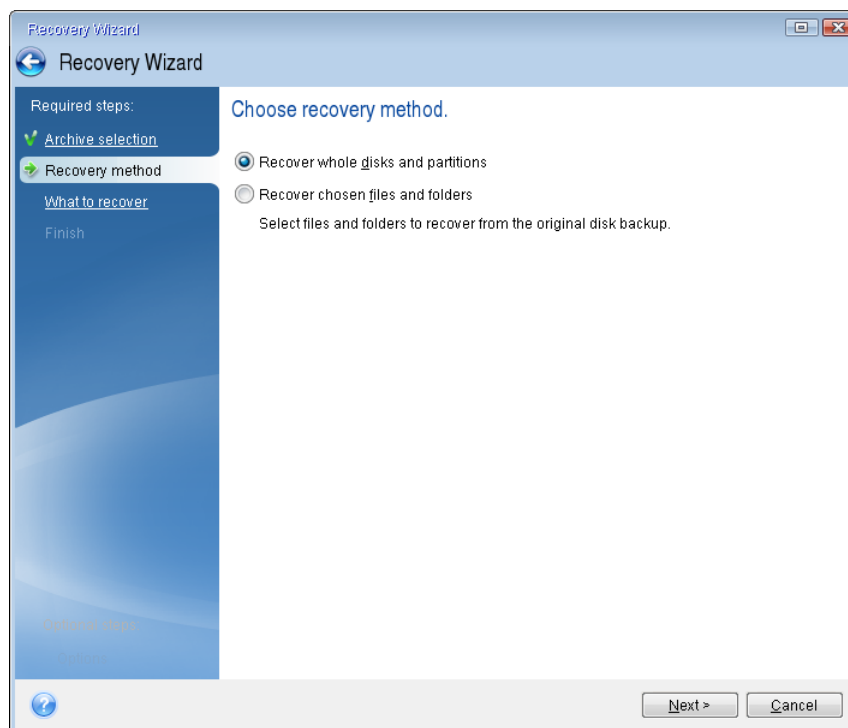
##### To recover your system:

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. 38).
3. Boot from the rescue media and select **True Image**.

4. On the **Home** screen, select **My disks** below **Recover**.

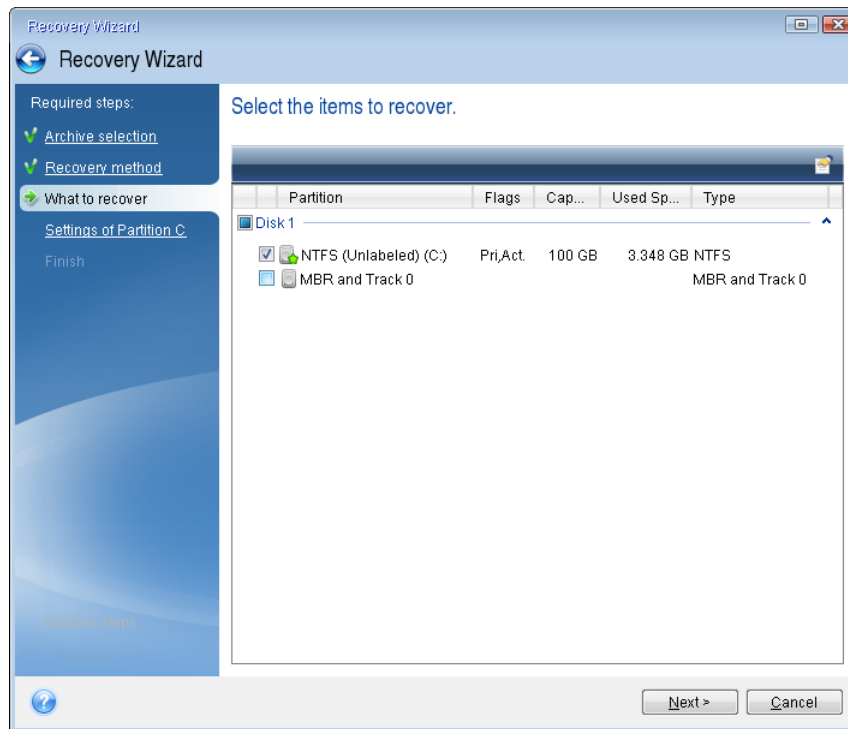


5. Select the system disk or partition backup to be used for recovery.  
When the backup is not displayed, click **Browse** and specify path to the backup manually.
6. Select **Recover whole disks and partitions** at the **Recovery method** step.

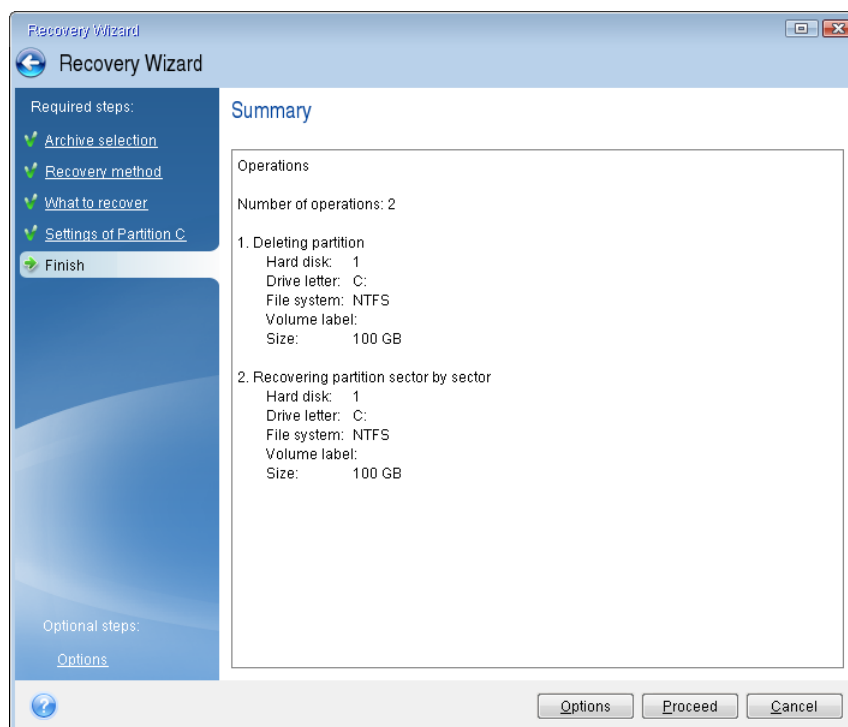


7. Select the system partition (usually C) on the **What to recover** screen. If the system partition has a different letter, select the partition using the **Flags** column. It must have the **Pri, Act** flags.

*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.
9. 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**.



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

## 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. 27). You do not need to format the new disk, as this will be done in the process of recovery.

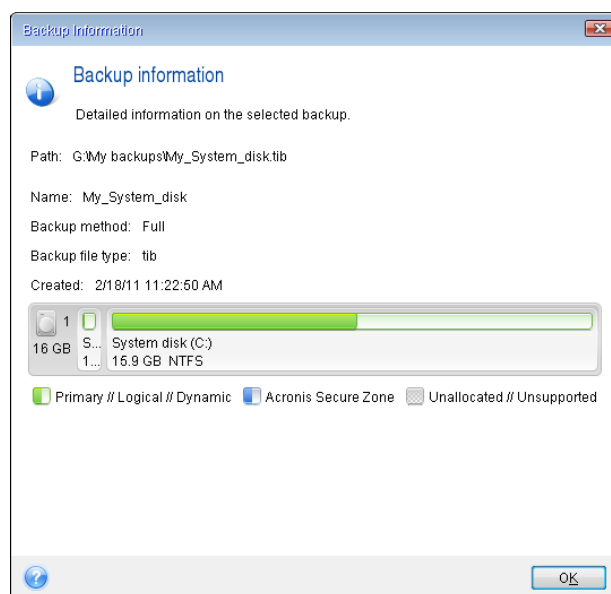
---

*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.*

---

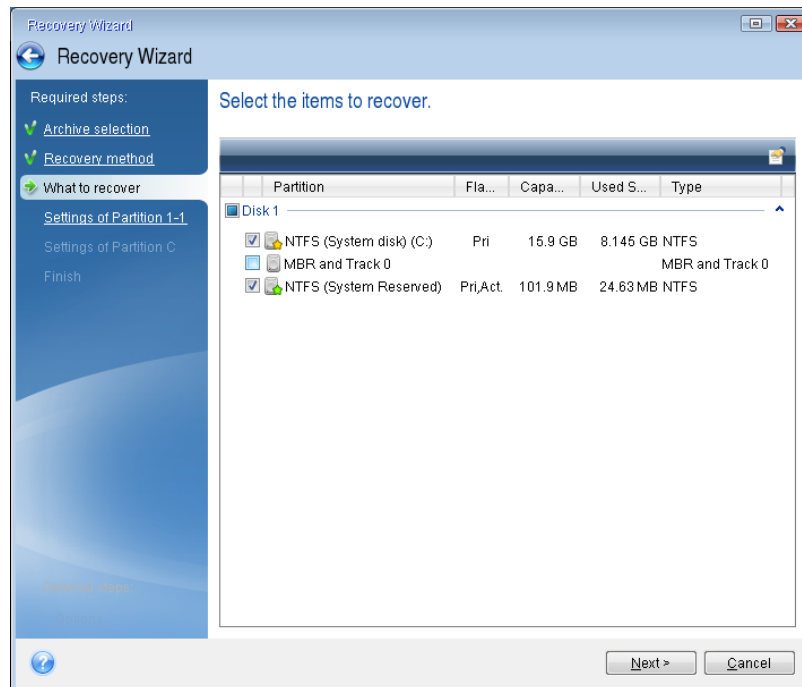
### To recover your system to a new disk:

1. 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.
2. Attach the external drive if it contains the backup to be used for recovery and make sure that the drive is powered on.
3. 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. 38).
4. Boot from the rescue media and select **True Image**.
5. 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.



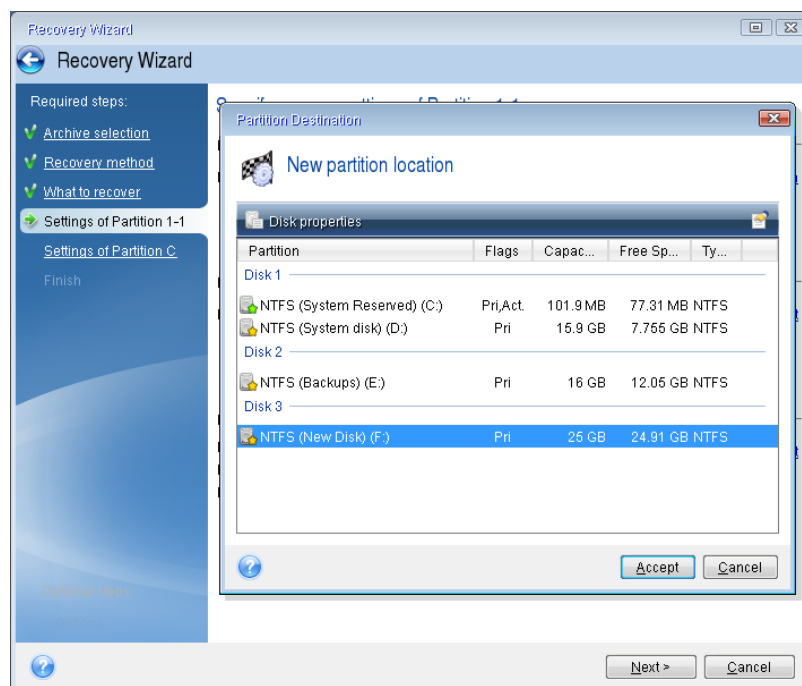
8. Select **Recover whole disks and partitions** at the **Recovery method** step.

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.



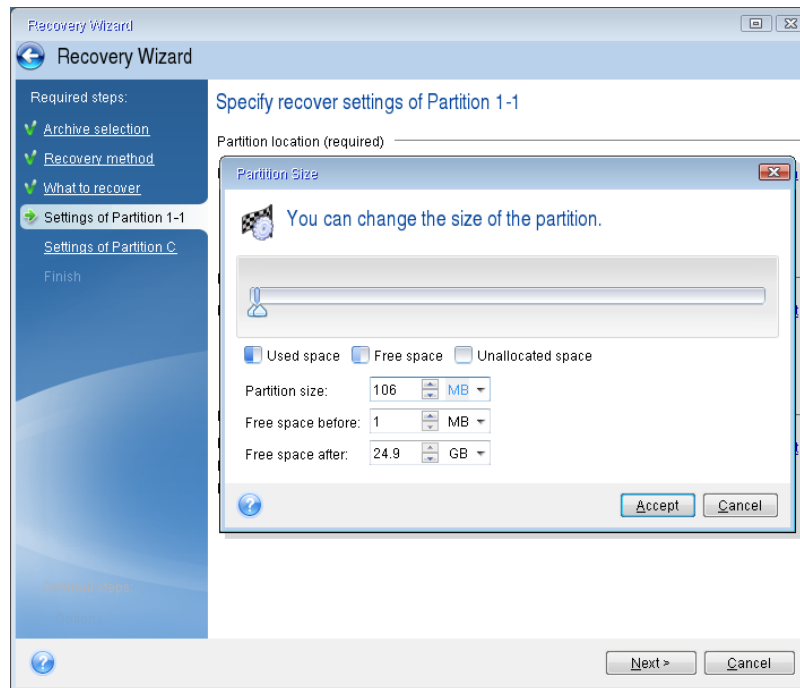
Selecting partitions leads to appearance of the relevant steps "Settings of partition ...". Note that these steps start with partitions which do not have an assigned disk letter (as usually is the case with hidden partitions). The partitions then take an ascending order of partition disk letters. This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



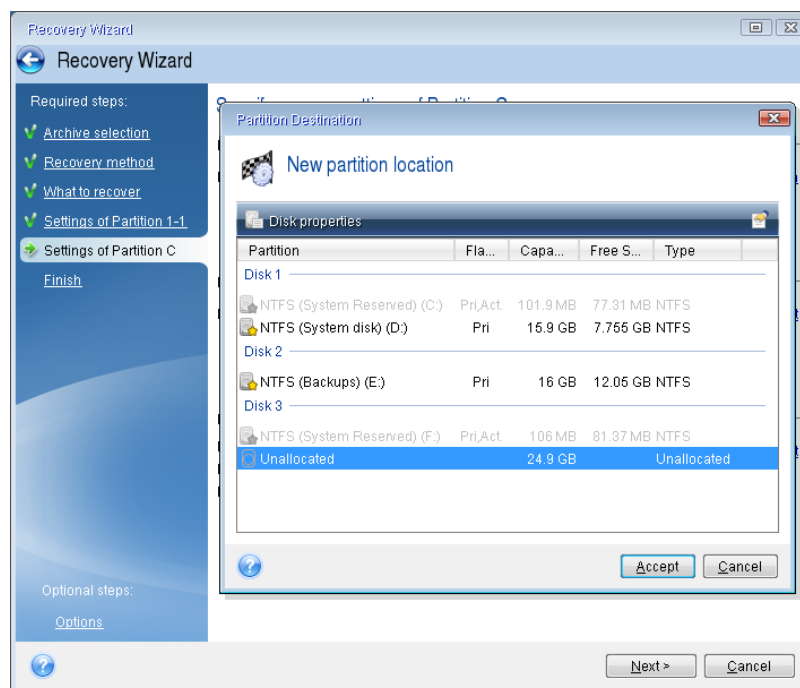


- **Type.** Check the partition type and change it, if necessary. Ensure that the System Reserved partition (if any) is primary and marked as active.
- **Size.** Click **Change default** in the Partition size area. By default the partition occupies the entire new disk. Enter the correct size in the Partition 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**.



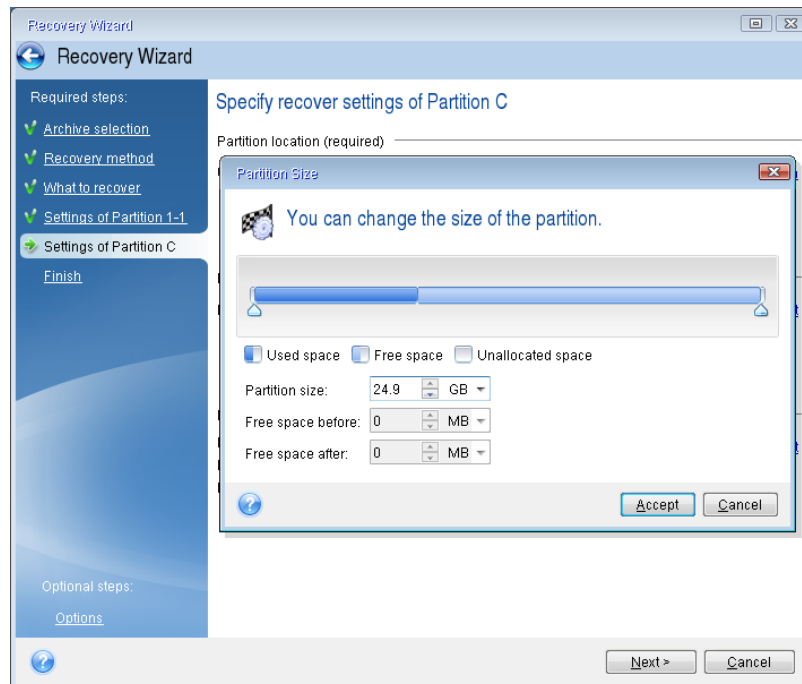
11. On the **Settings of Partition C** step, specify the settings for the second partition, which in this case is your system partition.

- 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.

- 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.
- At the next step, select the destination disk as the target for MBR recovery, click **Next** and then **Proceed**. After MBR recovery is complete, exit the standalone version of Acronis True Image WD Edition.

### 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.

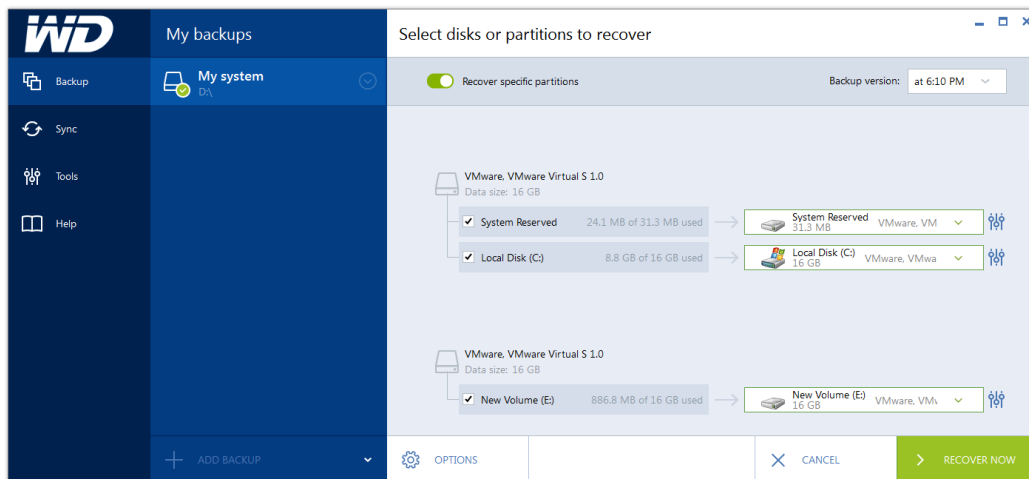
## 4.1.2 Recovering partitions and disks

You can recover your disks from backups located on local or network storage.

### To recover partitions or disks:

- Start Acronis True Image WD Edition.

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.

### Do I need to recover MBR?

We recommend that you recover the Master Boot Record (MBR) when Windows does not boot after recovery. To recover the MBR, click **Show MBR** and then select the MBR check box.

## 4.1.3 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:

	<b>My system is BIOS-booted (Windows or Acronis Bootable Media)</b>	<b>My system is UEFI-booted (Windows or Acronis Bootable Media)</b>
<b>My source disk is MBR and my OS does not support UEFI</b>	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.
<b>My source disk is MBR and my OS supports UEFI</b>	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. 36).
<b>My source disk is GPT and my OS supports UEFI</b>	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. 36).

### 4.1.3.1 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).

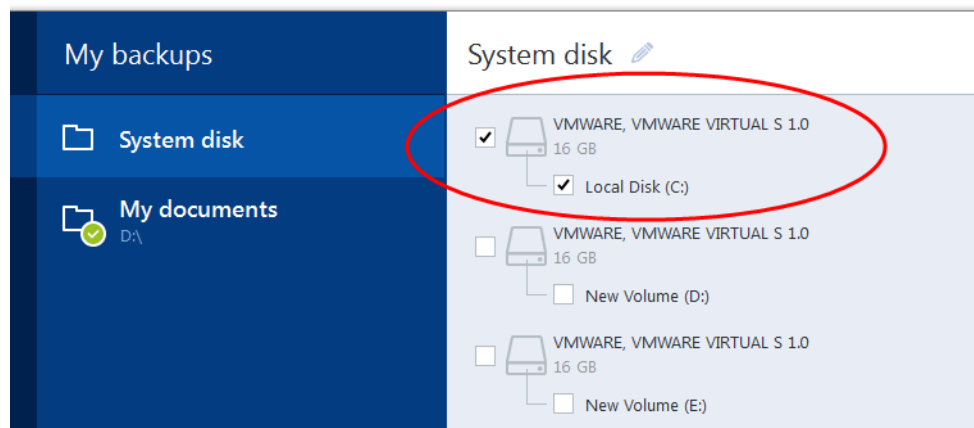
Before you start the procedure, please ensure that you have:

- **Bootable rescue media.**

Refer to Creating bootable rescue media for details.

- **Backup of your system disk created in disk mode.**

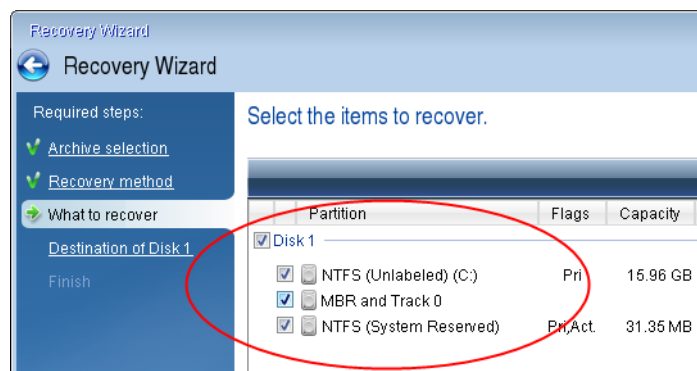
To create this backup, switch to disk mode, and then select the hard drive that contains your system partition. Refer to Backing up disks and partitions for details.



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

1. Boot from the rescue media in UEFI mode and select True Image.
2. Run the **Recovery wizard** and follow the instructions described in Recovering your system (p. 28).
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.

## 4.1.4 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:

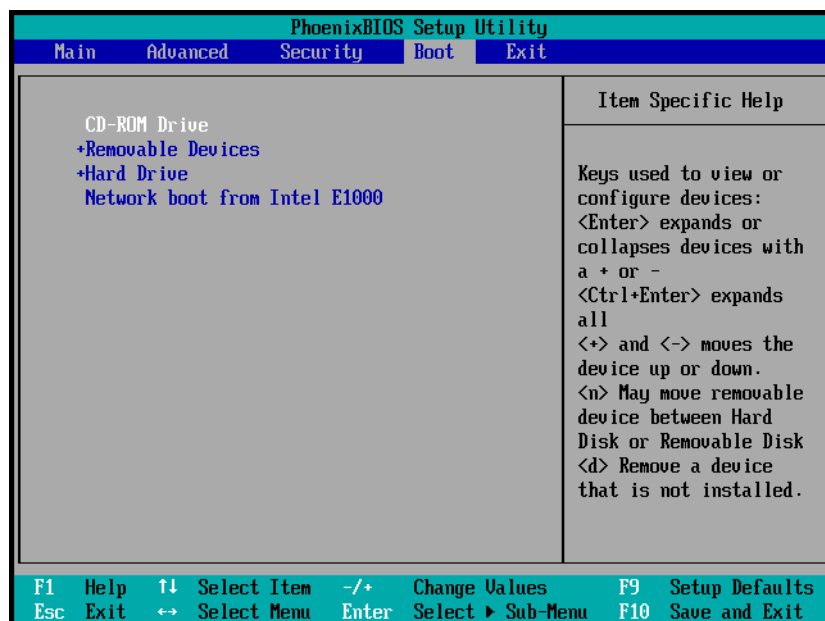
1. If you use a USB flash drive as a bootable media, plug it into the USB port.
2. Turn your computer on. During the Power-On Self Test (POST), you will see the key combination that you need to press in order to enter BIOS.
3. Press the key combination (such as, **Del**, **F1**, **Ctrl+Alt+Esc**, **Ctrl+Esc**).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



6. 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.*

---

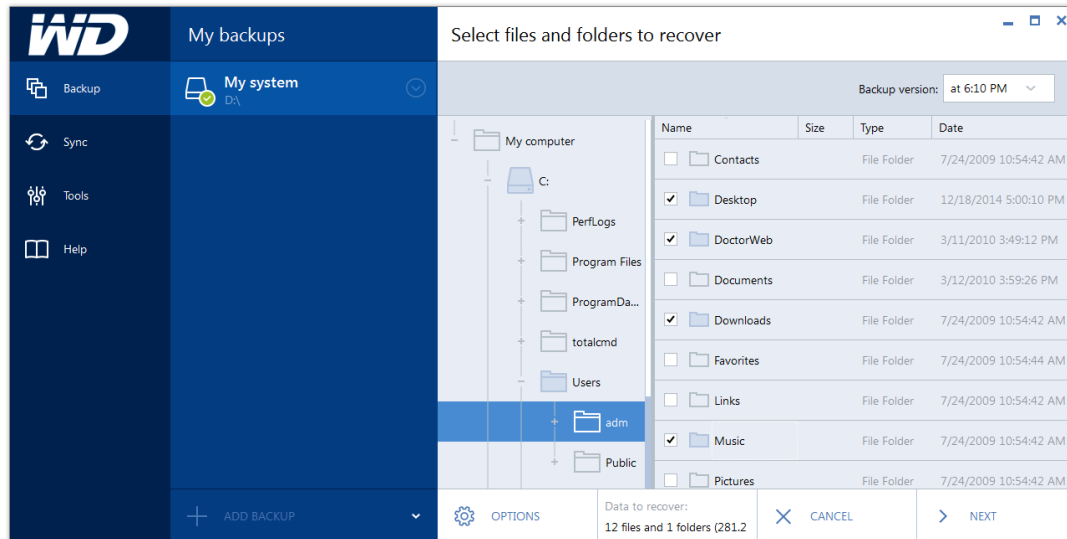
## 4.1.5 Recovering files and folders

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

### To recover files and folders:

1. Start Acronis True Image WD Edition.

2. On the sidebar, click **Backup**.
3. From the backup list, select the backup which contains the files or folders that you want to recover.
4. On the right panel, click **Recover files**.
5. Select backup version (data state on specific date and time).
6. Select the files and folders that you want to recover, and then click **Next**.



7. 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 you choose a new location, the selected items will be recovered by default without recovering the original, absolute path. You may also wish to recover the items with their entire folder hierarchy. In this case select the **Keep the original folder structure** check box.
8. 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.
9. 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.*

## 4.2 Recovery options

In the **Disk Recovery Options** and **File Recovery Options** windows 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.

Note, that disk recovery options and file recovery options are fully independent, and you should configure them separately.

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 .....	40
Pre/Post commands for recovery.....	40
Validation option.....	41
Computer restart.....	41
File recovery options .....	41
Overwrite file options.....	41
Performance of recovery operation .....	42
Notifications for recovery operation .....	42

### 4.2.1 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.

### 4.2.2 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.

#### 4.2.2.1 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.

### 4.2.3 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.*

---

### 4.2.4 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.

### 4.2.5 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 (see File-level security settings for backup (p. 23)), 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.

### 4.2.6 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.

## 4.2.7 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 WD Edition.

## 4.2.8 Notifications for recovery operation

### 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 WD Edition 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 WD Edition can monitor free space on the following storage devices:

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

---

*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.*

---

## 5 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. 44).
- Back up your old disk drive, and then recover it to the new one (p. 31).

### In this section

General information .....44


Migrating your system from an HDD to an SSD .....49

## 5.1 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](#). 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.

### 5.1.1 Clone Disk wizard

Before you start, we recommend that you read general information about Disk cloning utility (p. 44).

### 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.

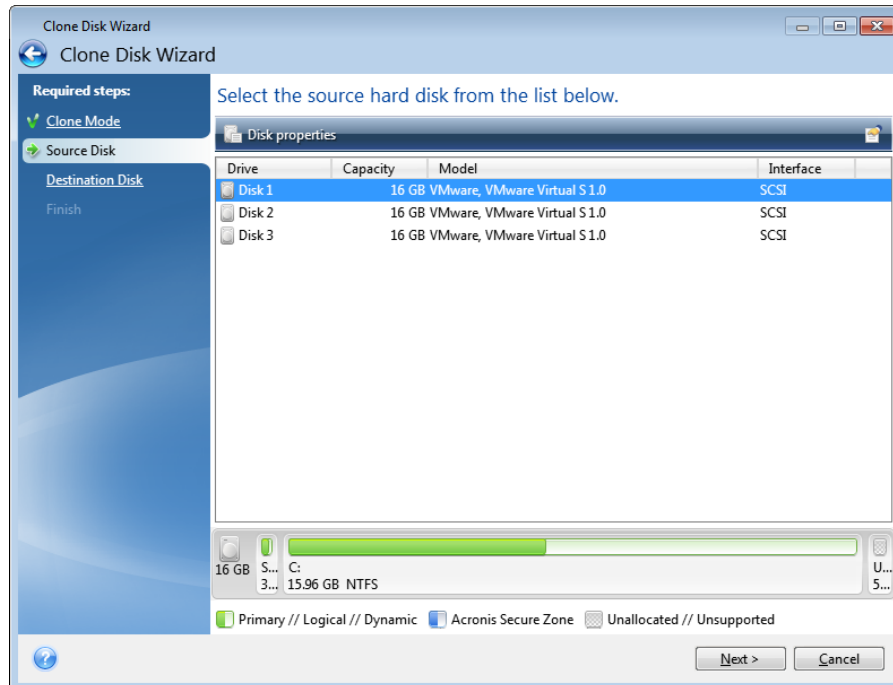
- **Automatic**—Recommended in most cases.
- **Manual**—Manual mode will provide more data transfer flexibility. Manual mode can be useful if you need to change the disk partition layout.

---

*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 WD Edition does not support cloning of dynamic disks.*

---

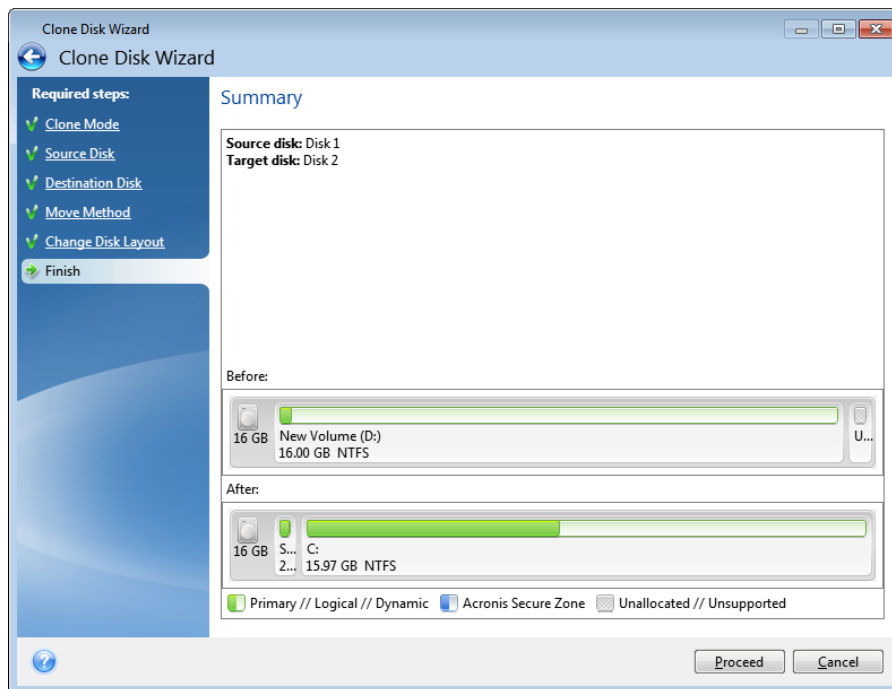
4. On the **Destination Disk** step, select the destination disk for the cloned data.  
 If the selected destination disk contains partitions, you will need to confirm deletion of the partitions. Note that the real data destruction will be performed only when you click **Proceed** on the last step of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

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

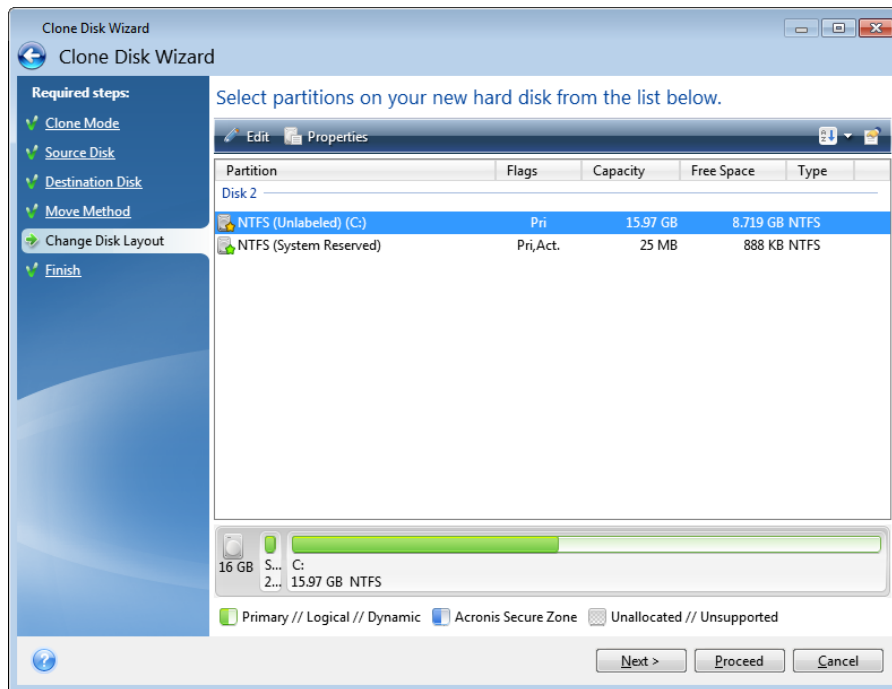


If the cloning operation is stopped for some reason, you will have to configure and start the procedure again. You will not lose your data, because True Image does not alter the original disk and data stored on it during cloning.

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 WD Edition 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.

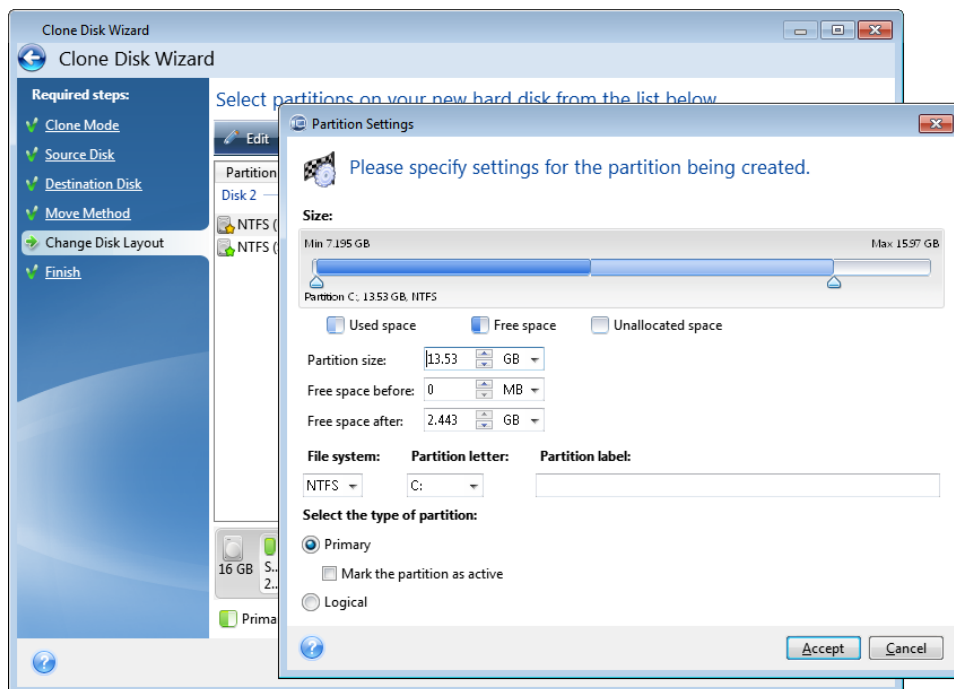
## 5.1.2 Manual partitioning

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. 56) 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.

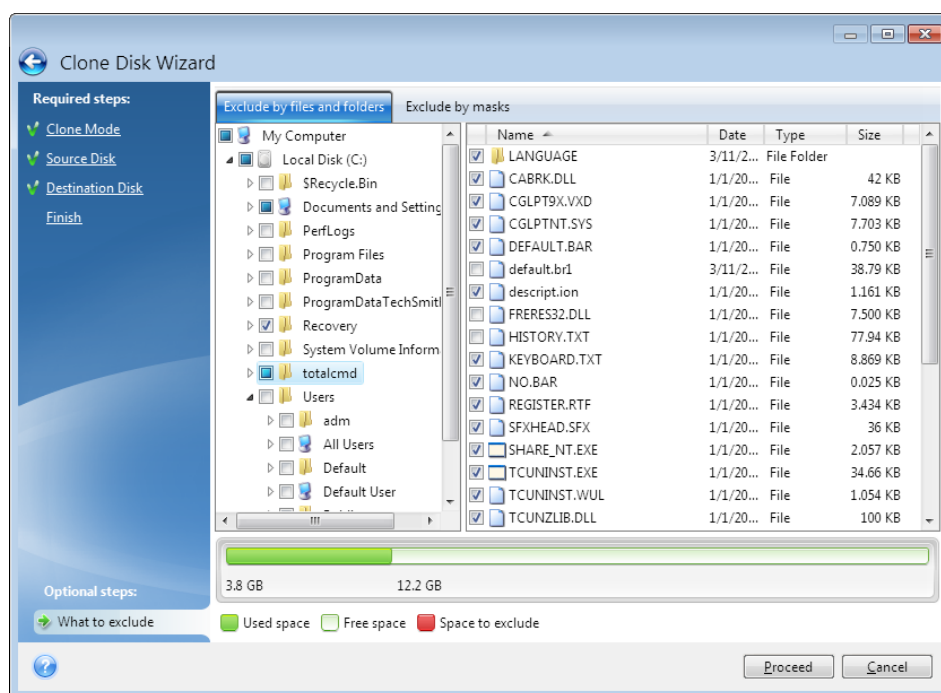
## 5.1.3 Excluding items from cloning

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.

## 5.2 Migrating your system from an HDD to an SSD

### In this section

Preparing for migration .....	49
Migrating to SSD using the backup and recovery method .....	51

### 5.2.1 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 WD Edition 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 WD Edition does not recognize your SSD](#) (p. 50).

#### 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. See [What to do if your SSD does not have enough space for all HDD content](#).

#### 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.

For more information see [SSD support](#).

## 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. 44).

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. 51).

### 5.2.1.1 What to do if Acronis True Image WD Edition does not recognize your SSD

Sometimes Acronis True Image WD Edition 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:

For Windows Vista/Windows 7 type **cmd** in the Search field and press **Enter**.

---

*For Windows XP, type **cmd** in the Run field and 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 WD Edition 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. 53).

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

1. Boot from the rescue 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 rescue 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 rescue media detects the SSD, you may use the following procedure for recovery or cloning under rescue 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 rescue 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 request a custom rescue media from Acronis Support. For more information, see [Creating a custom rescue CD](#).

---

*Please be aware that finding the appropriate drivers and making the custom rescue media may take time. Furthermore, finding the appropriate drivers may not be possible in some cases.*

---

## 5.2.2 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 WD Edition.
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 WD Edition.
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. 31).

## 6 Tools

Acronis Tools and utilities include protection tools, mounting tools, clone disk utility, security and privacy utilities, and disk management utilities.

### Protection tools

- **Rescue Media Builder**

Allows you to create a bootable rescue media with Acronis products (or their specified components) installed on your computer.

### Clone disk

Use Clone disk wizard if you need to clone your hard disk drive by copying the partitions to another hard disk.

### Security and privacy

- **Acronis DriveCleanser**

Acronis DriveCleanser utility provides for secure destruction of data on your hard disk.

### Disk management

- **Add new disk**

Add new disk wizard helps you to add a new hard disk drive to your computer. You will be able to prepare the new hard disk drive by creating and formatting new partitions on this hard disk.

### Image mounting

- **Mount image**

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**

With this tool you can unmount the temporary logical drives you have created to explore an image.

## 6.1 Adding a new hard disk

If you do not have enough space for your data, you can either replace the old disk with a new higher-capacity one, or add a new disk only to store data, leaving the system on the old disk.

### To add a new hard disk:

1. Shut down your computer, and then install the new disk.
2. Turn on your computer.
3. Click the **Start** button —> **Acronis** (product folder) —> **True Image** —> **Tools and Utilities** —> **Add New Disk**.
4. Follow the wizard steps.
5. On the **Finish** step, ensure that the configured disk layout suits your needs, and then click **Proceed**.

### In this section

Selecting a hard disk .....54

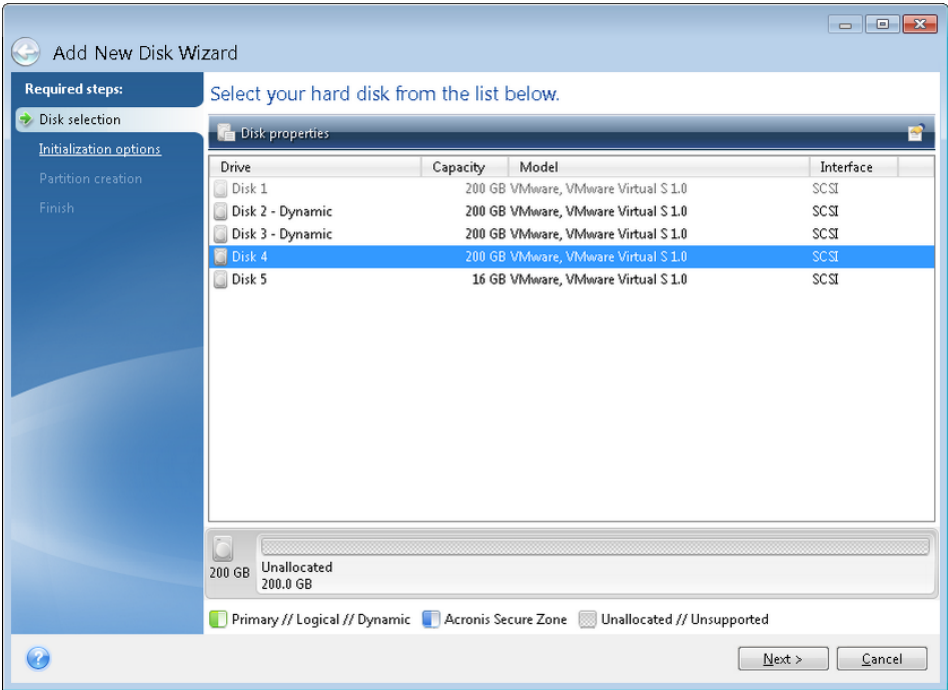
Selecting initialization method .....55

Creating new partitions .....55

6.1.1 Selecting a hard disk

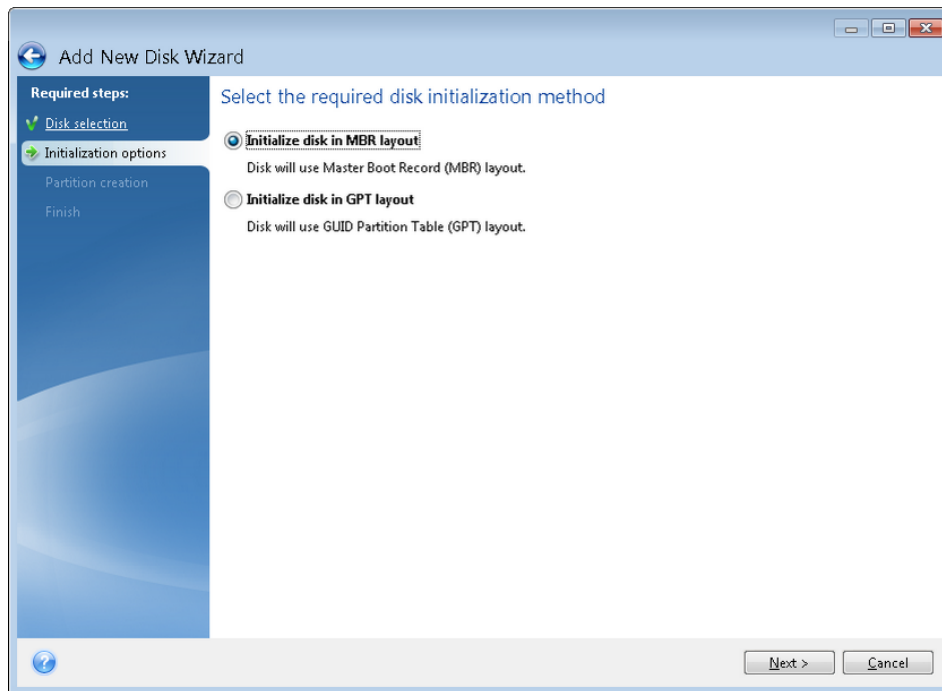
Select the disk that you have added to the computer. If you have added several disks, select one of them and click **Next** to continue. You can add the other disks later by restarting the Add New Disk Wizard.

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



## 6.1.2 Selecting initialization method

Acronis True Image WD Edition 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**.

---

*If you use a 32-bit version of Windows XP, the GPT initialization method will be unavailable and the **Initialization options** step will be absent.*

---

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

## 6.1.3 Creating new partitions

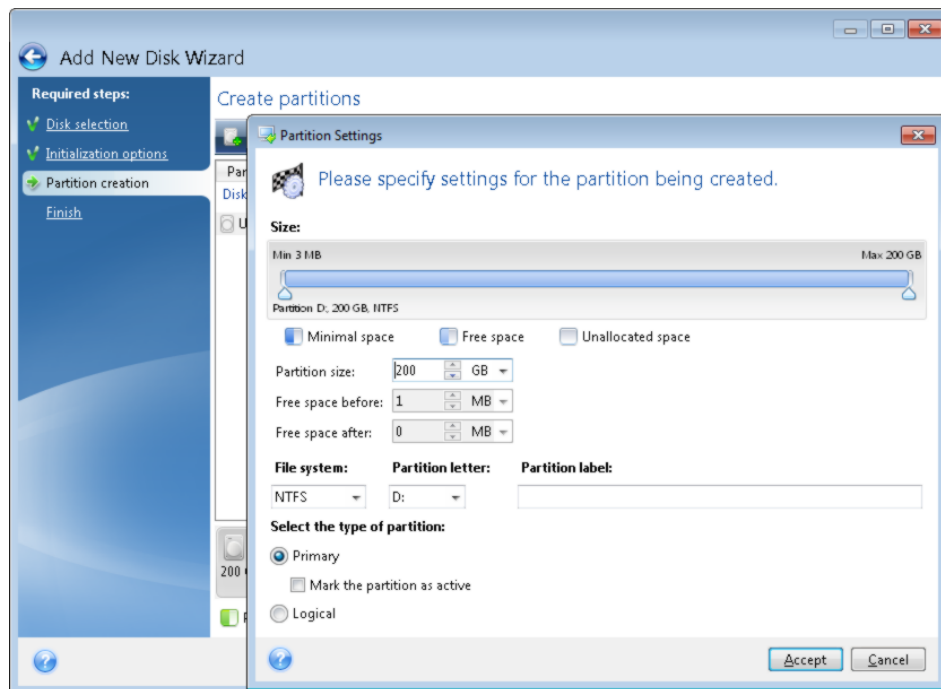
To use the space on a hard disk, it must be partitioned. Partitioning is the process of dividing the hard disk's space into logical divisions which are called partitions. Each partition may function as a separate disk with an assigned drive letter, its own file system, etc.

### 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. 56) for details.

3. Click **Accept**.



### 6.1.3.1 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.

## 6.2 Creating bootable rescue media

You can run Acronis True Image WD Edition 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 WD Edition 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:
  - 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.
- Create WinPE-based media with Acronis plug-in.

## 6.2.1 Acronis Media Builder

You can run Acronis True Image WD Edition 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 will need bootable media that has a copy of the standalone Acronis True Image WD Edition version installed on it.

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

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

### Notes

- If you have chosen not to install the Bootable Media Builder during Acronis True Image WD Edition installation, you will not be able to use this feature.
- When booting from the Rescue Media, you cannot perform backups to disks or partitions with Ext2/Ext3/Ext4, ReiserFS, and Linux SWAP file systems.
- Please keep in mind that the backups created by the later program version may be incompatible with the previous program versions. Due to this reason, we strongly recommend that you create a new bootable media after each Acronis True Image WD Edition upgrade.
- When booting from the rescue media and using a standalone version of Acronis True Image WD Edition you cannot recover files and folders encrypted with use of the encryption available in Windows XP and later operating systems.

### 6.2.1.1 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 WD Edition.
3. In the **Tools** section, click **Rescue Media Builder**.
4. Choose a media type that you want to create. Refer to Acronis Media Builder 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**.

- **WIM image file** (available only for WinPE-based media)

Acronis True Image adds the Acronis plug-in to the .wim file from Windows AIK or Windows ADK. You will need to specify a name for the new .wim file and the destination folder.

To create a bootable media by using a .wim file, you first need to convert it to an .iso file. Refer to Creating an .iso file from a .wim file for details.

6. Click **Proceed**.

### 6.2.1.2 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 (nousb, 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.

## 6.2.2 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.

If you purchased a boxed version of the product that has a bootable CD, please test this CD.

### 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.
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 **True Image**.

---

*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 Acronis 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 you to 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**

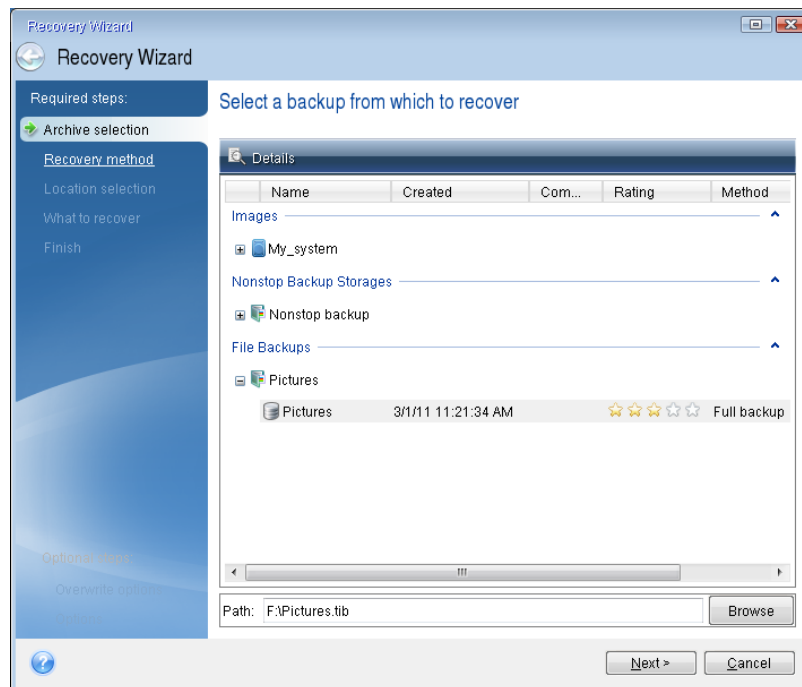
1. If you have file backups, start Recovery Wizard by clicking **Recovery** -> **File Recovery** on the toolbar.

---

*If you have only disk and partition backup, Recovery Wizard also starts and the recovery procedure is similar. In such a case, you need to select **Recover chosen files and folders** at the **Recovery Method** step.*

---

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

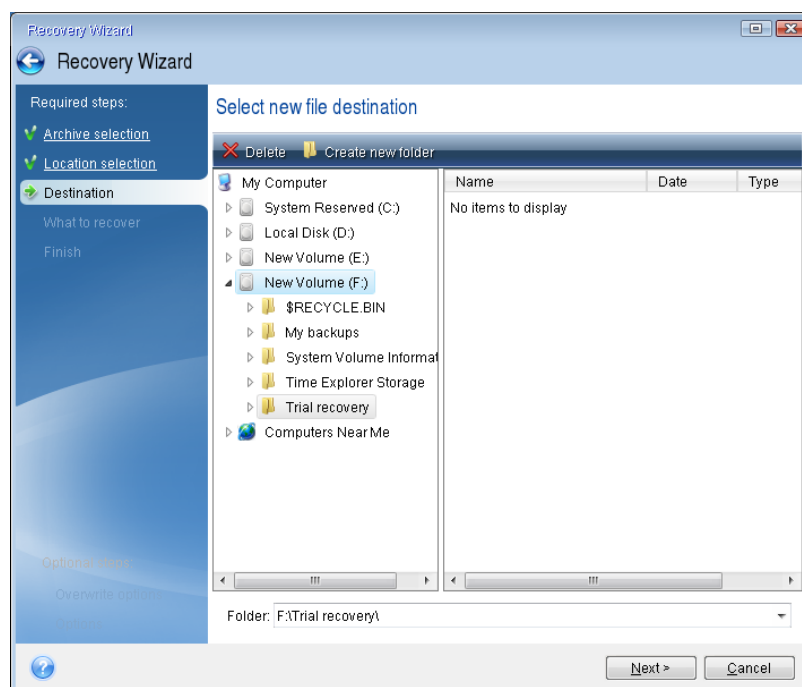


3. When recovering files with the rescue CD you are able to select only a new location for the files to be recovered. Therefore just click **Next** at the **Location selection** step.
4. After the **Destination** window opens, check that all your drives are shown under **My Computer**.

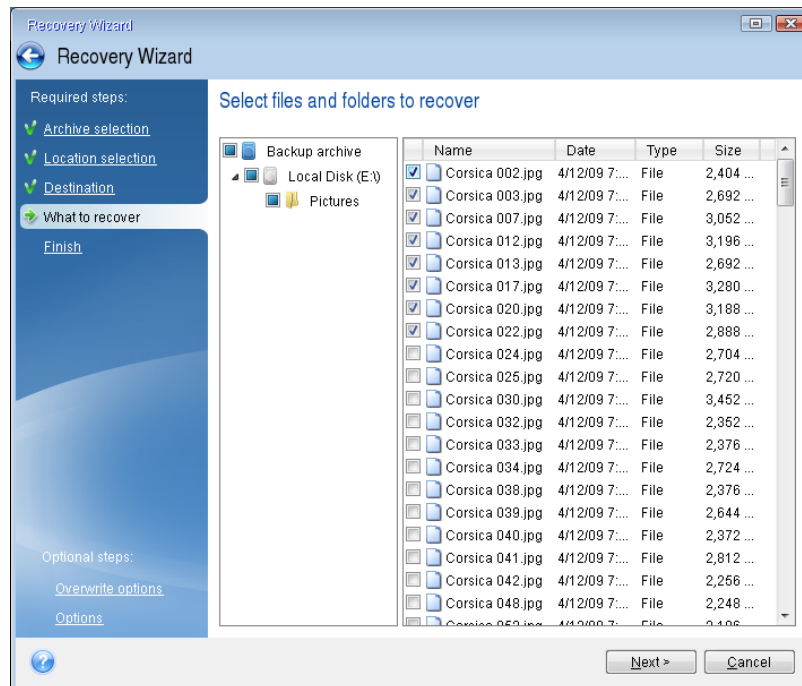
*If you store your backups on the network, you should also check that you can access the network.*

*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 WD Edition.*



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 WD Edition.

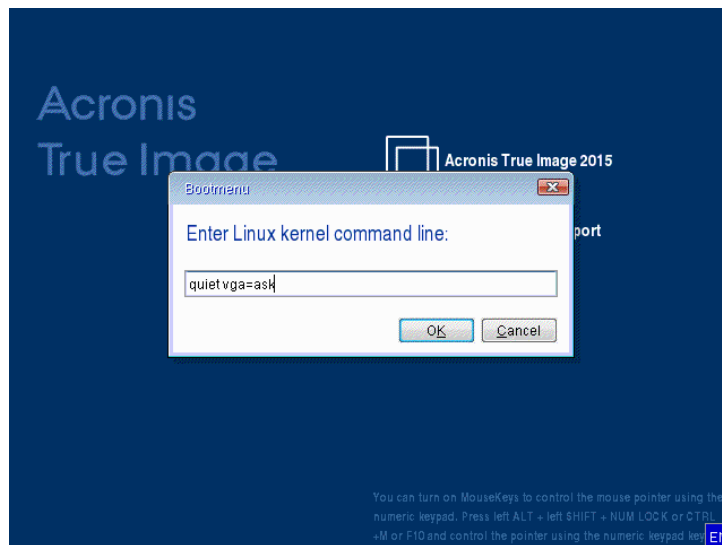
Now you can be reasonably sure that your rescue CD will help you when needed.

### 6.2.2.1 Selecting video mode when booting from the rescue media

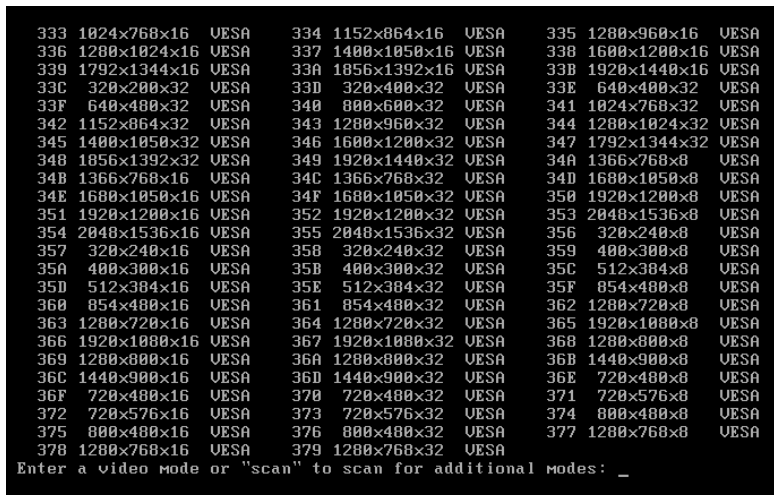
When booting from the rescue media the optimal video mode is selected automatically depending on the specifications of your video card and monitor. However, sometimes the program can select the wrong video mode, which is unsuitable for your hardware. In such case you can select a suitable video mode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

1. Start booting from the rescue media. When the boot menu appears, hover the mouse over **True Image** item and press the F11 key.

- When the command line appears, type "vga=ask" (without quotes) and click **OK**.



- Select **True Image** in the boot menu to continue booting from the rescue media. To see the available video modes, press the Enter key when the appropriate message appears.
- 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).



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

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

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

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

## 6.3 Acronis Extended Capacity Manager

The Acronis Extended Capacity Manager (ECM) allows your operating system (OS) to support large capacity disks that have the MBR partition style. You are able to use the disk space beyond 2 TB. This



free space will be recognized as a separate disk, and will be usable by your operating system and applications as if it was a regular physical hard disk.

## When it is needed

If you have hard disks larger than 2 TB and your OS does not see the entire disk space, you can resolve this issue through one of the following options:

- Use Extended Capacity Manager. You can use this tool for all cases, because it doesn't delete any data on a large disk. Therefore, we recommend that you use this tool if your large disk contains an operating system or useful data. See details below.
- Convert the MBR disk to GPT disk. The easiest way to do this is by using Windows built-in **Disk Management** utility. Note that this utility erases all data on the disk while converting it to GPT.

The following table helps you to find out which option to choose. It relates only to disks larger than 2 TB.

	MBR disk containing OS or data	Clear MBR disk without OS and data
Windows XP (x32)	Use ECM	Use ECM
Windows XP (x64)	Use ECM	Convert to GPT
Windows Vista	Use ECM	Convert to GPT
Windows 7	Use ECM	Convert to GPT
Windows 8	Use ECM	Convert to GPT

## How it works

Acronis Extended Capacity Manager wizard displays all hard disks larger than 2 TB (unallocated or with MBR partition style). You can see the disk space which Windows recognizes and allocates. This space is called Windows Native Capacity in the wizard.

The space beyond 2 TB is displayed as Extended Capacity. You can enable Extended Capacity Disks, and once it is done, this space becomes visible to the operating system and ready for disk management operations.

## How to use it

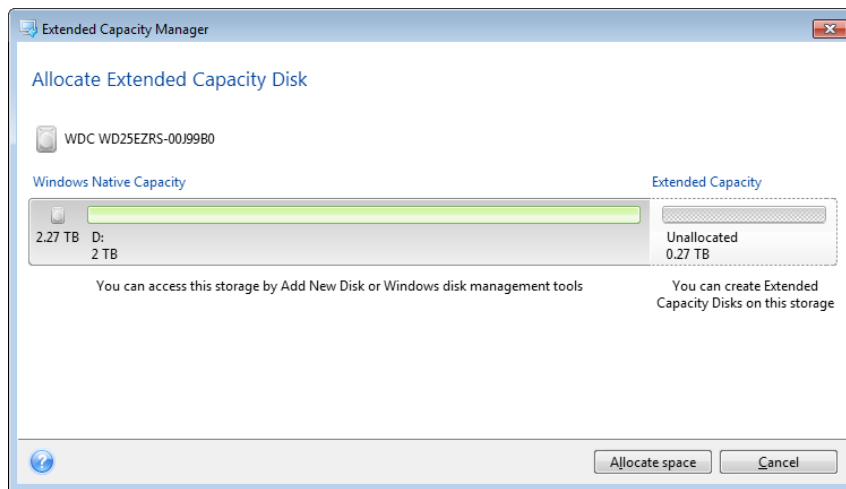
1. To start Acronis Extended Capacity Manager, select the **Tools** tab, then click **More tools**, and then click **Acronis Extended Capacity Manager**.

---

*If the program does not find any MBR disks with a capacity of more than 2 TB, it displays a message that the entire disk space is accessible and you do not need to use Acronis Extended Capacity Manager.*

---

2. Acronis Extended Capacity Manager shows the Extended Capacity available for allocation.



3. Click **Allocate space** to see the possible disk space allocation in the next step.  
After clicking the **Apply** button, an Extended Capacity Disk will be emulated on your physical disk. If your physical disk's capacity is more than 4 TB and your operating system does not support the GPT partition style, the program creates several MBR Extended Capacity Disks.

---

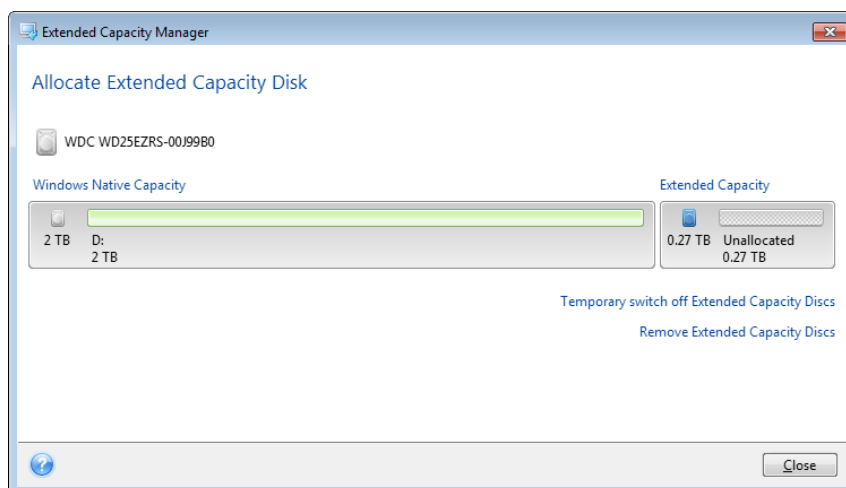
*Note that Extended Capacity Disks are not bootable, though most of their properties are the same as that of physical disks.*

---

4. Click **Close** to exit the Acronis Extended Capacity Manager.

## What else you can do

After allocating the space, you can temporarily switch off the Extended Capacity Disks by clicking **Temporary switch off Extended Capacity Disks**. This makes the Extended Capacity Disks invisible for disk management tools, though the disk space will remain allocated and you will be able to make these partitions visible again later. To do this, start the Acronis Extended Capacity Manager and then click **Allocate space**.



To remove the Extended Capacity Disks, click **Remove Extended Capacity Disks** and then click the **Apply** button in the next step. These disks will be removed from your system, and the disk space beyond 2 TB will become inaccessible. To allocate this space later, you need to start the Extended Capacity Manager again and then repeat the wizard's steps.

You will be able to continue using the Extended Capacity Disks even after uninstalling Acronis True Image WD Edition. During uninstallation, you will be asked whether you want to remove the Extended Capacity Disk. If you choose not to remove the disk, it will remain usable.

## 6.4 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. 68) 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. 67) 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. 68) 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. 72) 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.*

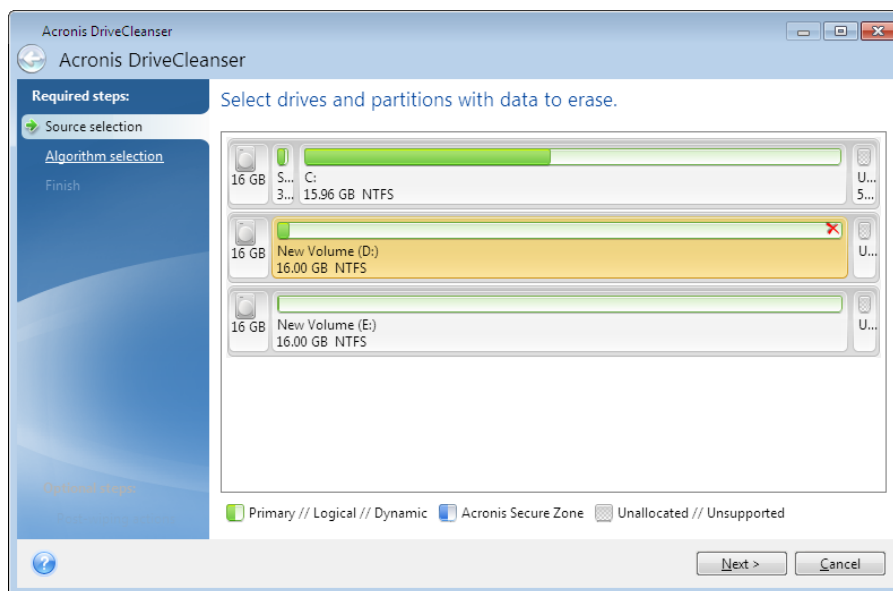
---

### 6.4.1 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 (  ).




---

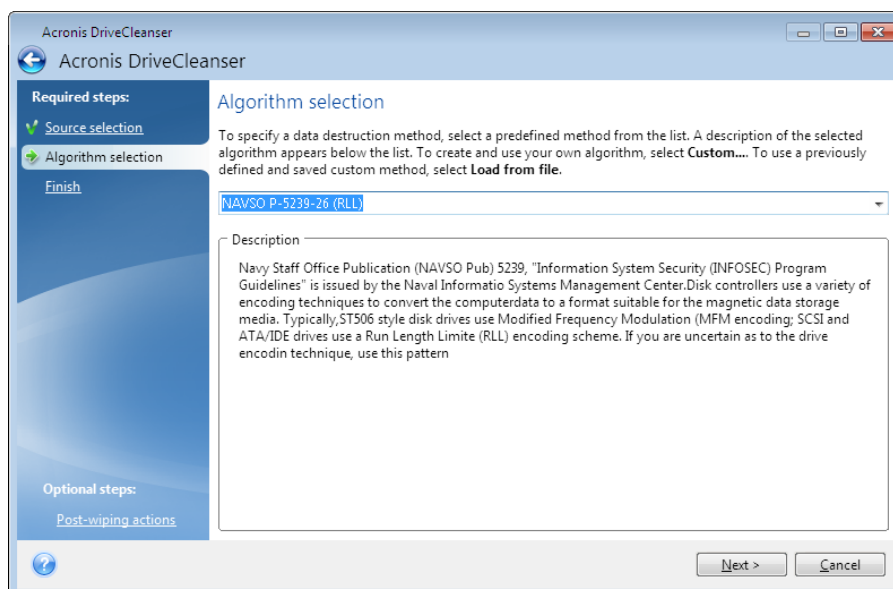
*Acronis DriveCleanser cannot wipe partitions on dynamic and GPT disks, so they will not be shown.*

---

## 6.4.2 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. 69) 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.



## 6.4.2.1 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 [http://www.cs.auckland.ac.nz/~pgut001/pubs/secure\\_del.html](http://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 <sup>st</sup> pass – randomly selected symbols to each byte of each sector, 2 – complementary to written during the 1 <sup>st</sup> pass; 3 – random symbols again; 4 – writing verification.
2.	United States: NAVSO P-5239-26 (RLL)	4	1 <sup>st</sup> pass – 0x01 to all sectors, 2 – 0x27FFFFFF, 3 – random symbol sequences, 4 – verification.
3.	United States: NAVSO P-5239-26 (MFM)	4	1 <sup>st</sup> pass – 0x01 to all sectors, 2 – 0x7FFFFFFF, 3 – random symbol sequences, 4 – verification.
4.	German: VSITR	7	1 <sup>st</sup> – 6 <sup>th</sup> – alternate sequences of: 0x00 and 0xFF; 7 <sup>th</sup> – 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 <sup>th</sup> to 4 <sup>th</sup> security level systems.  Randomly selected symbols (numbers) to each byte of each sector for 3 <sup>rd</sup> to 1 <sup>st</sup> 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 <sup>st</sup> pass – 0xFF, 2 <sup>nd</sup> 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.

## 6.4.2.2 Creating custom algorithm

### Algorithm definition

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

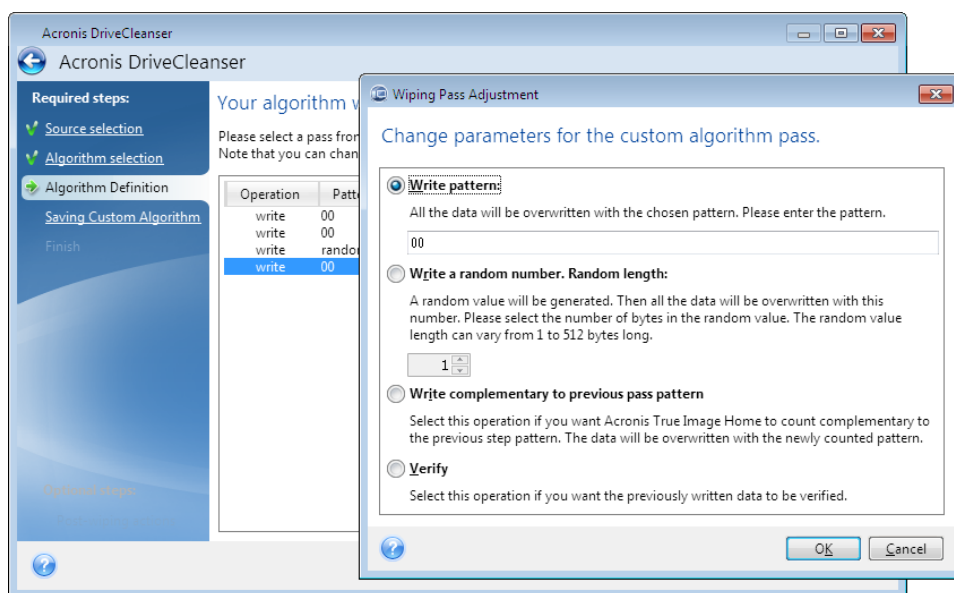
The table has the following legend:

- 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**.

### Wiping pass adjustment

The Wiping Pass Adjustment window allows you to define the pattern to be written to disk (hexadecimal value).

This is what the window control elements mean: You may enter any hexadecimal value into the field under the **Write pattern** switch to write it to a hard disk during any pass (during the first pass in this case).

By setting the switch to **Write a random number** position, you will first select to write a random value to disk, and specify the length of the random value in bytes in the field below.

The U.S. standard provides the writing of random values to each byte of each disk sector during the first pass, so set the switch to **Write a random number** position and enter 1 into the field.

Click the **OK** button to continue.

You will be taken to the algorithm definition window again and will see that the former record (write – 00) was replaced by write – random, 1 byte.

To define the next pass, click the **Add** button.

You will see the already-familiar window, but this time there will be more switch positions available: two additional positions will be available for selection:

- **Write complementary to previous pass pattern:** As during the second pass of the U.S. standard, each disk sector is filled with hexadecimal values that are complementary to those written during the previous pass. Therefore you should set the switch to the Write complementary to previous pass pattern position and click the **OK** button.

You will be taken to the algorithm definition window again. In this window, the second record looks like this: write – complementary to previous step pattern.

- **Verify**

Following the U.S. data destruction standard specification, define third and fourth data overwriting passes.

In the same way, you can create any data destruction algorithm to match your security requirements.

### 6.4.2.3 Saving custom algorithm

In the next Saving Custom Algorithm window, you will be able to save the algorithm you have created. This will be useful if you are going to use it again.

In order to save your algorithm, you need to give it a filename and define the path in the Select file field or locate an existing file on the disk.

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

### 6.4.3 Disk wiping summary

The summary window contains the list of operations to be performed.

Note that after you click the **Proceed** button, the selected partitions will be wiped permanently. So the button is disabled until you select the **Wipe the selected partitions irreversibly** check box.

Click the **Proceed** button to start the listed operations.

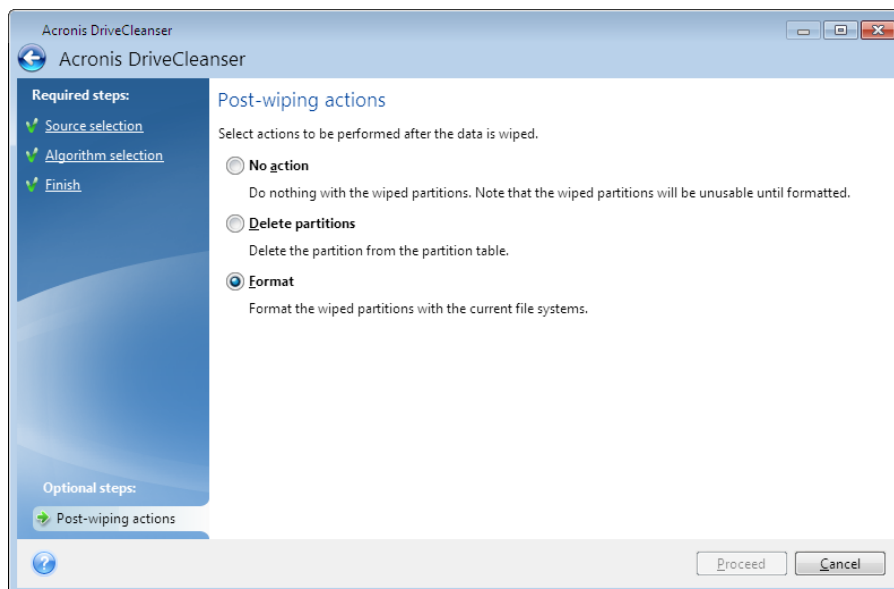
Click the **Options** button to perform the optional steps.

Click the **Cancel** button to exit the wizard without performing any operations.

### 6.4.4 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).



## 6.5 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**.

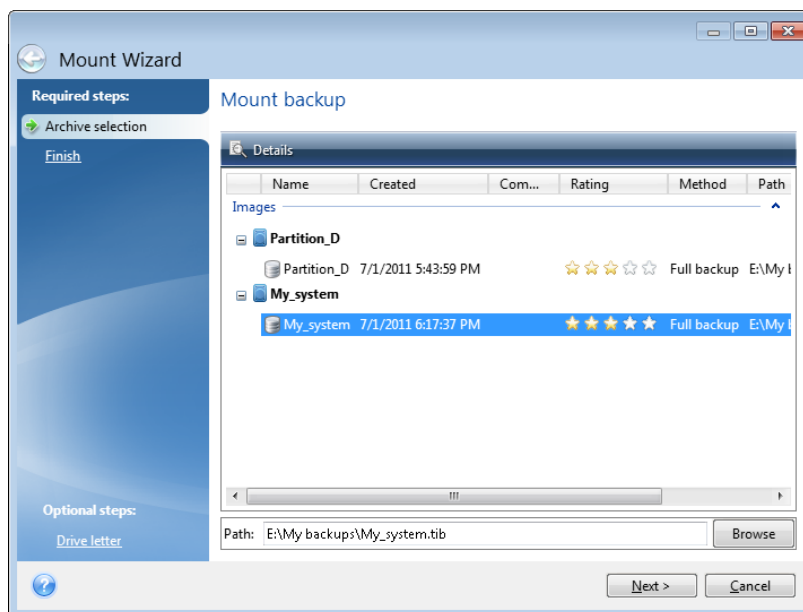
The Mount wizard opens.

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.

## 6.6 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.

## 7 Troubleshooting

### In this section

Acronis System Report..... 74

### 7.1 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 -> Acronis True Image WD Edition -> Tools and Utilities -> Acronis System Report**.
- Press **CTRL+F7**. Note that you can use the key combination even when Acronis True Image WD Edition 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**.

You can place the tool on your bootable rescue media as a separate component 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 WD Edition. 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.

**To place the Acronis System Report tool on a bootable rescue media:**

- Select the **Acronis System Report** check box on the **Rescue Media Content Selection** page of the **Acronis Media Builder** wizard.
- Click **Next** to continue.

**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 WD Edition installation folder. To do so, enter:

```
cd C:\Program Files (x86)\Acronis\True Image
```

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>
```

## Copyright Statement

Copyright © Acronis International GmbH, 2002-2015. 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 <http://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; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,145,607; 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 and patent pending applications.

## 8 Glossary of Terms

### B

#### Backup

1. The same as Backup operation (p. 77).
2. A set of backup versions created and managed by using backup settings. A backup can contain multiple backup versions created using full (p. 77) and incremental (p. 78) 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. 77). 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 files created by Acronis True Image WD Edition have a TIB extension. The TIB files resulting from consolidation of backup versions are also called backup versions.

#### Backup version chain

Sequence of minimum 2 backup versions (p. 77) 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 WD Edition.

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

#### Differential backup

---

**Note:** *Differential backups are not available in this product edition. To access this feature, please upgrade to full version.*

---

1. A backup method used for saving data changes that occurred since the last full backup version (p. 78) within a backup.
2. A backup process that creates a differential backup version (p. 77).

#### Differential backup version

---

**Note:** *Differential backups are not available in this product edition. To access this feature, please upgrade to full version.*

---

A differential backup version stores changes to the data against the latest full backup version (p. 78). You need access to the corresponding full backup version to recover the data from a differential backup version.

#### Disk backup (Image)

A backup (p. 77) 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 WD Edition 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. 78).

### Full backup version

A self-sufficient backup version (p. 77) 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. 77).

### Incremental backup

---

**Note:** Incremental backups are not available in this product edition. To access this feature, please upgrade to full version.

---

1. A backup method used for saving data changes that occurred since the last backup version (p. 77) (of any type) within a backup.
2. A backup process that creates an incremental backup version (p. 78).

### Incremental backup version

---

**Note:** Incremental backups are not available in this product edition. To access this feature, please upgrade to full version.

---

A backup version (p. 77) that stores changes to the data against the latest backup version. You need access to other backup versions from the same backup (p. 77) to restore data from an incremental backup version.

## N

### Nonstop backup

---

**Note!** Nonstop Backup is not available in this product edition. To access this feature, please upgrade to full version.

---

Nonstop backup actually is a disk/partition or file backup that is created using the Acronis Nonstop Backup feature. This is a set of one full backup version (p. 78) and a sequence of incremental backup versions (p. 78) that are created at short intervals. It gives almost continuous protection of data, that is, it allows recovery of previous data state at any recovery point you need.

### Nonstop protection

---

**Note!** Nonstop Backup is not available in this product edition. To access this feature, please upgrade to full version.

---

Nonstop protection - the process that the Nonstop Backup feature performs when it is turned on.

## O

### Online backup

Online backup - a backup that is created using Acronis Online Backup. Online backups are stored in a special storage named the Online storage, accessible over the Internet. The main advantage of an online backup is that all backups are stored on the remote location. It gives a guarantee that all backed up data will be safe independently of a user local storages. To begin to use the Online storage a user should subscribe to the service.

## R

### Recovery

Recovery is a process of returning of a corrupted data to a previous normal state from a backup (p. 77).

# V

## Validation

An operation that checks whether you will be able to recover data from a particular backup version (p. 77).

When you select for validation...

- a full backup version (p. 78) - the program validates the full backup version only.
- an incremental backup version (p. 78) - 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.