Acronis

acronis.com

# Acronis True Image for SANDISK

User Guide for Windows

REVISION: 1/29/2026

# Table of contents

# Copyright statement



# Acronis patented technologies

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

# Introduction

## What is Acronis True Image for SANDISK?

Acronis True Image for SANDISK is a solution that ensures the security of all your information. It can back up your documents, photos, and selected partitions, and even the entire disk drive, including operating system, applications, settings, and all of your data. One of its main advantages is the data protection.

Backups allow you to recover your computer system should a disaster occur, such as losing data, accidentally deleting critical files or folders, or suffering a complete hard disk crash.

**Key features:**

- Backing up your computer
- Acronis bootable media
- Hard disk cloning
- Security and privacy tools

Learn how to protect your computer: "Protecting your system".

## Backups created before Acronis True Image for SANDISK 2020

Acronis True Image for SANDISK currently mostly uses the TIBX backup format, which is more reliable and convenient than the previously used TIB format.

Backing up in the TIBX format supports all backup schemes. As opposed to the TIB format, which saves every backup version as a separate file, the TIBX format saves full and differential backup versions as separate files, while incremental backup versions are automatically merged into their base backups (full or differential).

To compare naming of a .tibx archive with a .tib archive in detail, see Backup file naming.

## System requirements and supported media

### Minimum system requirements

Acronis True Image for SANDISK requires the following hardware.

- At least one storage device by SANDISK hardware brands, including WD, SANDISK, and G-Tech, or a network attached storage by SANDISK.
- Intel CORE 2 Duo (2 GHz) or equivalent processor that supports SSE instructions.

**Note**
Acronis True Image for SANDISK supports only Windows systems based on x86 architecture. Devices running Windows on ARM processors (such as some lightweight laptops and tablets) are not supported.

- 2 GB RAM
- 7 GB of free space on the system hard disk
- CD-RW/DVD-RW drive or USB drive for bootable media creation
  - Required free space for Linux is about 660 MB.
  - Required free space for Windows is about 700 MB.
- Screen resolution is 1024 x 768
- Mouse or other pointing device (recommended)

**Warning!**
Successful backup and recovery are not guaranteed for the installations on virtual machines.

## Other requirements

- You need to have administrator privileges to run Acronis True Image for SANDISK.

# Supported operating systems

Acronis True Image for SANDISK has been tested on the following operating systems.

- Windows 11 (including 25H2)
- Windows 10 32-bit & 64-bit

**Note**
- Beta builds are not supported. See Windows Insider Preview builds support.
- Windows Embedded, IoT editions, Windows 10 LTSB, Windows 10 LTSC, and Windows 10 in S mode are not supported.

Acronis True Image for SANDISK also lets you create a bootable CD-R/DVD-R or USB drive that can back up and recover a disk/partition on a computer running any Intel- or AMD- based PC operating system, including Linux®.

It is possible for the software to work on other Windows operating systems, but it is not guaranteed.

**Warning!**
Successful recovery is guaranteed only for the supported operating systems. Other operating systems can be backed up using a sector-by-sector approach, but they may become unbootable after recovery.

## Supported file systems

- NTFS
- Ext2/Ext3/Ext4
- ReiserFS(3)[1]
- Linux SWAP[2]
- HFS+/HFSX[3]
- FAT16/32/exFAT[4]

If a file system is not supported or is corrupted, Acronis True Image for SANDISK copies data sector by sector. This means the program reads all data blocks on the disk even if files or folders cannot be accessed normally. This method helps recover data from damaged or unknown file systems, but it does not indicate full support for them (for example, for ReFS or Windows Storage Spaces).

## Supported storage media

- Hard disk drives (HDD)
- Solid-state drives (SSD)
- Networked storage devices (except WD My Cloud Home and WD My Cloud Home Duo)
  - My Cloud (Sequoia)
  - My Cloud (Glacier)
  - WD Cloud for Japan
  - My Cloud Mirror
  - My Cloud Mirror (Gen 2)
  - My Cloud EX2
  - My Cloud EX2 Ultra
  - My Cloud EX2100
  - My Cloud EX4
  - My Cloud EX4100
  - My Cloud DL2100
  - My Cloud DL4100
  - My Cloud PR2100
  - My Cloud PR4100
- FTP servers

[1]File systems are supported only for disk or partition backup/recovery operations.

[2]File systems are supported only for disk or partition backup/recovery operations.

[3]Disk recovery, partition recovery, and cloning operations are supported without resizing.

[4]Disk recovery, partition recovery, and cloning operations are supported without resizing.

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

- CD-R/RW, DVD-R/RW, DVD+R (including double-layer DVD+R), DVD+RW, DVD-RAM, BD-R, BD-RE
- USB, eSATA, FireWire (IEEE-1394), SCSI, and Memory cards
  Acronis True Image for SANDISK supports USB interfaces of all versions (1.1, 2.0, 3.0, 3.1, 3.2), as well as USB-C and Thunderbolt storage devices. Actual performance depends on the system configuration, controller, and connection quality.

### Limitations on operations with dynamic disks

- Recovery of a dynamic volume as a dynamic volume with manual resizing is not supported.
- Disk cloning operation is not supported for dynamic disks.

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

# Installing and uninstalling Acronis True Image for SANDISK

You cannot install Acronis True Image for SANDISK in the same system where Acronis True Image or any other Cyber Protection software by Acronis is already installed.

***To install Acronis True Image for SANDISK***

1. Run the setup file.
   Before starting the setup process, Acronis True Image for SANDISK will check for a newer build on the website. If there is one, the newer version will be offered for installation.
2. Select the installation mode:
   - Click **Install** for the default installation.

   Acronis True Image for SANDISK will be installed on your system partition (usually C:).
3. When the installation is complete, click **Start application**.
4. Read and accept the terms of the license agreements for Acronis True Image for SANDISK and Bonjour.
   Bonjour software will be installed on your computer for advanced support of NAS devices. You can uninstall the software at any time.

When Acronis True Image for SANDISK is started for the first time, it is activated automatically if it detects a SANDISK storage device. If the device is not detected automatically, click **Rescan** in the **Product activation required** window. See "Activating Acronis True Image for SANDISK" (p. 11) for details.

***To uninstall Acronis True Image for SANDISK completely***

1. Click **Start** > **Settings** > **Apps** > **Acronis True Image for SANDISK** > **Uninstall**.
2. Then follow the instructions on the screen. You may have to restart your computer afterwards to complete the task.

# Application settings

The **Settings** window contains general settings of Acronis True Image for SANDISK. To open it:

1. Open Acronis True Image for SANDISK.
2. In the Acronis True Image for SANDISK menu, click **Settings**.

The following settings are available:

- **Interface language**
  Select a preferred language from the list.
- **Application startup**
  - **Automatically check for updates at startup**
    See Installing and uninstalling Acronis True Image for SANDISK for details.
- **Customer insights**
  - **Allow Acronis to collect de-identified service usage information for analyzing and improving the service**
    If you agree to participate, Acronis will anonymously collect technical information to improve Acronis True Image for SANDISK. Personal data, such as name, address, phone number, email address, and keyboard input, will not be collected.

# Activating Acronis True Image for SANDISK

Acronis True Image for SANDISK is activated automatically when a SANDISK storage device is detected on your system. The license is valid for five years after the last addition of a storage device by SANDISK. When the license is about to expire, you will get a notification.

***To check the license expiration date***

To check the date when your license expires, click **About** on the sidebar.

***To extend the license by adding a new device***

1. Connect a new storage device by SANDISK.
2. Restart Acronis True Image for SANDISK. The device will be identified automatically.
3. You can manually start the search for the SANDISK device. To do that, on the sidebar, click **About**, and then click the **Prolong** button.

# Upgrading Acronis True Image for SANDISK

You can upgrade to the latest version of Acronis True Image.

Your backups created with a previous version of Acronis True Image for SANDISK are completely compatible with the newer version of Acronis True Image. After you upgrade, all of your backups will automatically be added to your backup list.

We strongly recommend that you create a new bootable media after each product upgrade.

***To purchase the full version***

1. Start Acronis True Image for SANDISK.
2. On the sidebar, click **About**, and then click **Upgrade**. The online store opens.
3. Click **Buy now**.
4. Provide your payment information and follow the on-screen instructions.

***To update Acronis True Image for SANDISK***

1. Start Acronis True Image for SANDISK.
2. On the sidebar, click **About**.
   If there is a new version available, you will see the appropriate message next to the current build number.
3. Click **Download and install**.
   Before you start downloading, make sure that your firewall will not block the download process.
4. When the new version is downloaded, click **Install now**.

To check for updates automatically, go to the **Settings** tab, and then select the **Automatically check for updates at startup** check box.

# Technical Support

If you need assistance with Acronis True Image for SANDISK, refer to the official support resources of SANDISK at https://www.sandisk.com/support.

# Getting started

## User interface language

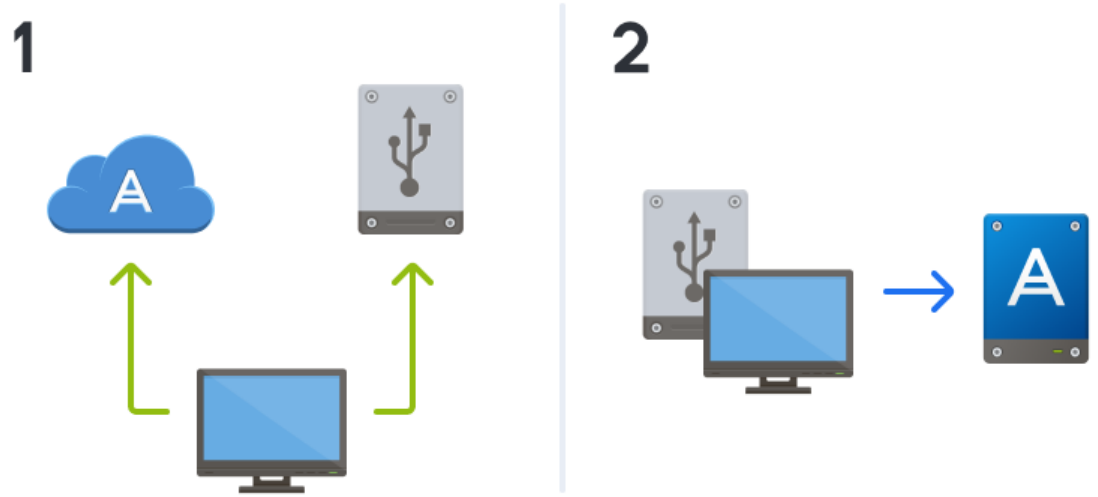
Before you start, select a preferred language for the Acronis True Image for SANDISK user interface. By default, the language is set in accordance with your Windows display language.

***To change the user interface language***

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

## Protecting your system

1. Back up your computer.
2. Create Acronis bootable media.




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

### Backing up your computer

***When should I back up my computer?***

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

Examples of these events include:

- You bought a new computer.
- You reinstalled Windows on your computer.

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

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

***How do I create a backup of my computer?***

You have two options to protect your system:

- **Entire PC backup (recommended)**
  Acronis True Image for SANDISK backs up all your internal hard drives in disk mode. The backup contains the operating system, installed programs, system settings, and all your personal data including your photos, music, and documents.
- **System disk backup**
  You can choose to back up your system partition or the entire system drive. See Backing up disks and partitions for details.

We do not recommend using nonstop backup as a primary way to protect your system, because the main purpose of this technology is protection of frequently changed files. For the safety of your system, use any other schedule. See examples in "Examples of custom schemes" (p. 51). See "Acronis Nonstop Backup" (p. 30) for more details about the Nonstop Backup feature.

***To back up your computer***

1. Start Acronis True Image for SANDISK.
2. On the sidebar, click **Backup**.
   If this is your first backup, you will see the backup configuration screen. If you already have some backups in the backup list, then click **Add backup**.
3. Click the **Backup source** icon, and then select **Entire PC**.
   If you want to back up your system disk only, then click **Disks and partitions**, and then select your system partition (usually C:) and the System Reserved partition (if any).
4. Click the **Backup destination** icon, and then select a storage place for the backup (see recommendation below).
5. Click **Back up now**.

As a result, a new backup box appears in the backup list. To create a new version of the backup in future, select the backup box from the list, and then click **Back up now**.

***Where do I store my disk backups?***

You can store your backups on internal or external drives, and network attached storage (NAS) devices by SANDISK.

See Deciding where to store your backups for details.

***How many backup versions do I need?***

In most cases, you need 2-3 backup versions of your entire PC contents or your system disk, with a maximum of 4-6 (see above for information about when to create backups). You can control the number of backup versions by using automatic cleanup rules. See Custom schemes for details.

Remember, the first backup version (the full backup version) is the most important. It is the biggest one, because it contains all data stored on the disk. Further backup versions (the incremental and differential backup versions) may be organized in different schemes. These versions contain only data changes. That's why they are dependent on the full backup version and why the full backup version is so important.

By default, a disk backup is created by using the incremental scheme. This scheme is optimal, in most cases.

**Note**
For advanced users: it is a good idea to create 2-3 full backup versions and store them on different storage devices. This method is much more reliable.

## Creating Acronis bootable media

Acronis bootable media is a CD, DVD, USB flash drive, or other removable media from which you can run Acronis True Image for SANDISK when Windows cannot start. You can make a media bootable by using Acronis Media Builder.

***To create Acronis bootable media***

1. Insert a CD/DVD or plug in a USB drive (USB flash drive, or an HDD/SSD external drive).
2. Start Acronis True Image for SANDISK.
3. On the sidebar, click **Tools**, and then click **Rescue Media Builder**.
4. On the first step, select **Simple**.
5. Select the device to use to create the bootable media.
6. Click **Proceed**.

***To use Acronis bootable media***

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

1. Connect the bootable media to your computer (insert the CD/DVD or plug in the USB drive).
2. Arrange the boot order in BIOS so that your Acronis bootable media is the first device to be booted.
   See Arranging boot order in BIOS for details.
3. Boot your computer from the bootable media and select **Acronis True Image for SANDISK**.
   Once Acronis True Image for SANDISK is loaded, you can use it to recover your computer.

See Acronis Media Builder for details.

## Using WinPE- or WinRE-based bootable media

In addition to the standard Linux-based bootable media, you can create bootable media based on Windows Preinstallation Environment (WinPE) or Windows Recovery Environment (WinRE). Such media may provide better hardware compatibility, for example with new storage controllers or network adapters.

You create WinPE- or WinRE-based bootable media by using Acronis Media Builder, the same way as for other types of bootable media.

When you boot your computer from this media, the recovery procedure is the same as described in Recovering your computer.

For detailed step-by-step instructions, see the Knowledge Base article: How to restore your computer with WinPE-based or WinRE-based media.

# Backing up all data on your PC

***What is an Entire PC backup?***

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

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

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

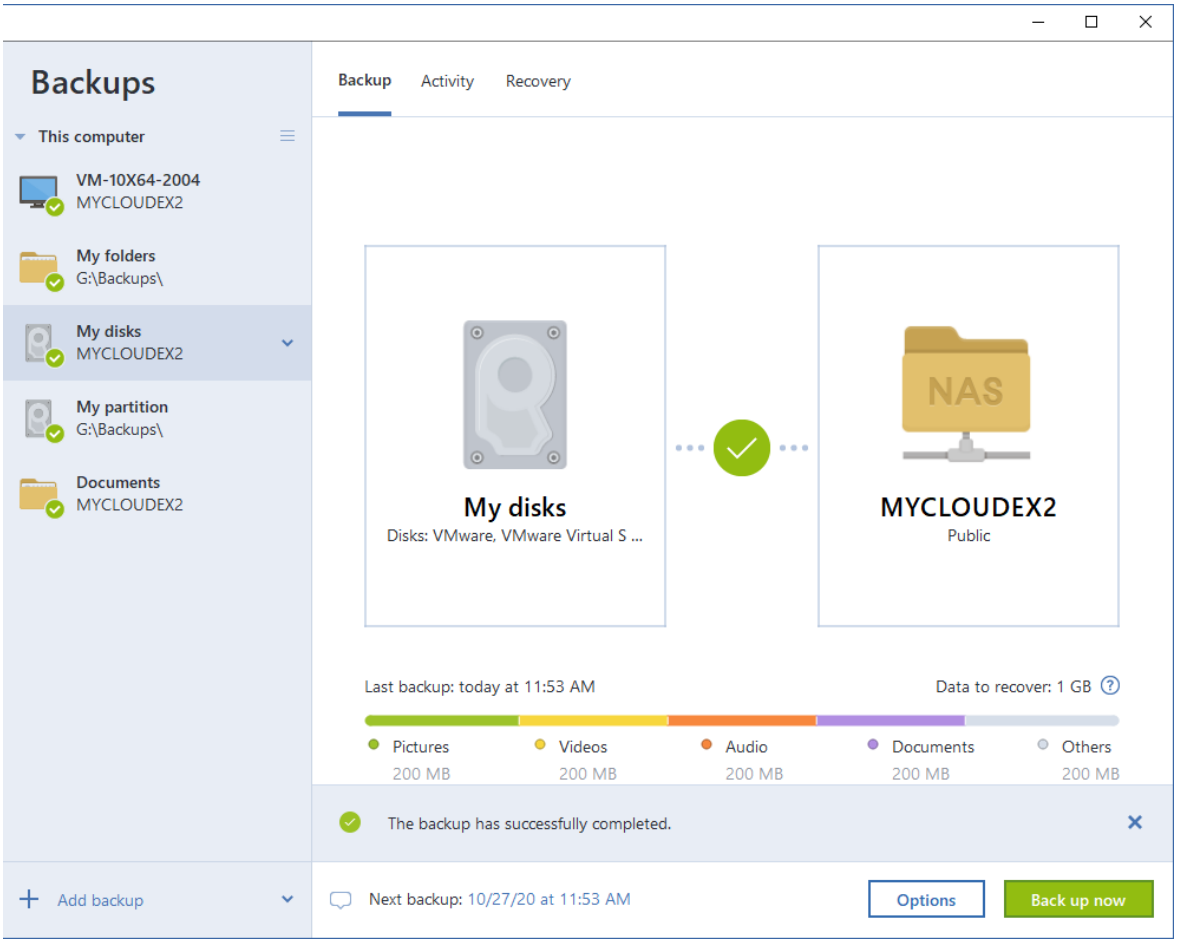
You can also recover specific files and folders from an Entire PC backup. See Backing up files and folders for details.

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

***To create an Entire PC backup***

1. Start Acronis True Image for SANDISK.
2. On the sidebar, click **Backup**.
3. Click the plus sign at the bottom of the backup list.
4. Click the **Backup source** icon, and then select **Entire PC**.

5. Click the **Backup destination** icon, and then select a destination for the backup.




6. [optional step] Click **Options** to set the options for the backup. For more information see Backup options.
7. Click **Back up now**.

# Backing up your files

To protect files such as documents, photos, music files, and video files, there is no need to back up the entire partition containing the files. You can back up specific files and folders and save them to the following storage types:

- **Local or network storage**

  This option is fast and easy. Use it to protect rarely changed files.

***To back up files and folders***

1. Start Acronis True Image for SANDISK.
2. On the sidebar, click **Backup**.
3. Click the **Backup source** icon, and then select **Files and folders**.
4. In the opened window, select the check boxes next to the files and folders that you want to back up, and then click **OK**.

5. Click the **Backup destination** icon, and then select a destination for backup:
   - **Your external drive** – When an external drive is plugged into your computer, you can select it from the list.
   - **NAS** – Select an NAS from the list of found NAS devices. If you have only one NAS, Acronis True Image for SANDISK will suggest using it as a backup destination by default.

     **Note**
     This option is available only if you have an internal or external SANDISK storage device attached to your system.

   - **Browse** – Select a destination from the folder tree.
6. Click **Back up now**.

See Backing up files and folders for details.

# Cloning your hard drive

This option is available only if you have an internal or external SANDISK storage device attached to your system.

## Why do I need it?

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

## Before you start

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

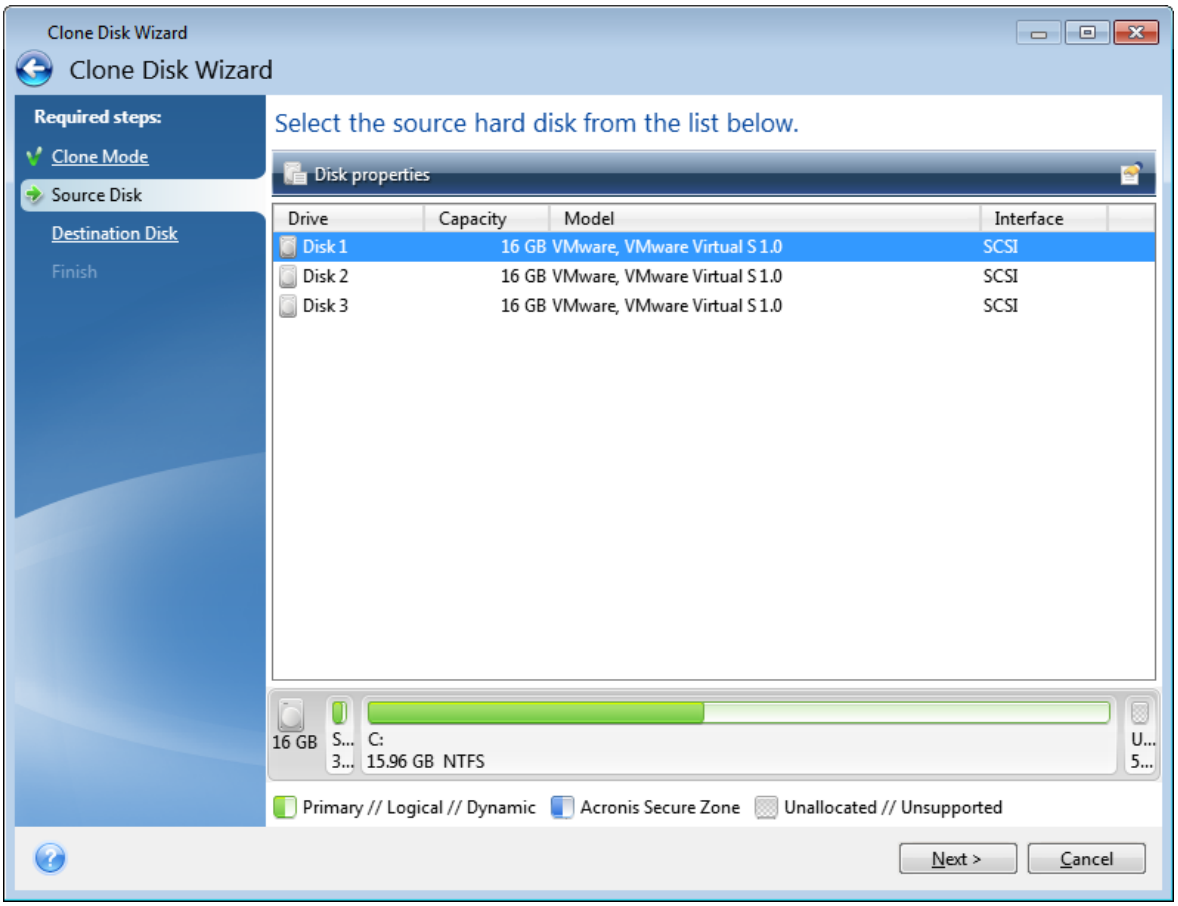
**Note**
It is recommended that your old and new hard drives work in the same controller mode. Otherwise, your computer might not start from the new hard drive.

## Cloning a disk

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

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

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




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

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

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

By default, Acronis True Image for SANDISK shuts down the computer after the clone process finishes.

# Recovering your computer

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

- Trying to determine the crash cause
- Preparing for recovery
- Recovering your system to the same disk

Let's consider two different cases:

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

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

1. Start Acronis True Image for SANDISK.
2. On the sidebar, click **Backup**.
3. From the backup list, select the backup that contains your system disk. The backup can be located on local or network storage.
4. On the right panel, click **Recovery**.
5. Depending on the backup type, click **Recover PC** or **Recover disks**.
6. In the opened window, select the backup version (the data state from a specific date and time).
7. Select the system partition and the System Reserved partition (if any) to be recovered.
8. Click **Recover now**.

**Note**
To complete the operation, Acronis True Image for SANDISK must restart your system.

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

1. Connect Acronis bootable media to your computer, and then run the special standalone version of Acronis True Image for SANDISK.
   See Step 2 Creating Acronis bootable media and Arranging boot order in BIOS for details.
   Alternatively, you can use WinPE- or WinRE-based bootable media to recover backups created in Acronis True Image for SANDISK.
2. On the Welcome screen, select **My disks** below **Recover**.
3. Select the system disk backup to be used for recovery. Right-click the backup and choose **Recover**.
   When the backup is not displayed, click **Browse** and manually specify the path to the backup.

   **Note**
   This option is available only if you have an internal or external SANDISK storage device attached to your system.

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

# 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:

- To recover an operating system when it is corrupted or cannot start (called disaster recovery). See Protecting your system for more details about protecting your computer from a disaster.
- To recover specific files and folders after they have been accidentally deleted or corrupted.

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

Recovery methods:

- **Full recovery** can be performed to the original location or to a new one.
  When the original location is selected, the data in the location is completely overwritten with the data from the backup. In case of a new location, the data is just copied to the new location from the backup.

***Backup versions***

Backup versions are the file or files created during each backup operation. The number of versions created is equal to the number of times the backup is executed. So, a version represents a point in time to which the system or data can be restored.

Backup versions represent full, incremental and differential backups - see Full, incremental and differential backups.

The backup versions are similar to file versions. The file versions concept is familiar to those who use a Windows 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 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.
- Back up your old disk drive, and then recover it to the new one.

***Backup file format***

Acronis True Image for SANDISK usually saves backup data in the proprietary TIBX format using compression. The data from .tibx file backups can be recovered only through Acronis True Image for SANDISK, in Windows or in the recovery environment.

Acronis Nonstop Backup uses a special hidden storage for data and metadata. The backed up data is compressed and split into files of about 1 GB. These files also have a proprietary format and the data they contain can be recovered only with the help of Acronis True Image for SANDISK.

***Backup validation***

The backup validation feature allows you to confirm that your data can be recovered. The program adds checksum values to the data blocks being backed up. During backup validation, Acronis True Image for SANDISK 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.

***Scheduling***

For your backups to be really helpful, they must be as up to date as possible. Schedule your backups to run automatically and on a regular basis.

***Deleting backups***

When you want to delete backups and backup versions you no longer need, do it by using the tools provided by Acronis True Image for SANDISK.

Acronis True Image for SANDISK stores information on the backups in a metadata information database. Therefore, deleting unneeded backup files in File Explorer will not delete information about these backups from the database. This will result in errors when the program tries to perform operations on the backups that no longer exist.

# 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 for SANDISK 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".

***What does a disk/partition backup contain?***

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:

a. Boot code.
b. File system meta data, including service files, file allocation table (FAT), and partition boot record.
c. 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).

***What is excluded from disk backups?***

To reduce image size and speed up image creation, by default Acronis True Image for SANDISK only stores the hard disk sectors that contain data.

Acronis True Image for SANDISK excludes the following files from a disk backup:

- pagefile.sys
- hiberfil.sys (a file that keeps RAM contents when the computer goes into hibernation)

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

# Full, incremental and differential backups

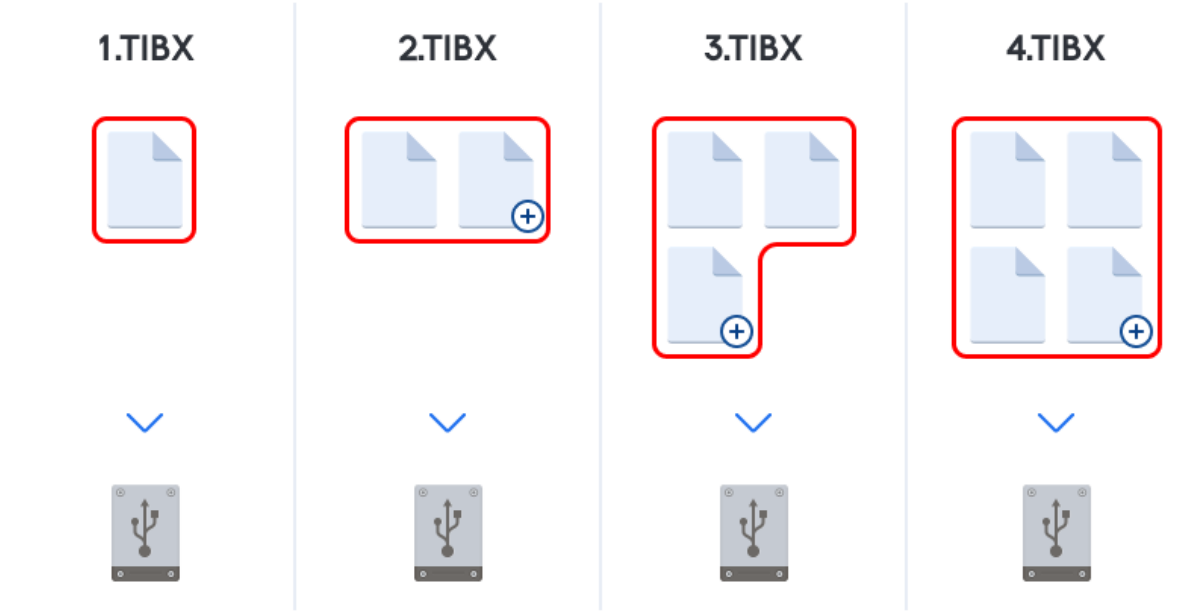
Acronis True Image for SANDISK offers three backup methods: full, incremental, and differential.

## 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. Acronis True Image for SANDISK saves the entire document every time you run backup.

1.tibx, 2.tibx, 3.tibx, 4.tibx – files of 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.

**Recovery:** In the example above, to recover the entire work from the 4.tibx file, you need to have only one backup version – 4.tib.

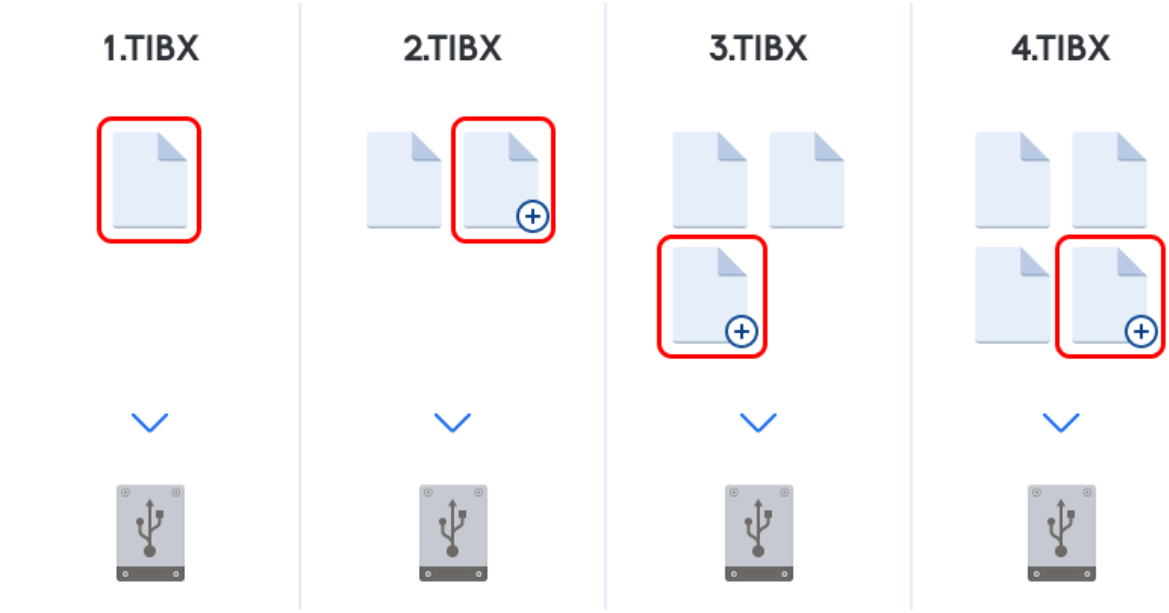
## Incremental method

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. Acronis True Image for SANDISK saves the new page every time you run backup.

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

- 1.tibx – file of full backup version.
- 2.tibx, 3.tibx, 4.tibx – files of 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.

**Recovery:** In the example above, to recover the entire work from the 4.tibx file, you need to have all the backup versions – 1.tibx, 2.tibx, 3.tibx, and 4.tibx. Therefore, if you lose an incremental backup version or it becomes corrupted, all later incremental versions are unusable.

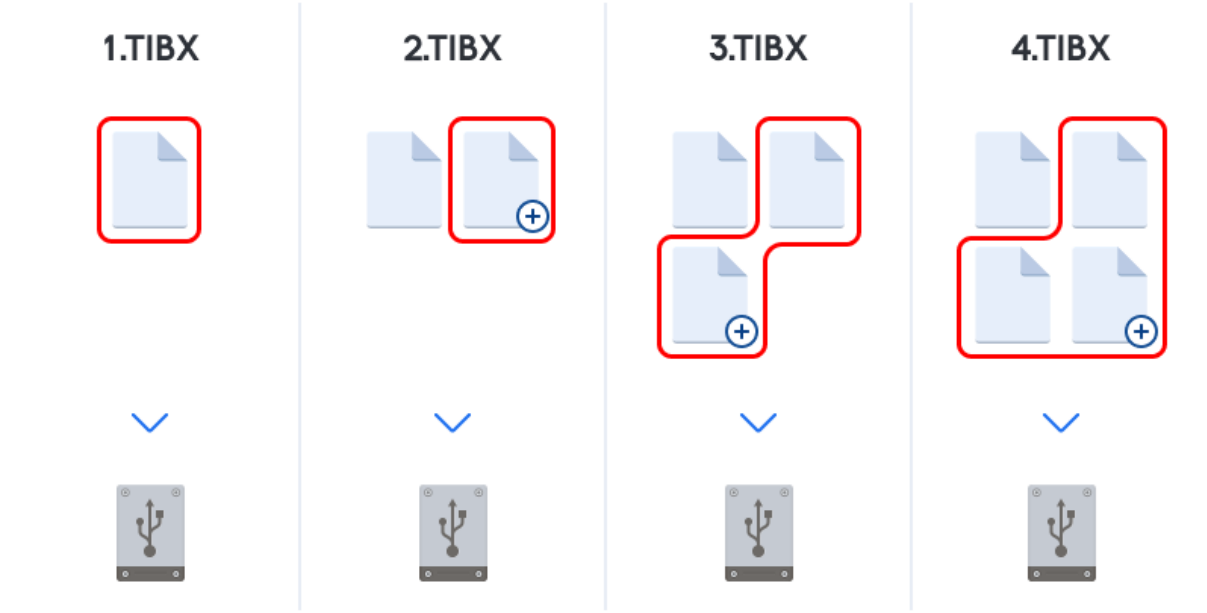
## Differential method

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. Acronis True Image for SANDISK 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.tibx – file of full backup version.
- 2.tibx, 3.tibx, 4.tibx – files of differential backup versions.




**Additional information**

Differential method is an intermediate between the first two approaches. It takes less time and space than a full one, but more than an incremental one. To recover data from a differential backup version, Acronis True Image for SANDISK 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.

**Recovery:** In the example above, to recover the entire work from the 4.tibx file, you need to have two backup versions – 1.tibx and 4.tibx.

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

**Note**
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.

## Changed Block Tracker (CBT)

The CBT technology accelerates the backup process when creating local incremental or differential disk-level backup versions. Changes to the disk content are continuously tracked at the block level. When a backup starts, the changes can be immediately saved to the backup.

# Deciding where to store your backups

Acronis True Image for SANDISK supports quite a few of storage devices. For more information, see "Supported storage media" (p. 9).

The table below shows possible backup destinations for your data.

| | HDD* | SSD* | USB flash drive | File server, NAS or NDAS | Network share | SMB | FTP | DVD | Memory card |
|---|---|---|---|---|---|---|---|---|---|
| MBR partitions or entire disks (HDD, SSD) | + | + | + | + | + | + | + | + | + |
| GPT/dynamic volumes or disks | + | + | + | + | + | + | + | + | + |
| Files and folders | + | + | + | + | + | + | + | + | + |

*Internal or external.

Though backing up to your local hard drive is the simplest option, we recommend that you store your backups off-site because it enhances the security of your data.

1. **External drive**

   If you plan to use an external USB hard drive with your desktop PC, we recommend that you connect the drive to a rear connector by using a short cable.
2. **Home file server, NAS, or NDAS**

   Check whether Acronis True Image for SANDISK detects the selected backup storage, both in Windows and when booted from the bootable 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 (five 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.
3. **Network share**

   See also: Authentication settings.

## Preparing a new disk for backup

A new internal or external hard drive may not be recognized by Acronis True Image for SANDISK. If this is the case, use the operating system tools to change the disk status to **Online** and then to initialize the disk.

***To change a disk status to Online***

1. Open **Disk Management**. To do this, go to **Control Panel** -> **System and Security** -> **Administrative Tool**, start **Computer Management**, and then click **Disk Management**.
2. Find the disk marked as **Offline**. Right-click the disk and then click **Online**.
3. The disk status will be changed to **Online**. After that, you will be able to initialize the disk.

***To initialize a disk***

1. Open **Disk Management**. To do this, go to **Control Panel** -> **System and Security** -> **Administrative Tool**, start **Computer Management**, and then click **Disk Management**.
2. Find the disk marked as **Not Initialized**. Right-click the disk and then click **Initialize Disk**.
3. Select a partition table for the disk - MBR or GPT, and then click **OK**.
4. [optional step] To create a volume on the disk, right-click the disk, click **New Simple Volume**, and then follow the wizard's steps to configure the new volume. To create one more volume, repeat this operation.

## Authentication settings

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

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

### Troubleshooting

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

- Windows account has a password on the computer where the shared folder is located.
- Password-protected sharing is turned off in Windows.
  For example, in Windows 10, you can find this setting at **Control Panel** > **Network and Internet** > **Network and Sharing Center** > **Advanced sharing settings** > Turn off password protected sharing.
  In Windows 11, you can access it at **Settings** > **Network & internet** > **Advanced sharing settings**.

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

# Acronis Nonstop Backup

Acronis Nonstop Backup provides easy protection of your disks and files. It allows you to recover entire disks, individual files and their different versions.

The main purpose of Acronis Nonstop Backup is continuous protection of your data (files, folders, contacts, etc.), though you can use it to protect partitions as well. If you choose to protect an entire partition, you will be able to recover the partition as a whole using the image recovery procedure.

We do not recommend using Nonstop Backup as a primary way to protect your system. For the safety of your system, use any other schedule. See Examples of custom schemes for examples and details.

## Nonstop Backup limitations

- You can create only one nonstop backup.
- Windows libraries (Documents, Music, etc.) can be protected with a disk-level nonstop backup only.
- You cannot protect data stored on external hard drives.

## How it works

Once you start Acronis Nonstop Backup, the program will perform an initial full backup of the data selected for protection. Acronis Nonstop Backup will then continually monitor the protected files (including open ones). Once a modification is detected, the changed data is backed up. The shortest interval between the incremental backup operations is five minutes. This allows you to recover your system to an exact point in time.

Acronis Nonstop Backup checks file changes on the disk, not in the memory. If, for instance, you are working in Word and do not save for a long time, your current changes in the Word document will not be backed up.

You may think that at these backup rates the storage will fill in no time. Do not worry as Acronis True Image for SANDISK will back up only so called "deltas". This means that only differences between old and new versions will be backed up and not whole changed files. For example, if you use Microsoft Outlook or Windows Mail, your pst file may be very large. Furthermore, it changes with each received or sent E-mail message. Backing up the entire pst file after each change would be an unacceptable waste of your storage space, so Acronis True Image for SANDISK backs up only its changed parts in addition to the initially backed up file.

## Retention rules

**Local backups**

Acronis Nonstop Backup keeps all backups for the last 24 hours. The older backups will be consolidated in such a way that Nonstop Backup will keep daily backups for the last 30 days and weekly backups until all Nonstop Backup data destination space is used.

The consolidation will be performed every day between midnight and 01:00 AM. The first consolidation will take place after the Nonstop Backup has been working for at least 24 hours. For example, you have turned on the Nonstop Backup at 10:00 AM on July 12. In this case the first consolidation will be performed between 00:00 and 01:00 AM on July 14. Then the program will consolidate the data every day at the same time. If your computer is turned off between 00:00 and 01:00 AM, the consolidation will start when you turn the computer on. If you turn off Nonstop Backup for some time, the consolidation will start after you turn it on again.

All other versions are automatically deleted. The retention rules are pre-set and cannot be changed.

## Acronis Nonstop Backup data storage

Acronis Nonstop Backup data storage can be created on local hard disk drives (both internal and external).

In many cases an external hard disk will be the best choice for Nonstop Backup data storage. You can use an external disk with any of the following interfaces: USB (including USB 3.0), eSATA, FireWire, and SCSI.

You can also use an NAS as the storage, but with one limitation - it must be accessible with the SMB protocol. It does not matter whether an NAS share you want to use for the storage is mapped as a local disk or not. If the share requires login, you will need to provide the correct user name and password. For more information see Authentication settings. Acronis True Image for SANDISK remembers the credentials and the subsequent connections to the share do not require login.

When an external hard disk or NAS is unavailable, the Nonstop Backup destination can be an internal disk, including a dynamic one. Keep in mind that you cannot use a partition to be protected as a Nonstop Backup storage.

Before creating Acronis Nonstop Backup data storage, Acronis True Image for SANDISK checks whether the selected destination has enough free space. Acronis True Image for SANDISK multiplies the volume of data to be protected by 1.2 and compares the calculated value with the available space. If the free space on the destination satisfies this minimum storage size criterion, the destination can be used for storing Nonstop Backup data.

## Nonstop Backup - Frequently asked questions

**Why does Acronis Nonstop Backup pause on its own?** - This is the designed behavior of Acronis Nonstop Backup. When the system load rises to a critical level, Acronis Nonstop Backup receives the overload alarm from Windows and pauses itself. This is done to aid Windows relieve the load caused by other applications. The overload can be caused by running resource-intensive applications (for example, performing a deep system scan with your antivirus software).

In such a case Nonstop Backup automatically pauses and you cannot restart it. After pausing, Acronis Nonstop Backup gives the system one hour to relieve the load and then attempts to restart.

The automatic restart count for Acronis Nonstop Backup is 6. This means that after the first automatic restart Acronis Nonstop Backup will attempt to restart five more times with intervals of exactly one hour between attempts.

After the sixth unsuccessful attempt, Acronis Nonstop Backup will wait for the next calendar day. On the next day the automatic restart count will automatically reset. When not interfered with, Acronis Nonstop Backup performs six restart attempts per day.

The restart attempt count can be reset by doing any of the following:

- Restarting Acronis Nonstop Backup service;
- Rebooting the computer.

Restarting Acronis Nonstop Backup service will only reset the restart count to 0. If the system is still overloaded, Acronis Nonstop Backup will pause again. For information on restarting the Acronis Nonstop Backup service, see Acronis True Image for SANDISK Nonstop Backup Pauses.

Rebooting the computer will reset the load and the restart count. If the system overloads again, Acronis Nonstop Backup will pause.

**Why does Acronis Nonstop Backup sometimes cause a high CPU load?** - This is the expected behavior of Acronis Nonstop Backup. This may happen on restart of a paused Acronis Nonstop Backup if a considerable amount of protected data has been modified during the pause.

For example, if you manually pause the Acronis Nonstop Backup that you use for protecting your system partition and then install a new application. When you restart Acronis Nonstop Backup, it loads the CPU for some time. However, the process (afcdpsrv.exe) then goes back to normal.

This happens because Acronis Nonstop Backup needs to check the backed up data against the data that have been modified during the pause to ensure protection continuity. If there was a considerable amount of data modified, the process may load CPU for some time. After the check is done and all the modified data is backed up, Acronis Nonstop Backup goes back to normal.

**Can I have Acronis Nonstop Backup storage on an FAT32 partition of a local hard disk?** - Yes, FAT32 and NTFS partitions can be used as the storage.

**Can I set up Acronis Nonstop Backup storage on a network share or NAS?** - Yes, Acronis Nonstop Backup supports network shares, mapped drives, NAS and other network attached devices with one limitation - they must use the SMB protocol.

# Backup file naming

## Naming convention for backup files created by Acronis True Image for SANDISK

A TIB backup file name has the following attributes:

- Backup name
- Backup method (full, inc, diff: full, incremental, differential)
- Number of backup chain[1] (in the form of b#)
- Number of backup version[2] (in the form of s#)
- Number of volume (in the form of v#)

  For example this attribute changes when you split a backup into several files. See Backup splitting for details.

Thus a backup name may look the following way:

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

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

# Integration with Windows

During installation Acronis True Image for SANDISK provides closer integration with Windows. Such merging allows you to get the most out of your computer.

Acronis True Image for SANDISK integrates the following components:

- Acronis items on the Windows **Start** menu
- Acronis True Image for SANDISK button on the taskbar
- Shortcut menu commands

***Windows Start menu***

The **Start** menu displays Acronis commands, tools and utilities. They give you access to Acronis True Image for SANDISK functionality, without having to start the application.

***Acronis True Image for SANDISK button on the taskbar***

The Acronis True Image for SANDISK button on the Windows taskbar shows the progress and result of Acronis True Image for SANDISK operations.

***Tray Notification Center***

---

[1]Sequence of minimum two backup versions that consist of the first full backup version and the subsequent one or more incremental or differential backup versions. Backup version chain continues till the next full backup version (if any).

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

When Acronis True Image for SANDISK is open, you can see the status of any operation in it. However, since some operations can take quite a while, such as a backup, there is no need to keep Acronis True Image for SANDISK to learn its result.

The Tray Notification Center contains latest notifications in one place, lets you see important operation statuses without opening Acronis True Image for SANDISK at the moment when you need them. The following notifications are shown in Acronis Tray Notification Center: information on the results of backup operations, and other important notifications from Acronis True Image for SANDISK. The Tray Notification Center is minimized and hidden under Acronis True Image for SANDISK in the tray.

***Shortcut menu commands***

To access shortcut menu commands, open File Explorer, right-click selected items, point to Acronis True Image for SANDISK, and then select a command.

- To create a new file-level backup, select **New file backup**.
- To create a new disk-level backup, select **New disk backup**.
- To mount a disk-level backup (.tibx file), select **Mount**.
- To validate a backup (.tibx file), select **Validate**.

***File-level recovery in File Explorer***

1. In File Explorer, double-click the backup file (.tibx file) that contains the data to recover.
2. Copy or drag the files and folders to any location on your computer, as if they were stored on an ordinary disk.

# Compatibility with Microsoft BitLocker encryption feature

## Overview

BitLocker is a built-in disk encryption feature in Microsoft Windows that protects data by encrypting entire volumes. Acronis True Image for SANDISK supports BitLocker-encrypted drives under certain conditions and provides partial compatibility.

## Backing up BitLocker-encrypted drives

Acronis True Image for SANDISK allows backing up BitLocker-encrypted drives with the following considerations:

- In sector-by-sector mode, the encryption is preserved.
- In normal mode, the data is backed up in a decrypted state.
- Ensure that the drive is unlocked before starting a backup operation.

### Restoring BitLocker-encrypted drives

When restoring data from a BitLocker-encrypted backup:

- The restored partition will not be encrypted.
- BitLocker encryption must be manually re-enabled after the restoration is complete.

### Cloning BitLocker-encrypted drives

Cloning BitLocker-encrypted drives requires additional steps:

- BitLocker must be disabled, and the drive decrypted before cloning.
- Attempting to clone an encrypted drive without decryption may result in a failed operation.

### System recovery with BitLocker

If BitLocker is enabled on the system partition, consider the following:

- Ensure that the recovery media supports BitLocker-encrypted partitions.
- BitLocker encryption must be manually re-applied after the recovery process.

### Recommendations

To ensure seamless operation when working with BitLocker-encrypted drives:

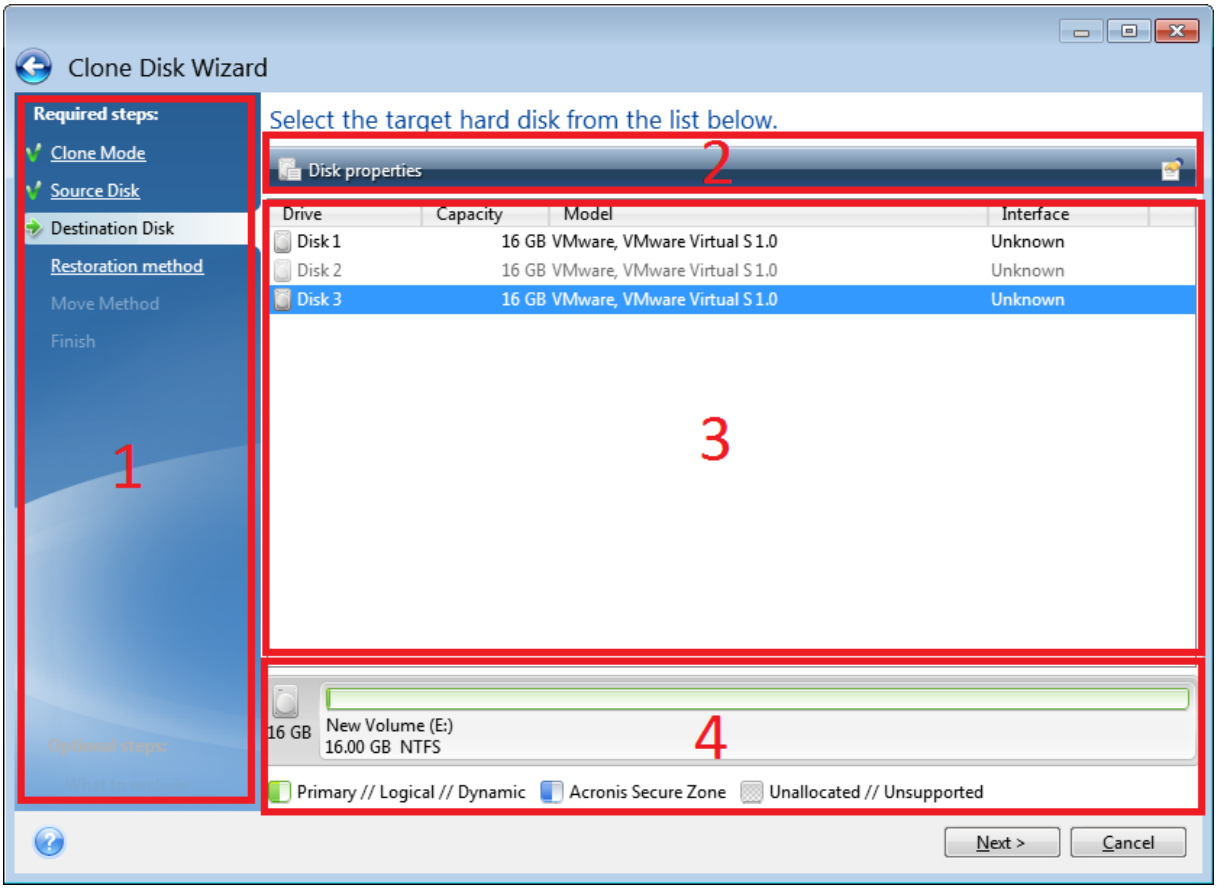
- Unlock and decrypt drives before performing backups or cloning.
- After restoring, allocate time to reapply encryption settings.
- For Windows 11 users, verify encryption settings since BitLocker is enabled by default.

For more details, see BitLocker Compatibility with Acronis True Image for SANDISK.

## Wizards

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

For example, see the screenshot 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.

# FAQ about backup, recovery and cloning

- **I have a 150 GB system partition, but the occupied space on that partition is only 80 GB. What will Acronis True Image for SANDISK include in a backup?** – By default, Acronis True

Image for SANDISK copies only the hard disk sectors that contain data, so it will include only 80 GB in a backup. You can also choose the sector-by-sector mode. Note that such a backup mode is required only in special cases. For more information, see Image creation mode. While creating a sector-by-sector backup, the program copies both used and unused hard disk sectors and the backup file will usually be significantly larger.

- **Will my system disk backup include drivers, documents, pictures, etc.?** – Yes, such a backup will contain the drivers, as well as the contents of the My documents folder and its subfolders, if you kept the default location of the My documents folder. If you have just a single hard disk in your PC, such a backup will contain all of the operating system, applications and data.
- **I have an old hard disk drive which is almost full in my notebook. I purchased a new bigger HDD. How can I transfer Windows, programs and data to the new disk?** – You can either clone the old hard disk on the new one or back up the old hard disk and then recover the backup to a new one. The optimum method usually depends on your old hard disk partitions layout.
- **I want to migrate my old system hard disk to an SSD. Can this be done with Acronis True Image for SANDISK?** – Yes, Acronis True Image for SANDISK provides such a function. For procedure details, see Migrating your system from an HDD to an SSD.
- **What is the best way to migrate the system to a new disk: cloning or backup and recovery?** – The backup and recovery method provides more flexibility. In any case, we strongly recommend to make a backup of your old hard disk even if you decide to use cloning. It could be your data saver if something goes wrong with your original hard disk during cloning. For example, there were cases when users chose the wrong disk as the target and thus wiped their system disk. In addition, you can make more than one backup to create redundancy and increase security.
- **What should I back up: a partition or the whole disk?** – In most cases, it is better to back up the whole disk. However, there may be some cases when a partition backup is advisable. For example, your notebook has a single hard disk with two partitions: system (disk letter C) and the data (disk letter D). The system partition stores your working documents in the **My documents** folder with subfolders. The data partition stores your videos, pictures, and music files. If you only want to back up the system partition, you don't have to back up the whole disk. In this case, a partition backup will be enough. Besides, if you only want to have your data backed up (not the system files), you can create a file backup. However, we recommend creating at least one whole disk backup if your backup storage has enough space.
- **Does Acronis True Image for SANDISK support RAID?** – Acronis True Image for SANDISK supports hardware RAID arrays of all popular types. Support of software RAID configurations on dynamic disks is also provided. Acronis bootable media supports most of the popular hardware RAID controllers. If the standard Acronis bootable media does not "see" the RAID as a single volume, the media does not have the appropriate drivers. In this case you can create WinPE-based media and add the required drivers there (in the advanced mode).

# Backing up data

## Backing up disks and partitions

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

**Note**
Virtual disks (e.g., VHD and VHDX) are not supported as sources for disk-level backups or entire PC backups. However, these formats can be selected for file-level backups or used as backup destinations.

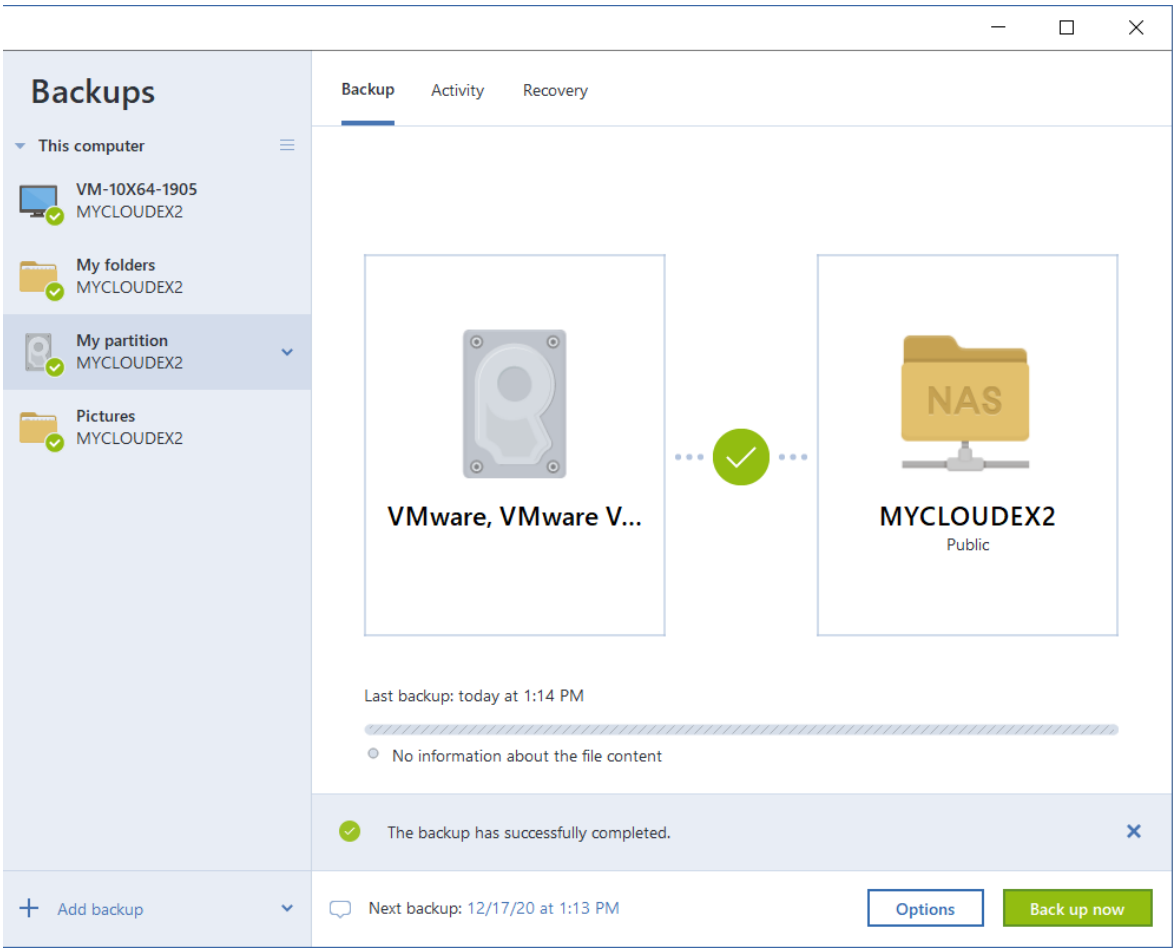
***To back up partitions or disks***

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

   **Note**
   Virtual disks stored on the same volume as the backup source may cause snapshot creation issues and result in backup errors. Avoid this setup for a seamless backup process.

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

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




7. Click the **Backup destination** area, and then select a destination for backup:
   - **Acronis Cloud** – Sign in to your account, and then click **OK**.
   - **Your external drive** – When an external drive is plugged into your computer, you can select it from the list.
   - **NAS** – Select an NAS from the list of found NAS devices. If you have only one NAS, Acronis True Image for SANDISK will suggest using it as a backup destination by default.
   - **Browse** – Select a destination from the folder tree.

**Note**
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.

**Note**
When backing up virtual disks, verify the backup destination to ensure compatibility and performance. Cloud backups and dynamic disk configurations may exhibit limitations in detection and performance.

8. [Optional] Click **Options** to set the options for the backup. For more information, see Backup options.

9. [Optional] Click the **Add a comment** icon, and then type a comment to the backup version. Backup comments will help you to find the necessary version later when recovering your data.
10. Perform one of the following:
    - To run the backup immediately, click **Back up now**.
    - To run the backup later or on a schedule, click the arrow to the right of the **Back up now** button, and then click **Later**.

Example: Testing virtual disk backups

1. Create a virtual hard disk (VHD or VHDX) using Windows Disk Management.
2. Format the virtual disk with a supported filesystem (e.g., NTFS).
3. Select the virtual disk as a file-level backup source or destination and proceed with the backup.
4. Avoid storing the virtual disk on the same physical drive as the backup source.

**Note**
Known issue: Entire PC backups intentionally skip virtual disks based on their interface type. To back up virtual disks, use file-level backups or create separate tasks for these disks.

## Backing up disks and partitions using bootable media

You can also perform disk- and partition-level backups by booting your computer from Acronis bootable media. This is useful if Windows cannot start or when you want to create a backup prior to loading the operating system.

To learn how to create such bootable media, see Creating Acronis bootable media.

To back up disks or partitions from bootable media:

1. Boot from the created media and click **Backup** or **Back up now**.
2. Select **Disks and partitions** as the backup source.
3. Choose a destination drive or network share. **Cloud storage** is available only when using WinPE- or WinRE-based media.
4. Start the backup.

For more details, see the Knowledge Base article: How to back up with Acronis bootable media.

**Note**
Backups are run one by one. The newest backups are added to queue until the previous ones are completed.

**Note**
When you back up your data to Acronis Cloud, the first backup may take a considerable amount of time to complete. Further backups will likely be much faster, because only changes to files will be transferred over the Internet.

**Note**
Once an online backup is started, you are free to close Acronis True Image for SANDISK. The backup process will continue in background mode. If you suspend the backup, turn off your computer, or disconnect it from the Internet, the backup will resume when you click **Back up now** or when the Internet connection is restored. A backup interruption does not cause your data to be uploaded twice.

# Backing up files and folders

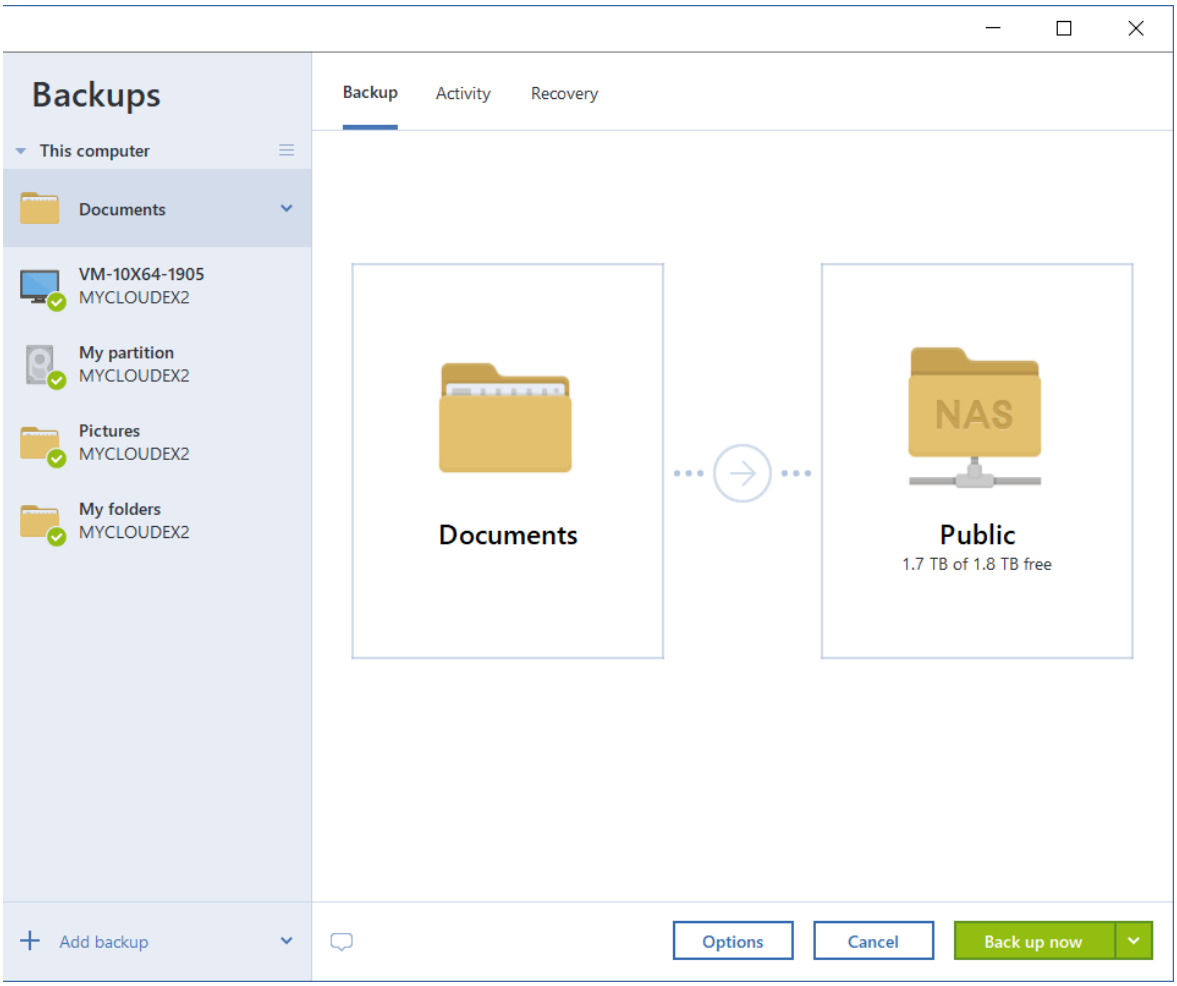
To protect files such as documents, photos, music files, video files, there is no need to back up the entire partition containing the files. You can back up specific files and folders.

***To back up files and folders***

1. Start Acronis True Image for SANDISK.
2. On the sidebar, click **Backup**.
3. Click **Add backup**.
4. [Optional] To rename the backup, click the arrow next to the backup name, click **Rename**, and then enter a new name.
5. Click the **Backup source** area, and then select **Files and folders**.

   **Important**
   To back up data that is synced to the cloud by a third-party cloud service provider, the actual data must be stored locally. If the files or folders are stored in the cloud, you will see only their local placeholders. Placeholders often have a cloud icon and are also considerably smaller in size. When you select source files for backup, you must select the local files, and not the placeholders. If the cloud service does not store your data locally, it cannot be backed up and recovered.

6. In the opened window, select the check boxes next to the files and folders that you want to back up, and then click **OK**.




7. Click the **Backup destination** area, and then select a destination for backup:
   - **Your external drive** – When an external drive is plugged into your computer, you can select it from the list.
   - **NAS** – Select an NAS from the list of found NAS devices. If you have only one NAS, Acronis True Image for SANDISK will suggest using it as a backup destination by default.
   - **Browse** – Select a destination from the folder tree.
8. [Optional] Click **Options** to set the options for the backup. For more information, see Backup options.
9. [Optional] Click the **Add a comment** icon, and then type a comment to the backup version. Backup comments will help you to find the necessary version later, when recovering your data.
10. Perform one of the following:
    - To run the backup immediately, click **Back up now**.
    - To run the backup later or on a schedule, click the down arrow to the right of the **Back up now** button, and then click **Later**.

**Note**
Backups are run one by one. The newest backups are added to queue until the previous ones are completed.

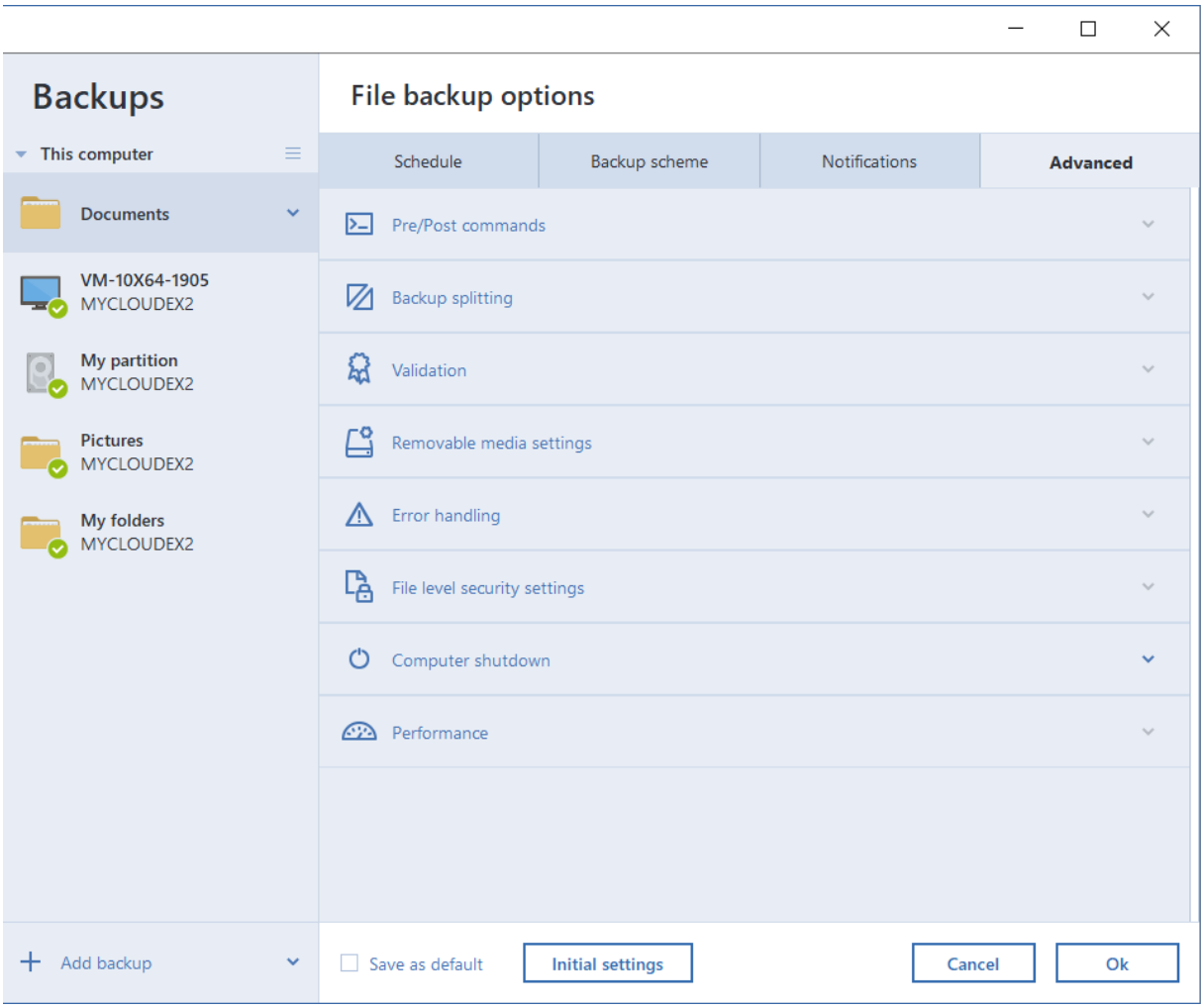
Additionally, watch the English-language video instructions at https://goo.gl/i4J1AN.

# 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 as default** check box to apply the modified settings to all further backup operations by default.



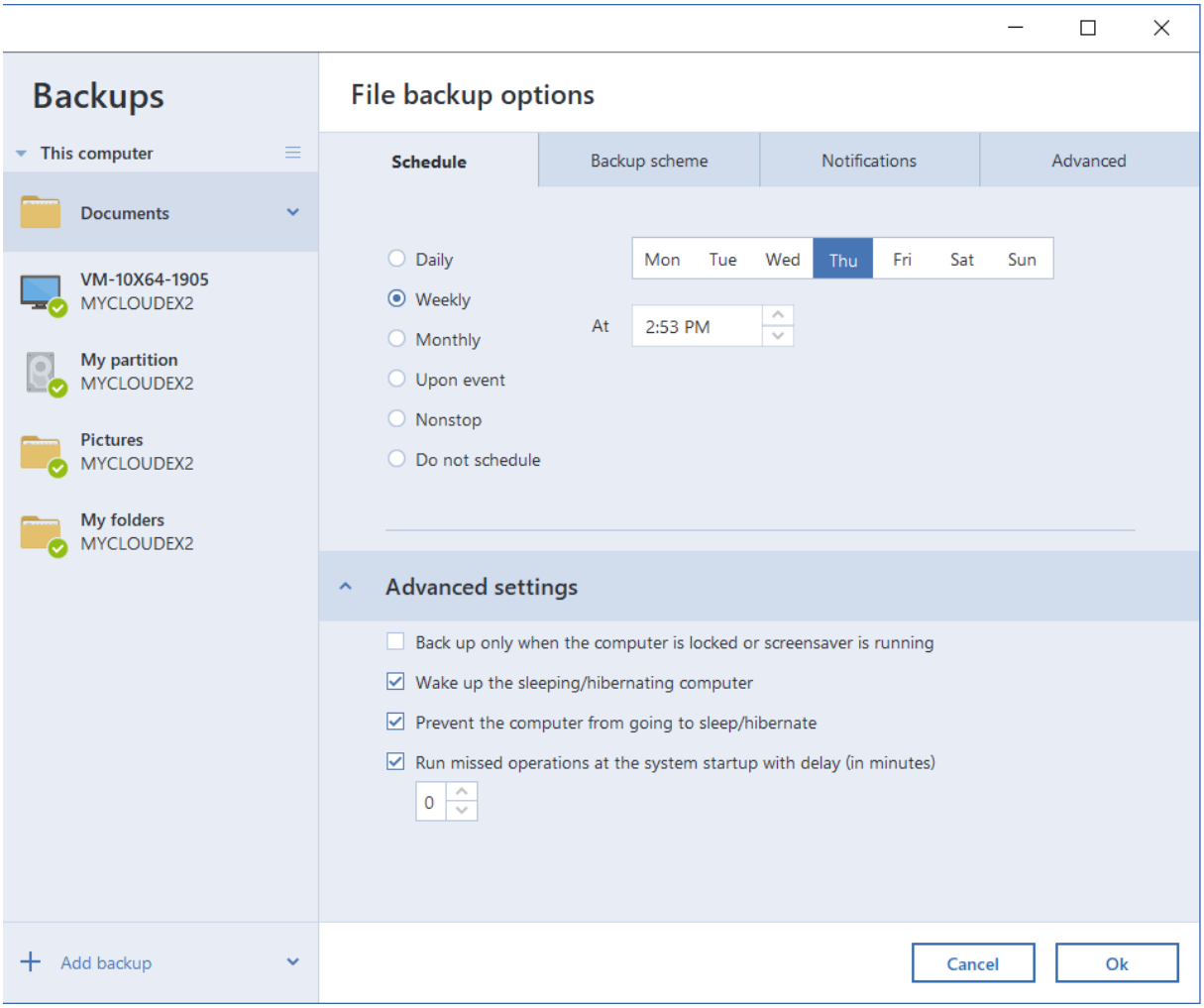

If you want to reset all the modified options to the values that were set after the product installation initially, click the **Reset to initial settings** button. Note that this will reset the settings for the current backup only. To reset the settings for all further backups, click **Reset to initial settings**, select the **Save the settings as default** check box, and then click **OK**.

Additionally, watch the English-language video instructions at https://goo.gl/bKZyaG.

# Scheduling

Location: **Options** > **Schedule**

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




You can specify a schedule for backups created or validated regularly:

- **Daily** – The operation will be executed once a day or more frequently.
- **Weekly** – The operation will be executed once a week or several times a week on the selected days.
- **Monthly** – The operation will be executed once a month or several times a month on the selected dates.
- **Upon event** – The operation will be executed upon an event.
- **Nonstop** – The operation will run every five minutes.
- **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:

- **Back up only when the computer is locked or screensaver is running** – Select this check box to postpone a scheduled operation until the next time the computer is not in use (a screen saver is displayed or computer is locked). For the validation schedule, the check box changes to **Run the validation only when the computer is idle**.
- **Wake up the sleeping/hibernating computer** – Select this check box to wake up the sleeping/hibernating computer to perform the scheduled operation.
- **Prevent the computer from going to sleep/hibernate** – Select this check box to eliminate a situation when a time-consuming backup is interrupted if the computer goes into sleep or hibernation mode.
- **Run missed operations at the system startup with delay (in minutes)** – Select this check box to force the missed operation to run at the next system startup, if the computer was switched off at the scheduled time, and the operation was not performed.

  Additionally, you can set a time delay to start backup after the system startup. For example, to start backup 20 minutes after system startup, enter *20* in the appropriate box.
- **Run missed operations when an external device is connected** [optional, if you schedule a backup to a USB flash drive, or validation of a backup that is located on a USB flash drive] – Select this check box to run a missed operation when the USB flash drive is attached if it was disconnected at the scheduled time.

## Daily backup parameters

You can set up the following parameters for backups created or validated daily:

- **Every** – Select the daily periodicity from the dropdown list (for example, every 2 hours).
- **Once a day** – The operation starts once a day at the specified time.
- **Twice a day** – The operation starts twice a day. Select the time for each operation.

Description of the **Advanced settings** see in Scheduling.

## Weekly backup parameters

You can set up the following parameters for backups created or validated weekly:

- **Days of the week** – Select the days on which to run the operation.
- **At** – Select the operation start time.

Description of the **Advanced settings** see in Scheduling.

## Monthly backup parameters

You can set up the following parameters for backups created or validated monthly:

- **Every** – Select a numeral and a day of the week from the dropdown lists. For example, select **Every first Monday** to run the operation on the first Monday of every month.
- **On selected days of the month** – Select the date(s) for backup. For example, you may want to run the operation on the 10th and the last day of the month.
- **At** – Select the operation start time.

Description of the **Advanced settings** see in Scheduling.

### Upon event execution parameters

You can set up the following parameters for backups created or validated upon some event:

- **Once a day only** – Select the check box if you want to run the operation only at the first occurrence of the event on the current day.
- Specify the event triggering the backup creation or validation:
  - **When an external device is connected** – The operation starts each time the same external device (USB flash drive or an external HDD) you previously used as a backup destination is plugged into your computer. Note that Windows should recognize this device as external.
  - **User logon** – The operation starts each time the current user logs on to the OS.
  - **User logoff** – The operation starts each time the current user logs off the OS.
  - **System shutdown or restart** – The operation starts at every computer shutdown or reboot.
  - **System startup with delay (in minutes)** – The operation starts at every OS startup with the delay time you specified.

Description of the **Advanced settings** see in Scheduling.

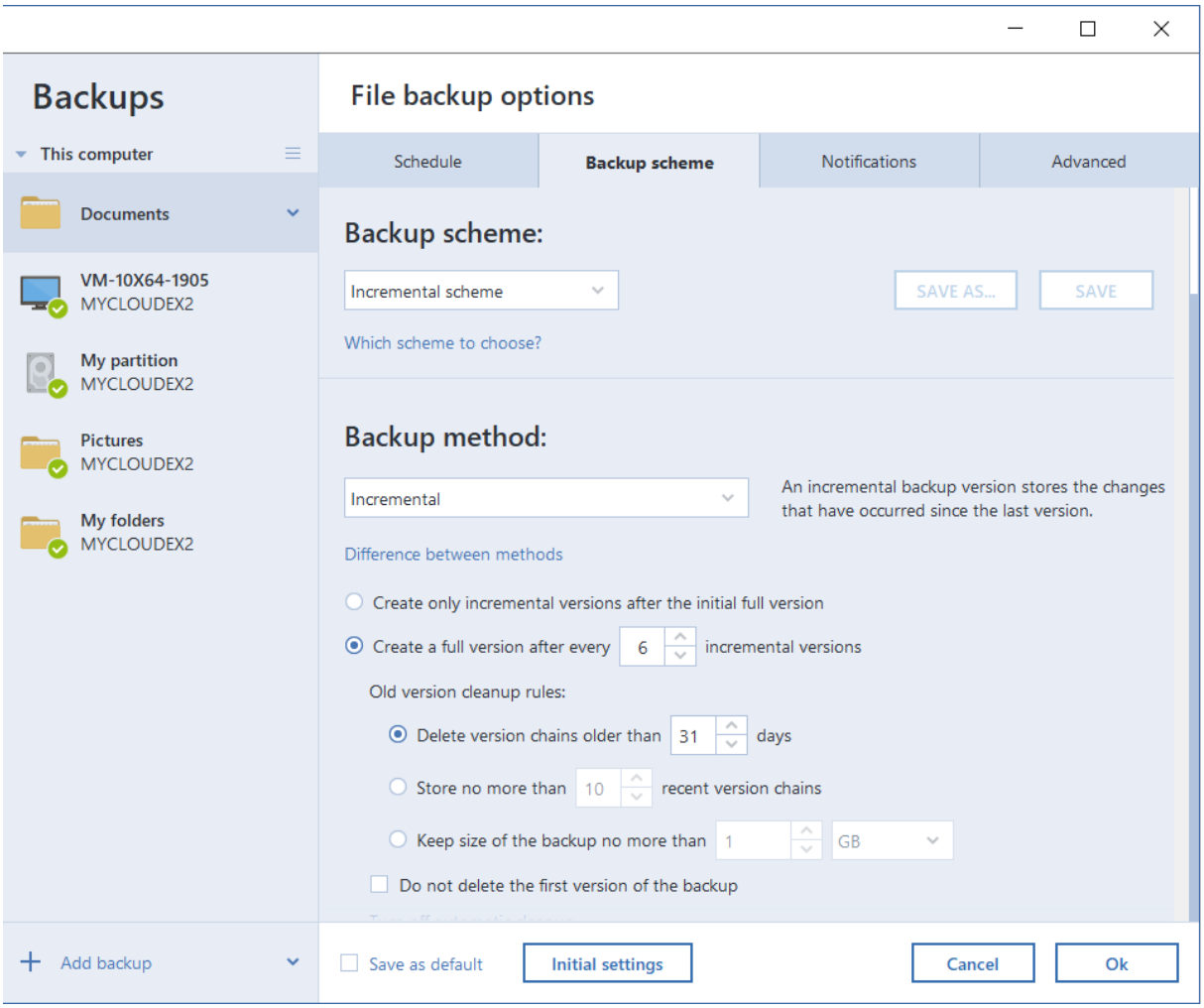
## Backup schemes

Location: **Options** > **Backup scheme**

Backup schemes along with the scheduler help you 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.

The backup scheme defines the following parameters:

- Backup methods that will be used to create backup versions (full, differential or incremental)
- Sequence of the backup versions created using different methods
- Version cleanup rules




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

- **Single version scheme** – Select this scheme if you want to use the smallest backup storage.
- **Version chain scheme** – This may be the optimal scheme in many cases.
- **Incremental scheme** – Select to create a full version after every five incremental versions. This is the default scheme.
- **Differential scheme** – Select to create only differential backups after an initial full backup.
- **Custom scheme** – Select to set up a backup scheme manually.

You can easily change the backup scheme for a pre-existing backup. This will not affect the integrity of the backup chains, so you will be able to recover your data from any previous backup version.

**Note**

You cannot change the backup scheme when backing up to optical media such as a DVD/BD. In this case, Acronis True Image for SANDISK by default uses a custom scheme with only full backups. This is because the program cannot consolidate backups stored on optical media.

## Single version scheme

This backup scheme is the same for both disk backup and file backup types (except scheduler settings).

The program creates a full backup version and overwrites it every time according to the specified schedule or when you run the backup manually. In this process, the old version is deleted only after a new version is created.

**Note**
The very first file will remain for auxiliary purposes, without your data in it. Do not delete it!

Backup scheduler setting for disk backup: monthly.

Backup scheduler setting for file backup: daily.

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

Required storage space: minimal.

## Version chain scheme

This backup scheme differs for disk backup and file backup types.

**Disk backup version chain**

At first the program creates the 1st full backup version. The version will be kept until you delete it manually. After that, according to the specified schedule (or when you run backup manually) the program creates: 1 full and 5 differential backup versions, then again 1 full and 5 differential backup versions and so on. The versions will be stored for 6 months. After the period the program analyzes if the oldest backup versions (except the 1st full version) may be deleted. It depends on the minimum number of versions (eight) and version chains consistency. The program deletes the oldest versions one by one after creating new versions with the same backup method (for example, the oldest differential version will be deleted after creation of the newest differential version). First of all the oldest differential versions will be deleted, then - the oldest full version.

Backup scheduler setting: monthly.

Result: you have monthly backup versions for the last 6 months plus the initial full backup version that may be kept for a longer period.

Required storage space: depends on the number of versions and their sizes.

**File backup version chain**

According to the specified schedule (or when you run backup manually) the program creates: 1 full and 6 incremental backup versions, then again 1 full and 6 incremental versions and so on. The versions will be stored for 1 month. After the period the program analyzes if the oldest backup versions may be deleted. It depends on the version chain consistency. To keep the consistency, the

program deletes the oldest versions by chains "1 full + 6 incremental backup versions" after creating a new analogous version chain.

Backup scheduler setting: daily.

Result: you have backup versions for every day of the last month.

Required storage space: depends on the number of versions and their sizes.

## Custom schemes

With Acronis True Image for SANDISK 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.

**Note**
You cannot overwrite existing pre-defined backup schemes.

In addition, you can create custom schemes from scratch based on full, differential or incremental backup versions.

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

- Full

  Select this method if you want to create only full backup versions.
- Incremental

  Select this method if you want to create backup chains containing only full and incremental backup versions.

  You can configure the scheme by using one of the following options:
  - **Create only incremental versions after the initial full version** – Select this option to create only one backup version chain. Automatic cleanup is not available for this option.
  - **Create a full version after every [n] incremental versions** – Select this option to create several backup version chains. This is a more reliable but more space-consuming backup scheme.
- Differential

  Select this method if you want to create backup chains containing only full and differential backup versions.

  You can configure the scheme by using one of the following options:
  - **Create only differential versions after the initial full version** – Select this option to create only one backup version chain. Automatic cleanup is not available for this option.
  - **Create a full version after every [n] differential versions** – Select this option to create several backup version chains. This is a more reliable but more space-consuming backup scheme.

**Turn on automatic cleanup**

- **Old version cleanup rules** – To delete obsolete backup versions automatically, you can set one of the following cleanup rules:
  - **Delete versions older than [n] days** [available for full method only – Select this option to limit the age of backup versions. All versions that are older than the specified period will be automatically deleted.
  - **Delete version chains older than [n] days** [available for incremental and differential methods only – Select this option to limit the age of backup version chains. The oldest version chain will be deleted only when the most recent backup version of this chain is older than the specified period.
  - **Store no more than [n] recent versions** [available for full method only – Select this option to limit the maximum number of backup versions. When the number of versions exceeds the specified value, the oldest backup version will be automatically deleted.
  - **Store no more than [n] recent version chains** [available for incremental and differential methods only – Select this option to limit the maximum number of backup version chains. When the number of version chains exceeds the specified value, the oldest backup version chain will be automatically deleted.
  - **Keep size of the backup no more than [defined size]** [not available for local backups – Select this option to limit the maximum size of the backup. After creating a new backup version, the program checks whether the total backup size exceeds the specified value. If it's true, the oldest backup version will be deleted.
- **Do not delete the first version of the backup** – Select this check box to keep the initial data state. The program will create two initial full backup versions. The first version will be excluded from the automatic cleanup, and will be stored until you delete it manually.

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

  Note that when the check box is selected for the full method, the **Store no more than [n] recent versions** check box changes 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 confirm in the **Delete scheme** window.

**Note**
The pre-defined backup schemes cannot be deleted.

## Examples of custom schemes

### 1. Entire PC backup "Two full versions"

Case: You want to protect all data on your computer with two full versions and you want to update the backup once a month. Let's see how you can do it by using a custom backup scheme.

1. Start configuring an entire PC backup.
2. Make sure Entire PC is selected as the backup source.
3. Click **Options**, open the **Schedule** tab, click **Monthly**, and then specify a day of the month (for example, the 20-th). This will result in a backup version being created on a monthly basis, on the day you specify. Then, specify a start time for the backup operation.
4. Open the **Backup scheme** tab, and then choose **Custom scheme** instead of **Incremental scheme**.
5. In the **Backup method** box, select **Full** from the drop-down list.
6. To limit the number of versions, click **Store no more than [n] recent versions**, and type or select **2**, and click **OK**.

   In this case, the program will create a new full version every month, on the 20-th day. After creating the third version, the oldest version will be automatically deleted.
7. Check that all settings are correct and click **Back up now**. If you want your first backup to be run only at the time you specified in the Scheduler, click the down arrow to the right of the **Back up now** button and select **Later** in the drop-down list.

### 2. File backup "Daily incremental version + weekly full version"

Case: You have files and/or folders you work with every day. You need to save your daily work results and want to be able to recover data state to any date for the last three weeks. Let's see how you can do this using a custom backup scheme.

1. Start configuring a file backup. See Backing up files and folders for details.
2. Click **Options**, open the **Schedule** tab, click **Daily**, and then specify a start time for the backup operation. For example, if you finish your everyday work at 8 PM, specify this time or a little later (8.05 PM) as the start time.
3. Open the **Backup scheme** tab, and then choose **Custom scheme** instead of **Incremental scheme**.
4. In the **Backup method** box, select **Incremental** from the drop-down list.
5. Click **Create a full version after every [n] incremental versions**, and type or select **6**.

   In that case, the program will first create the initial full backup version (no matter how you set up a backup process, the first backup version will always be the full one), and then six incremental

versions day by day. Then, it will create one full version and six incremental versions again and so on. So every new full version will be created in exactly a week's time.

6. To limit the storage time for the versions, click **Turn on automatic cleanup**.
7. Click **Delete version chains older than [n] days**, type or select **21**, and click **OK**.
8. Check that all settings are correct and click **Back up now**. If you want your first backup to run only at the time you specified in the Scheduler, click the down arrow to the right of the **Back up now** button and select **Later** in the drop-down list.

### 3. Disk backup "Full version every 2 months + differential version twice a month"

Case: You need to back up your system partition twice a month and create a new full backup version every two months. In addition, you want to use no more than 100 GB of disk space to store the backup versions. Let's see how you can do it using a custom backup scheme.

1. Start configuring a disk backup. See Backing up disks and partitions.
2. Select your system partition (usually C:) as the backup source.
3. Click **Options**, open the **Schedule** tab, click **Monthly**, and then specify, for example, the 1st and 15th days of the month. This will result in a backup version in about every two weeks. Then, specify a start time for the backup operation.
4. Open the **Backup scheme** tab, and then choose **Custom scheme** instead of **Incremental scheme**.
5. In the **Backup method** box, select **Differential** from the drop-down list.
6. Click **Create a full version after every [n] differential versions**, and type or select **3**.

   In that case the program will first create the initial full backup version (no matter how you set up a backup process, the first backup version will always be the full one), and then three differential versions, each one in about two weeks. Then again a full version and three differential versions and so on. So every new full version will be created in two months.
7. To limit storage space for the versions, click **Turn on automatic cleanup**.
8. Click **Keep size of the backup no more than [defined size]**, type or select **100 GB**, and click **OK**.

   **Note**
   When the total backup size exceeds 100 GB, Acronis True Image for SANDISK will clean up the existing backup versions to make the remaining versions satisfy the size limit. The program will delete the oldest backup chain consisting of a full backup version and three differential backup versions.
9. Check that all settings are correct and click **Back up now**. If you want your first backup to be run only at the time you specified in the Scheduler, click the down arrow to the right of the **Back up now** button and select **Later** in the drop-down list.

## Notifications for backup operation

Location: **Options** > **Notifications**

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

By default, all notifications are disabled.

## Free disk space threshold

You may want to be notified when the free space on the backup storage becomes less than the specified threshold value. If after starting a backup Acronis True Image for SANDISK 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.

Acronis True Image for SANDISK can monitor free space on the following storage devices: local hard drives, USB cards and drives, and Network shares (SMB). This option cannot be enabled for FTP servers and CD/DVD drives.

***To set the free disk space threshold***

1. Select the **Show notification message on insufficient free disk space** check box.
2. Enter a threshold value in the **Notify me when free disk space is less than** box.

**Note**
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.

## Email notification

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

***If the test message sending fails***

1. Click **Show extended settings**.
2. Configure additional email settings:
   - Enter the sender's email address in the **From** field. If you are not sure what address to specify, then type any address you like in a standard format, for example *aaa@bbb.com*.
   - Change the message subject in the **Subject** field, if necessary.

     To simplify monitoring a backup status, you can add the most important information to the subject of the email messages. You can type the following text labels:
     - %BACKUP_NAME – The backup name
     - %COMPUTER_NAME – The name of the computer where the backup was started
     - %OPERATION_STATUS – The result of the backup or other operation

       For example, you can type: *Status of backup %BACKUP_NAME%: %OPERATION_STATUS% (%COMPUTER_NAME%)*
   - Select the **Log on to incoming mail server** check box, and enter the incoming mail server (POP3) under it.
   - Set the port of the incoming mail server. By default, the port is set to 110.
3. Click the **Send test message** button again.

***Additional notification settings***

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

**Note**
You will only get email notifications for a particular backup.

## Image creation mode

Location: **Options** > **Advanced** > **Image creation mode**

You can use these parameters to create an exact copy of your whole partitions or hard disks, and not only the sectors that contain data. For example, this can be useful when you want to back up a partition or disk containing an operating system that is not supported by Acronis True Image for SANDISK. Keep in mind 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.

## Backup protection

Location: Backup dashboard > **Options** > **Advanced** > **Backup protection**

By default, there is no password protection for backups, but you can configure passwords to protect your backup files.

**Note**
You cannot change the backup protection option for an existing backup.

***To protect a backup***

1. Enter the password for the backup into the corresponding 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.

   **Note**
   A password cannot be retrieved. Memorize the password that you specify for a backup protection.

2. To confirm the previously entered password, retype it into the corresponding 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

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

- Recover data from the backup
- Edit settings

- Mount
- Move

To access the backup, you must specify the correct password. For safety reasons, there is no way to recover lost passwords.

## Backup splitting

Location: **Options** > **Advanced** > **Backup splitting**

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

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

The default setting - **Automatic**. With this setting, Acronis True Image for SANDISK 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.

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.

## Backup validation option

Location: **Options** > **Advanced** > **Validation**

You can specify the following settings:

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

- **The latest backup version when it is completed**
- **Entire backup when it is completed**

The default settings are as follows:

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

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

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

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

  Example: You start a backup operation on July 15, at 12.00. The backup version is created at 12.05. Its validation will run at 12.15 if your computer is in the "screen saver" state at the moment. If not, then the validation will not run. In a month, August 15, at 12.15, the validation will start again. As before, your computer must be in the "screen saver" state. The same will occur on September 15, and so on.

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

## Removable media settings

Location: **Options** > **Advanced** > **Removable media settings**

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

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

The following settings are available:

- **Place Acronis True Image for SANDISK on media** – We strongly recommend selecting this option to support USB, PC Card (formerly PCMCIA), and SCSI interfaces along with the storage devices connected via them.
- **Place Acronis True Image for SANDISK (64-bit) on media** – The same option for 64-bit systems.
- **Place Acronis System Report on media** – Select this option to generate System Report that is used for collecting information about your system in case of any program problem. Report generation will be available before you start Acronis True Image for SANDISK from the bootable media. The generated System Report can be saved to a USB flash drive.
- **Place Acronis System Report (64-bit) on media** – The same option for 64-bit systems.
- **Ask for first media while creating backups on removable media** – Select this option to display the **Insert First Media** prompt when backing up to removable media. With the default

setting (option selected), backing up to removable media may not be possible if the user is away, because the program will wait for someone to click **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.

### 32-bit or 64-bit components

Pay attention to which versions of Acronis True Image for SANDISK and Acronis System Report are compatible with your computer.

| | 32-bit components | 64-bit components |
|---|---|---|
| BIOS-based 32-bit computers | + | - |
| BIOS-based 64-bit computers | + | + |
| EFI-based 32-bit computers | + | - |
| EFI-based 64-bit computers | - | + |

## Error handling

When Acronis True Image for SANDISK encounters an error while performing a backup, it stops the backup process and displays a message, waiting for a response on how to handle the error. You can configure an error handling policy, so Acronis True Image for SANDISK will not stop the backup process, but will handle the error according to the rules that you set, and will continue working.

**Note**
This topic applies to backups that use local or network backup destinations.

***To set up the error handling policy***

1. On the Backup dashboard > **Options** > **Advanced** > **Error handling**
2. Set the error handling policy:
   - **Do not show messages and dialogs while processing (silent mode)** - Enable this setting to ignore errors during backup operations. This is useful when you cannot control the backup process.
   - **Ignore bad sectors** - This option is available only for disk and partition backups. It lets you successfully complete a backup even if there are bad sectors on the hard disk.
     We recommend that you select this check box when your hard drive is failing, for example:
     - Hard drive is making clicking or grinding noises during operation.
     - The S.M.A.R.T. system has detected hard drive issues and recommends that you back up the drive as soon as possible.

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

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

  **Note**
  Scheduled backup operations will not start until all attempts are completed.

3. Click **OK**.

## Computer shutdown

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

You can configure the following options:

- **Stop all current operations when I shut down the computer** – When you turn off your computer while Acronis True Image for SANDISK is performing a long operation (for example, a disk backup) this operation prevents the computer from shutdown. When this check box is selected, Acronis True Image for SANDISK automatically stops all its current operations before shutdown. This may take about two minutes. The next time you run Acronis True Image for SANDISK, it will restart the stopped backups.
- **Shut down the computer after the backup is complete** – Select this option if the backup process you are configuring may take a long time. 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.

## Performance of backup operation

Location for backups to local destinations: **Options** > **Advanced** > **Performance**

### Compression level

You can choose the compression level for a backup:

- **Normal** – The recommended data compression level (set by default).
- **High** – Higher backup file compression level, takes more time to create a backup.
- **Max** – Maximum backup compression, but takes a long time to create a backup.

**Note**
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.

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

## Operation priority

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

You can set up the operation priority:

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

## Snapshot for backup

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

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

Select an option from the **Snapshot for backup** list:

- **No snapshot** – A snapshot will not be created. The files will be backed up one by one as an ordinary copy operation.
- **VSS** – This option is default for disk-level and the Entire PC backups, and guarantees data consistency in the backup.

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

- **Acronis snapshot** – A snapshot will be created with the Acronis driver used in previous versions of Acronis True Image for SANDISK.
- **VSS without writers** – This option is default for file-level backups. VSS writers are special VSS components for notifying applications that a snapshot is going to be created, so that the applications prepare their data for the snapshot. The writers are needed for applications that perform large number of file operations and require data consistency, for example databases. Because such applications are not installed on home computers, there is no need to use writers. In addition, this reduces the time required for file-level backups.

## Laptop power settings

Location: **Settings** > **Battery saver**

**Note**
This setting is only available on computers with batteries (laptops, computers with UPS).

Long-term backups may consume the battery power quite fast. When you work on your laptop and there is no power supply around you or when your computer has switched to UPS after a blackout, it's reasonable to save the battery charge.

***To save the battery charge***

- On the sidebar, click **Settings** > **Battery saver**, select the **Do not back up when battery power is less than** check box, and then use the slider to set the exact battery level for the charge saving to start.

When this setting is turned on, if you unplug your laptop power adapter or use a UPS for your computer after a blackout, and the remaining battery charge is equal or below the level in the slider, all current backups are paused and scheduled backups will not start. Once you plug the power adapter back in or the power supply is restored, the paused backups will be resumed. The scheduled backups that have been missed because of this setting will be started as well.

This setting does not block backup functionality completely. You can always start a backup manually.

# Operations with backups

## Backup operations

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

The backup operations menu can contain the following items:

- **Rename** (not available for backups to Acronis Cloud) – Set a new name for a backup in the list. The backup files will not be renamed.
- **Validate the latest version** – Start quick validation of the last backup slice.
- **Validate all versions** – Start validation of all backup slices.
- **Clean up versions** – Delete backup versions you no longer need.
- **Clone settings** – Create 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** – Move all of the backup files to another location. The subsequent backup versions will be saved to the new location.

  If you change the backup destination by editing the backup settings, only new backup versions will be saved to the new location. The earlier backup versions will remain in the old location.
- **Delete** – Depending on a backup type, you can completely delete the backup from its location or choose whether you want to delete the backup box only. When you delete a backup box, the backup files remain in the location and you will be able to add the backup to the list later. Note that when you delete a backup completely, the deletion cannot be undone.
- **Open location** – Open the folder containing the backup files.
- **Search files** – Find a specific file or folder in a backup by entering its name into the search field.
- **Convert to VHD** (for disk-level backups – Convert a selected Acronis backup version (.tibx file) to virtual hard disks (.vhd(x) files). The initial backup version will not be modified.

You can also reconfigure the backup settings to adjust parameters such as the source, destination, and schedule, ensuring they meet your current requirements.

Depending on the backup type, the **Reconfigure** option behaves differently:

- **Reconfigure** (for backups manually added to the backup list) – Configure the settings of a backup created by a previous 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) – 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.

***To reconfigure backups:***

1. Navigate to the **Backup** tab on the main interface.
2. Select the desired backup from the list.
3. Click the **Reconfigure** button in the bottom-right corner of the screen.

Once reconfigured, the backup will become available for editing and operations such as running **Back up now**.

## Backup activity and statistics

On the **Activity** tab and the **Backup** tab, you can view additional information on a backup, such as backup history and file types the backup contains. The **Activity** tab contains a list of operations performed on the selected backup starting from its creation, the operation statuses, and statistics. This comes in handy when you need to find out what was happening to the backup in background mode, for example the number and statuses of scheduled backup operations, size of backed-up data, results of backup validation, etc.

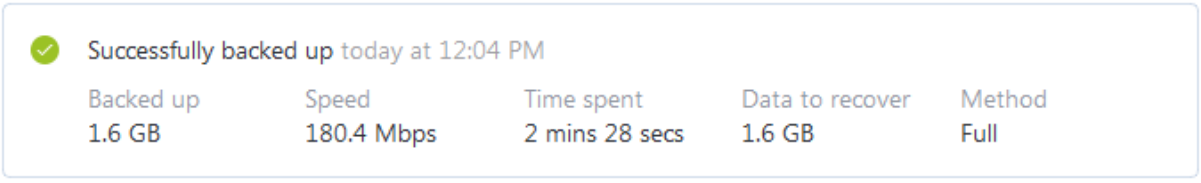
When you create the first version of a backup, the **Backup** tab displays a graphical representation of the backup content by file types.

### The Activity tab

**Note**
Nonstop backups do not have an activity feed.

***To view backup activity***

1. On the sidebar, click **Backup**.
2. In the backup list, select the backup, the history of which you want to view.
3. On the right pane, click **Activity**.




#### What you can view and analyze

- Backup operations and their statuses (successful, failed, canceled, interrupted, and so on)
- Operations performed on the backup, and their statuses
- Error messages
- Backup comments
- Backup operation details, including:
  - **Backed up** – size of the data that the last backup version contains.
  - **Speed** – backup operation speed.
  - **Time spent** – time spent for the backup operation.

- **Data to recover** – size of the data that can be recovered from the last backup version.
- **Method** – backup operation method (full, incremental, or differential).

### Backup size metrics (TIB archives)

- For file-level backups, Acronis True Image for SANDISK calculates the size of files to back up. The value of **Backed up** is equal to the value of **Data to recover** for full backup versions. For differential and incremental versions, **Backed up** is usually less than **Data to recover**, because the product additionally uses data from the previous versions for recovery.
- For disk-level backups, Acronis True Image for SANDISK calculates the size of the hard drive sectors that contain data to back up. Because sectors may contain hard links to files, even for full disk-level backup versions the value of **Backed up** can be less than the value of **Data to recover**.

### Backup size metrics (current format, TIBX archives)

- **Backed up** – shows the amount of data stored in the archive after applying Acronis compression, the inbuilt deduplication mechanism (Archive3), and backup exclusions.
- **Data to recover** – shows how much space the recovered data will take on the disk.

### Causes of possible discrepancies in sizes

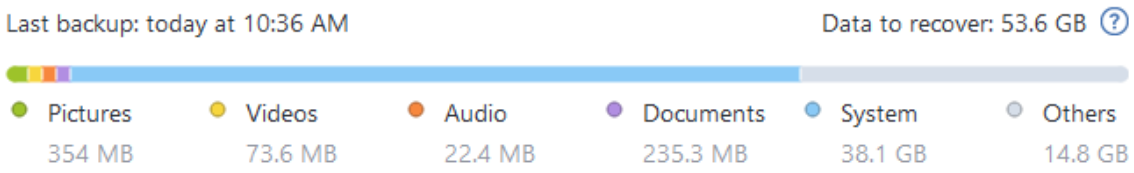
Acronis True Image for SANDISK uses different metrics to represent data at various stages. Because of this, the values of **Backed up** and **Data to recover** in the **Activity** tab can differ. Review the specifics above and validate the backup to ensure its consistency.

- If the **Data to recover** size is bigger than the actual size of the selected data that was backed up, the reason can be hard links and sparse files in the file system of the backup source.

For more information, see the Support Portal article.

## The Backup tab

When a backup is created, you can view statistics on types of the backed-up files that the last backup version contains:




Point to a color segment to see the number of files and the total size for each data category:

- Pictures
- Video files
- Audio files
- Documents

- System files
- Other file types, including hidden system files

**Data to recover** – shows the size of the original data that you selected to back up.

## Sorting backups in the list

By default, the backups are sorted by the date they were created, starting from the newest to oldest. To change the order, select the appropriate sorting type in the upper part of the backup list. You have the following options:

| Command | | Description |
|---|---|---|
| **Sort by** | **Name** | This command sorts all backups in alphabetical order.<br>To reverse the order, select **Z → A**. |
| | **Date created** | This command sorts all backups from newest to oldest.<br>To reverse the order, select **Oldest on top**. |
| | **Date updated** | This command sorts all backups by date of the last version. The newer the last backup version, the higher the backup will be placed in the list.<br>To reverse the order, select **Least recent on top**. |
| | **Size** | This command sorts all backups by size, from biggest to smallest.<br>To reverse the order, select **Smallest on top**. |
| | **Source type** | This command sorts all backups by the source type. |
| | **Destination type** | This command sorts all backups by the destination type. |

## Validating backups

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

For example, backup validation is important before you recover your system. If you start recovery from a corrupted backup, the process will fail and your computer may become unbootable. We recommend that you validate system partition backups under bootable media. Other backups may be validated in Windows. See also Preparing for recovery and Basic concepts.

***To validate an entire backup in Windows***

1. Start Acronis True Image for SANDISK, and then click **Backup** on the sidebar.
2. In the backup list, click the down arrow icon next to the backup to validate, and then click **Validate**.

***To validate a specific backup version or an entire backup in a standalone version of Acronis True Image for SANDISK (bootable media)***

1. On the **Recovery** tab, find the backup that contains the version that you want to validate. If the backup is not listed, click **Browse for backup**, and then specify the path to the backup. Acronis True Image for SANDISK 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**.

## Backup to various places

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

The subsequent incremental or differential backups will be written to the USB stick.

**Note**
You cannot continue backing up to an optical disc.

### Splitting backups on the fly

When free space on the destination storage (CD-R/RW or DVD-R/RW) is insufficient to complete the current backup operation, the program displays a warning message.

To complete the backup, perform one of the following

- Free up some space on the disk, and then click **Retry**.
- Click **Browse**, and then select another storage device.
- Click **Format** to erase all data on the disk, and then proceed with the backup.

When versions of a backup are stored in different locations, you may need to specify the locations during recovery.

## Adding an existing backup to the list

You may have Acronis True Image for SANDISK backups created by a previous product version or copied from another computer.

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, at the bottom of the backup list, click the arrow icon, and then click **Add existing backup**. The program opens a window where you can browse for backups on your computer.
2. Select a backup version (a .tibx file), and then click **Add**.
   The entire backup will be added to the list.

# Deleting backups

To delete backups and backup versions that you no longer need, use the tools provided by Acronis True Image for SANDISK.

Acronis True Image for SANDISK stores information on the backups in a metadata information database. Therefore, deleting unneeded backup files in File Explorer will not delete the information about these backups from the database. This will result in errors when the program tries to perform operations on the backups that no longer exist.

***To delete an entire backup locally in Acronis True Image for SANDISK***

In the **Backup** section, click the down arrow icon next to the backup to delete, and then click **Delete**.

Depending on the backup type, this command completely deletes the backup from its location, or allows you to choose between deleting the backup files completely or just removing the backup name from Acronis True Image for SANDISK. Note that if you delete a backup completely, the deletion cannot be undone. When you only remove the backup name from Acronis True Image for SANDISK, the backup files remain in their current location and you will be able to add the existing backup to Acronis True Image for SANDISK later.

If a backup location is not available any longer, then the backup files cannot be deleted there, but you can remove the name of this backup from Acronis True Image for SANDISK. If you want to delete backup files that you see locally, but not in Acronis True Image for SANDISK, try adding this existing backup to Acronis True Image for SANDISK. After that, you can completely delete this backup and its files by using Acronis True Image for SANDISK.

**See also**

"Cleaning up backups and backup versions" (p. 67)

# Cleaning up backups and backup versions

## Cleanup rules for backups

1. Go to the **Backup** section.
2. From the backup list, select the backup for which you want to clean up versions, and then click **Options**.
3. On the **Backup scheme** tab, select **Custom scheme**, select a backup method, and then click **Turn on automatic cleanup**.
4. Configure cleanup rules for the backup.

   See Custom schemes for details.

**Note**
After the cleanup, some auxiliary files may stay in the storage. Do not delete them!

## Cleaning up backups manually

When you want to delete backup versions that you no longer need, use the tools provided in the application. If you delete backup version files outside Acronis True Image for SANDISK, for example in File Explorer, this will result in errors during operations with the backups.

Versions of the following backups cannot be deleted manually:

- Backups stored on CD, DVD, BD.
- Nonstop backups.

***To clean up backup versions locally in Acronis True Image for SANDISK***

1. In the **Backup** section, click the down arrow icon next to the backup to clean up, and then click **Clean up versions**.
   The **Clean up backup versions** window opens.
2. Select the required versions and click **Delete**.
3. Click **Delete** in the confirmation request.

Please wait for the cleanup operation to complete. After the cleanup, some auxiliary files may stay in the storage. Do not delete them.

**Cleaning up versions that have dependent versions**

Depending on the backup type and scheme, a backup version may be part of a backup version chain[1]. For this reason, deleting this backup version affects the entire chain. The affected dependent versions are also selected for deletion, because data recovery from such versions becomes impossible.

- When you select a full version[2] - the program also selects all dependent incremental and differential versions till the next full one. In other words, the entire backup chain will be deleted. However, if the chain is made up of only full versions, any of them can be deleted independently.
- When you select a differential version[3] - it can be deleted independently.
- When you select an incremental version[4] - the program also selects all dependent incremental versions within the backup version chain[5].

**See also**

---

[1]Sequence of minimum two backup versions that consist of the first full backup version and the subsequent one or more incremental or differential backup versions. Backup version chain continues till the next full backup version (if any).
[2]A self-sufficient backup version 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.
[3]A differential backup version stores changes to the data against the latest full backup version. You need access to the corresponding full backup version to recover the data from a differential backup version.
[4]A backup version that stores changes to the data against the latest backup version. You need access to other backup versions from the same backup to restore data from an incremental backup version.
[5]Sequence of minimum two backup versions that consist of the first full backup version and the subsequent one or more incremental or differential backup versions. Backup version chain continues till the next full backup version (if any).

### Full, incremental and differential backups

"Deleting backups" (p. 67)

# Recovering data

## Recovering disks and partitions

### 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. 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 and then proceed with recovering your system.

### 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. See Recovering your system for details.

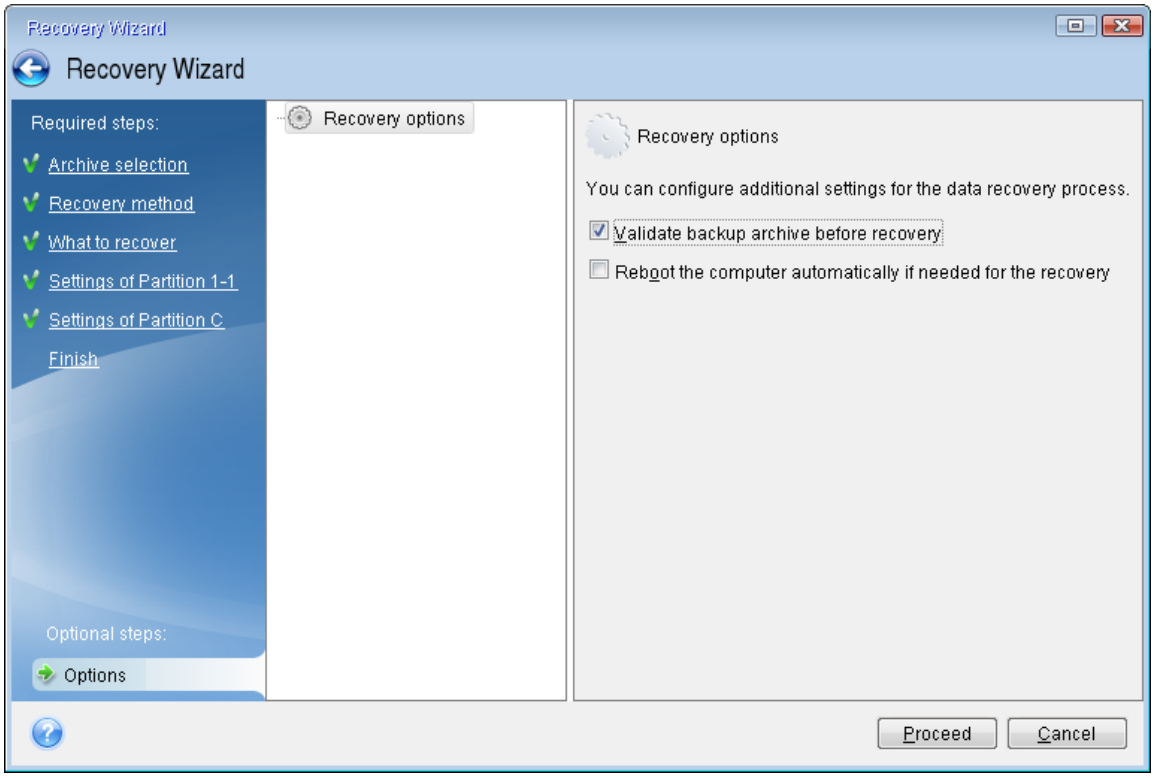
### Preparing for recovery

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 bootable media, it creates disk drive letters that might differ from the way Windows identifies drives. For example, the D: disk identified in the bootable media might correspond to the E: disk in Windows.

## Recovering your system to the same disk

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

***To recover your system***

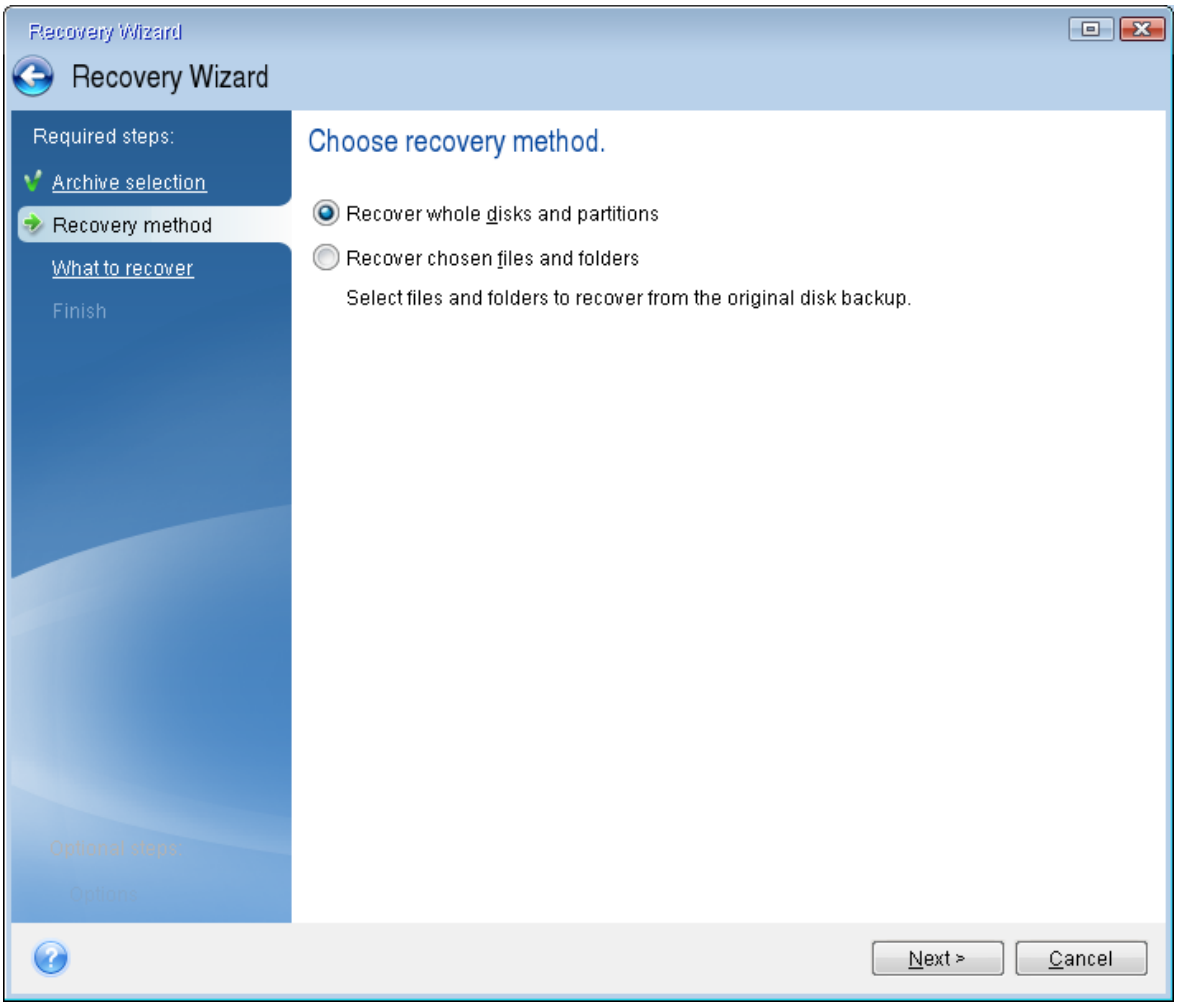
1. Attach the external drive if it contains the backup to be used for recovery and make sure that the drive is powered on.
2. Arrange the boot order in BIOS so as to make your Acronis bootable media (CD, DVD or USB drive) the first boot device. See Arranging boot order in BIOS or UEFI BIOS.

   If you use a UEFI computer, pay attention to the boot mode of the bootable media in UEFI BIOS. It is recommended that the boot mode matches the type of the system in the backup. If the backup contains a BIOS system, then boot the bootable media in BIOS mode; if the system is UEFI, then ensure that UEFI mode is set.

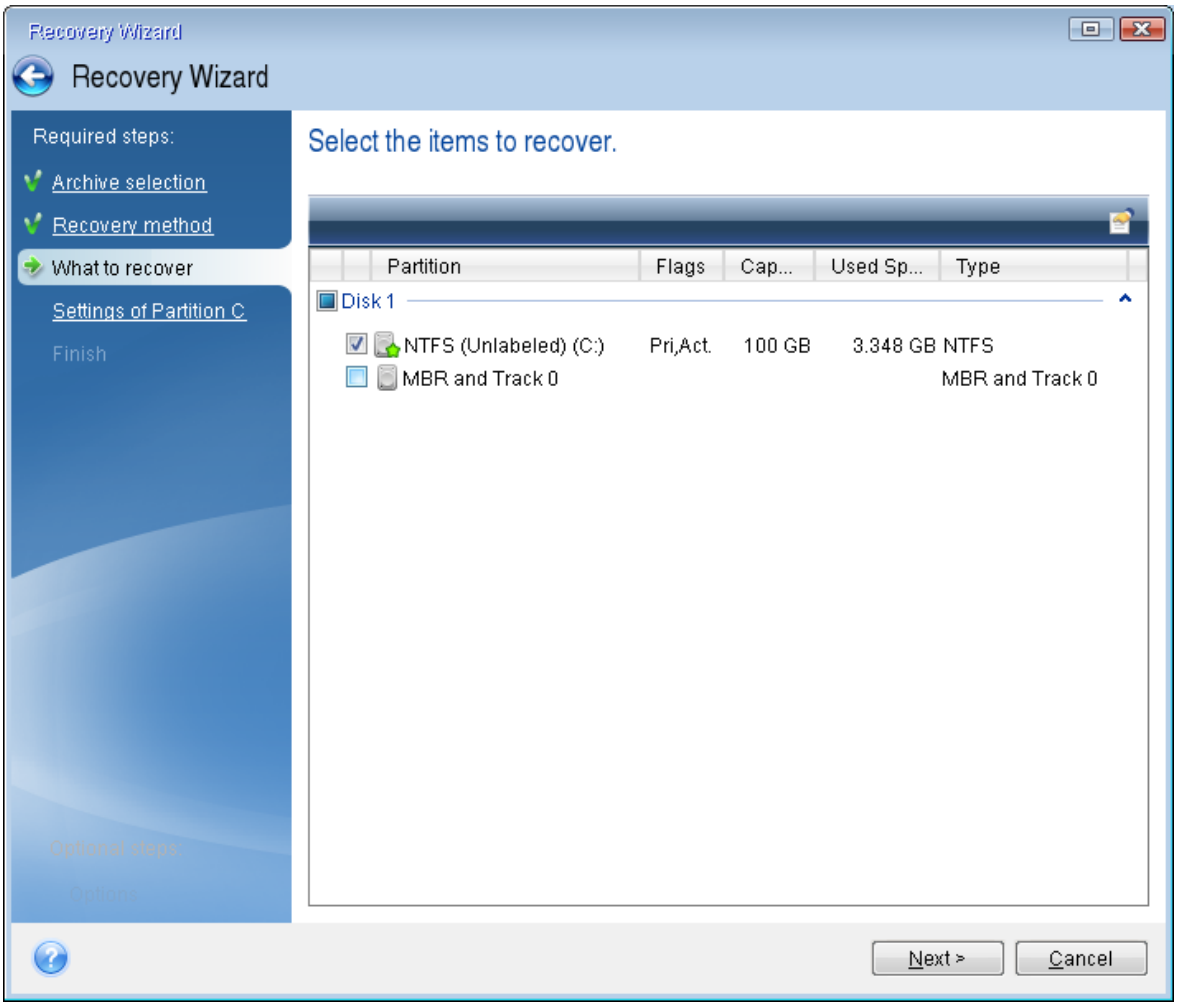
3. Boot from Acronis bootable media and select **Acronis True Image for SANDISK**.
4. On the **Home** screen, select **My disks** below **Recover**.
5. Select the system disk or partition backup to be used for recovery.
   When the backup is not displayed, click **Browse** and specify path to the backup manually.

   **Note**
   If the backup is located on a USB drive, and the drive is not recognized correctly, check the USB port version. If it is a USB 3.0 or USB 3.1, try connecting the drive to a USB 2.0 port.

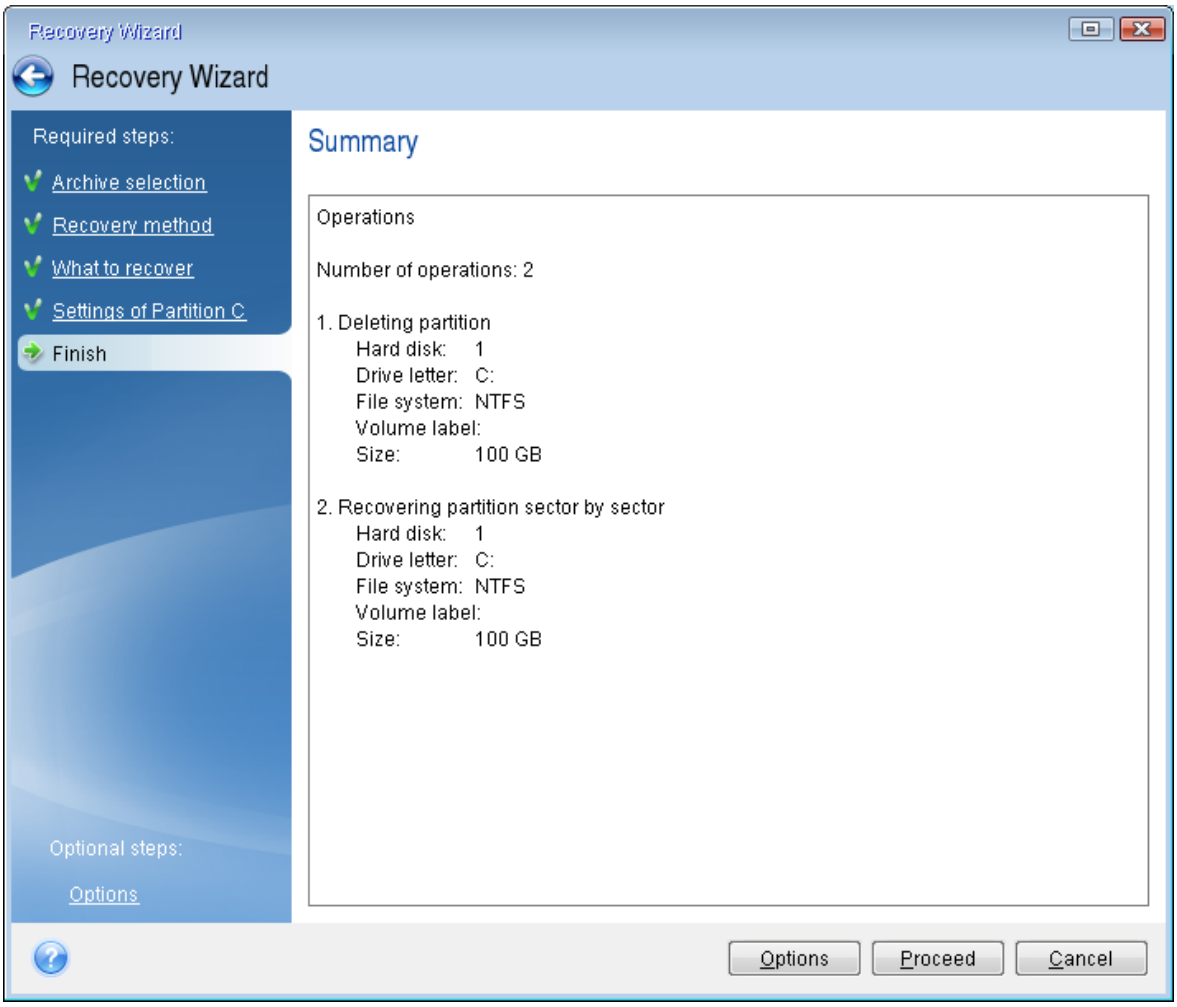
6. Select **Recover whole disks and partitions** at the **Recovery method** step.




7. [Optional] At the **Recovery point** step, select the date and time to recover your system to.
8. 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. If you have the System Reserved partition, select it, too.




9. 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.
10. 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**.




11. When the operation finishes, exit the standalone version of Acronis True Image for SANDISK, remove Acronis bootable 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. You do not need to format the new disk, as this will be done in the process of recovery.

**Note**
It is recommended that your old and new hard drives work in the same controller mode. Otherwise, your computer might not start from the new hard drive.

***To recover your system to a new disk***

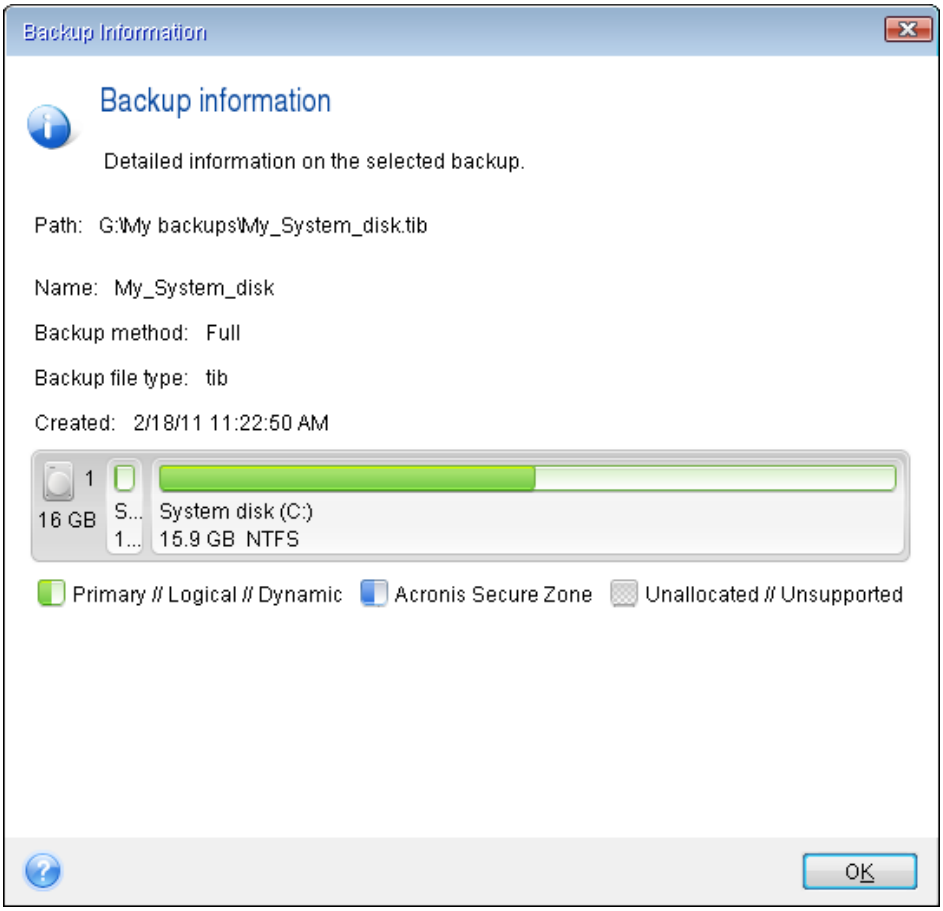
1. Install the new hard drive to the same position in the computer and use the same cable and connector that was used for the original drive. If this is not possible, install the new drive to where it will be used.
2. Attach the external drive if it contains the backup to be used for recovery and make sure that the drive is powered on.

3. Arrange the boot order in BIOS so as to make your bootable media (CD, DVD or USB stick) the first boot device. See Arranging boot order in BIOS or UEFI BIOS.

   If you use an UEFI computer, pay attention to the boot mode of the bootable media in UEFI BIOS. It is recommended that the boot mode matches the type of the system in the backup. If the backup contains a BIOS system, then boot the bootable media in BIOS mode; if the system is UEFI, then ensure that UEFI mode is set.
4. Boot from the bootable media and select **Acronis True Image for SANDISK**.
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.

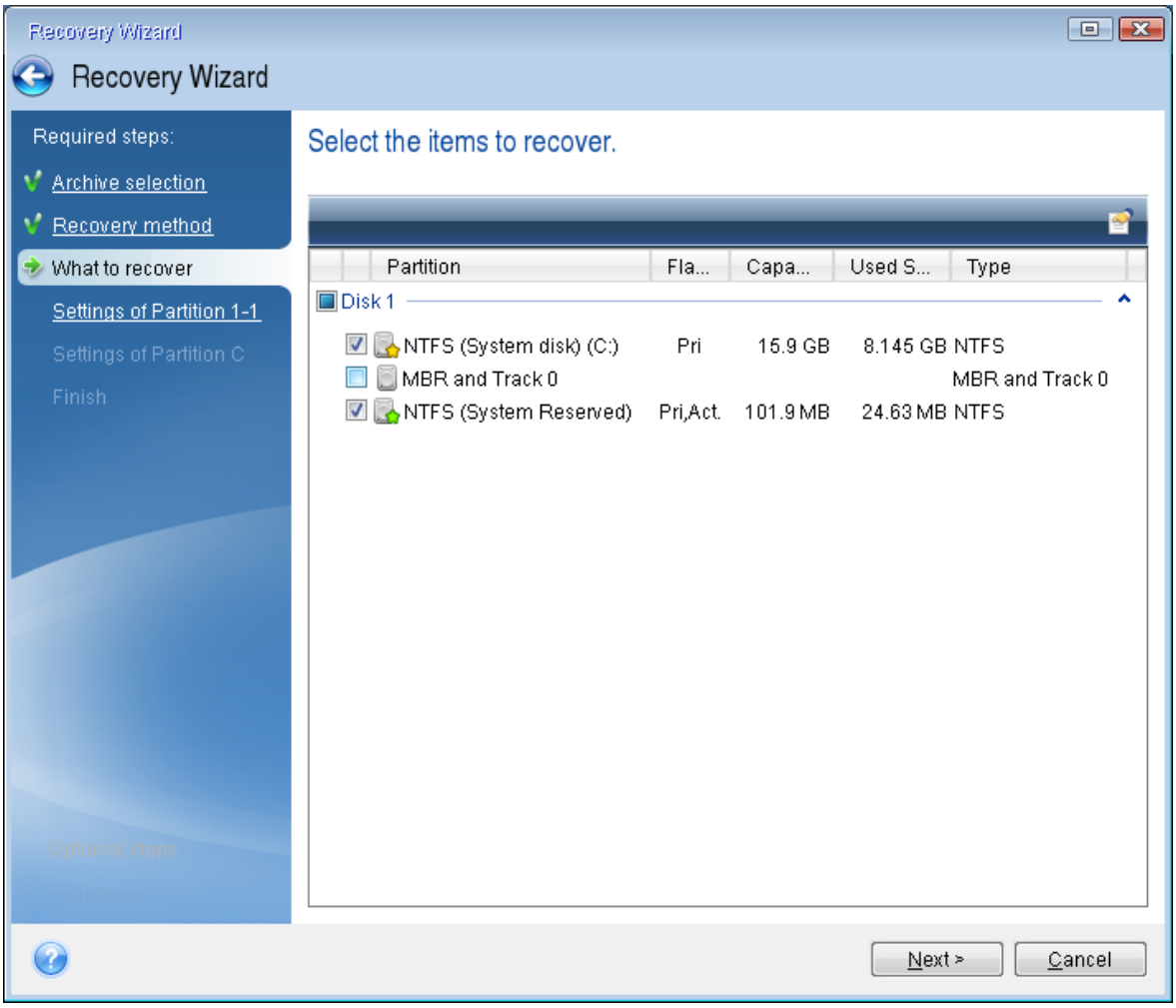
   **Note**
   If the backup is located on a USB drive, and the drive is not recognized correctly, check the USB port version. If it is a USB 3.0 or USB 3.1, try connecting the drive to a USB 2.0 port.

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. Remember the location and size of the hidden partition, because these parameters need to be the same on your new disk.



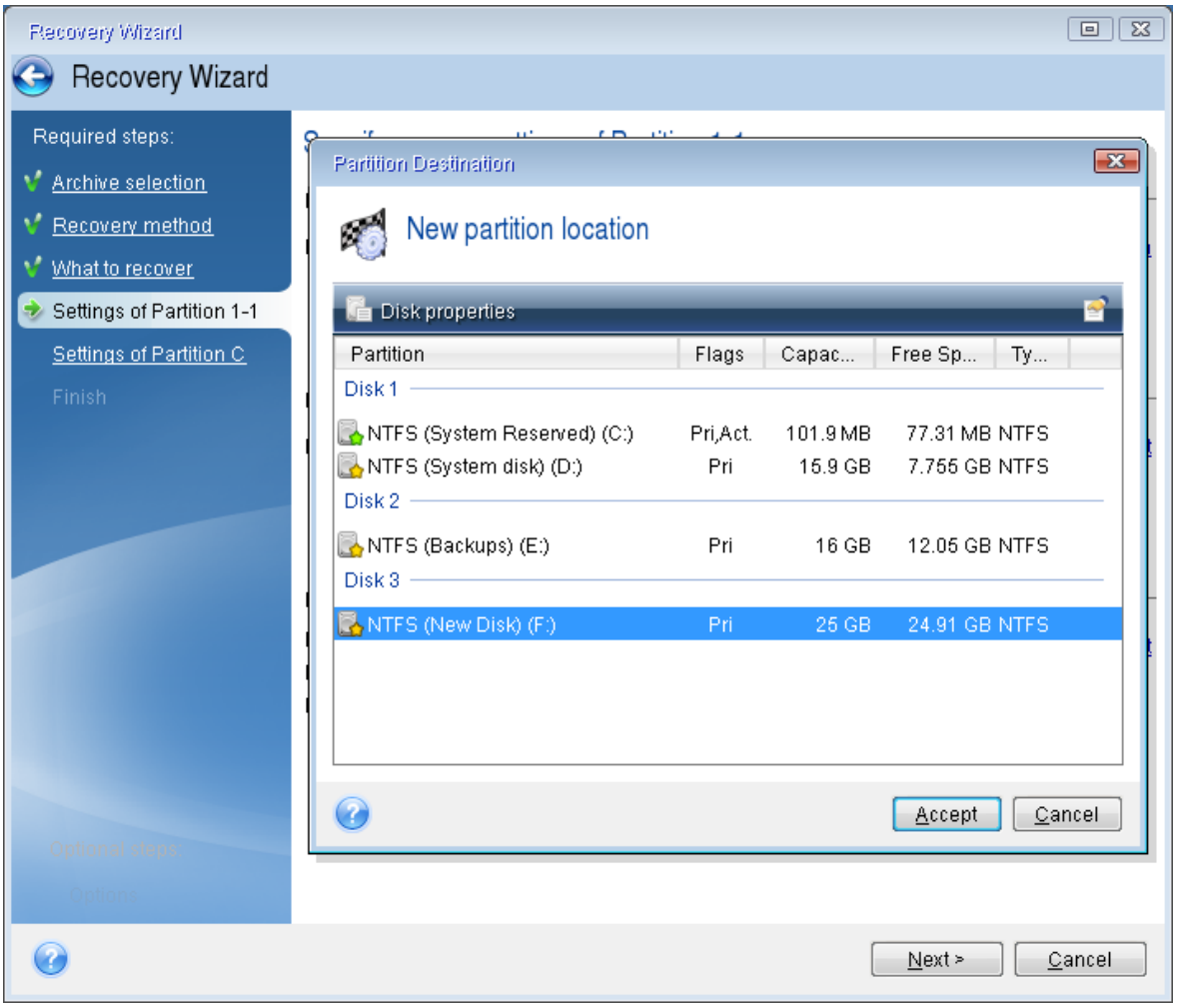

8. Select **Recover whole disks and partitions** at the **Recovery method** step.
9. On the **What to recover** step, select the boxes of the partitions to be recovered.

   If you select an entire disk, MBR and Track 0 of the disk will also be recovered.

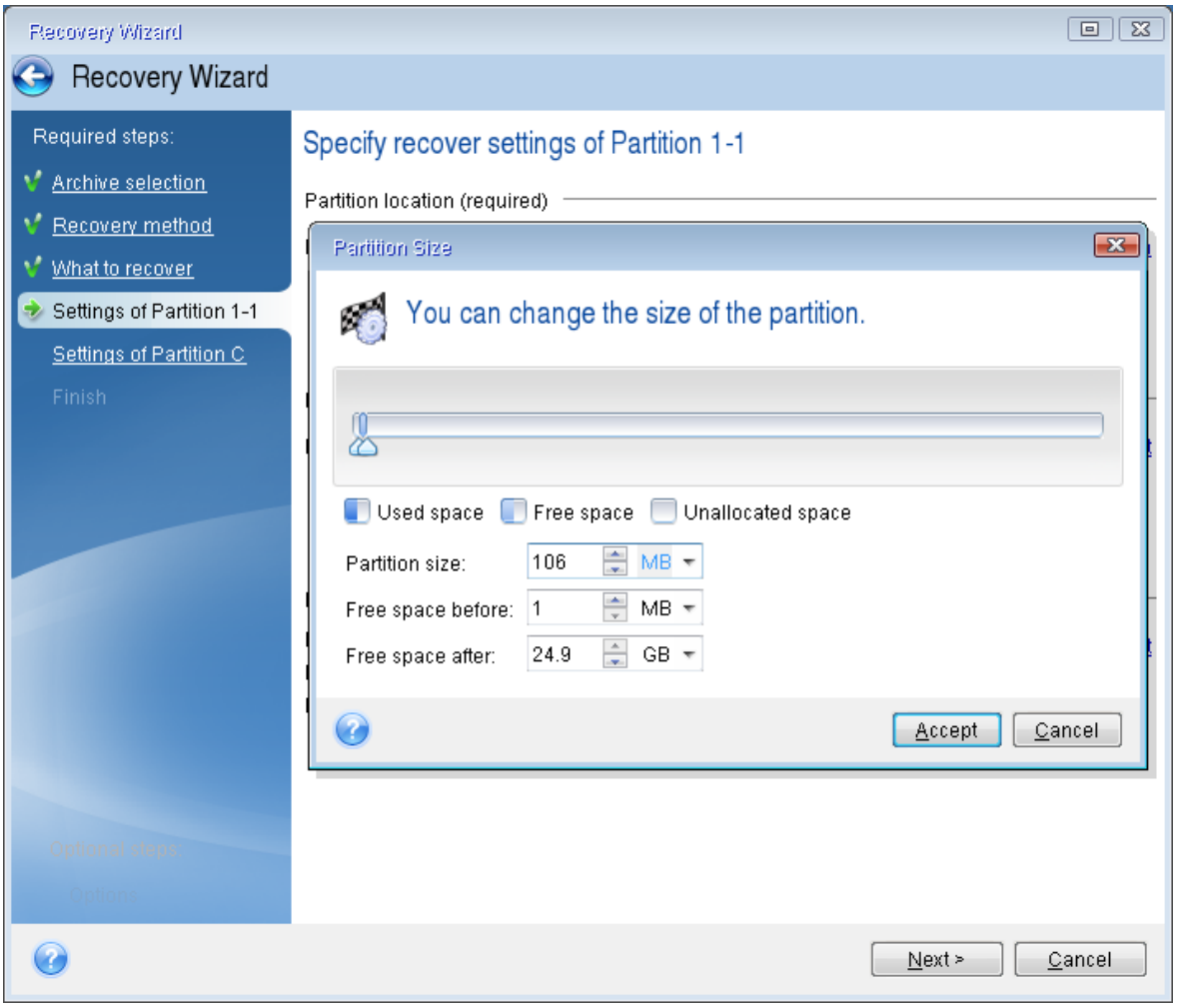



Selecting partitions leads to appearance of the relevant steps **Settings of partition**. Note that these steps start with partitions which do not have an assigned disk letter (as usually is the case with hidden partitions). The partitions then take an ascending order of partition disk letters. This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

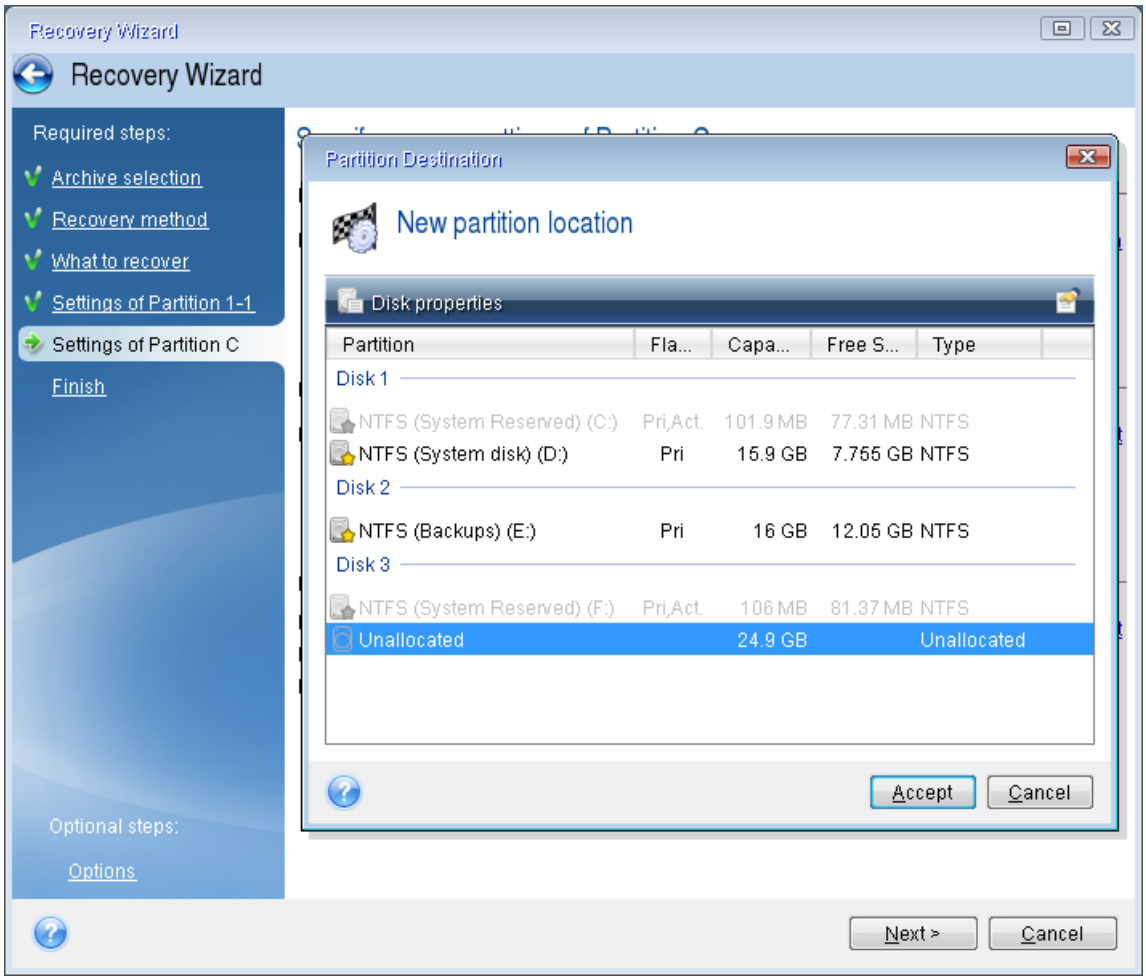
10. On the Settings of the hidden partition step (usually named Settings of Partition 1-1), specify the following settings:
    - **Location** – Click **New location**, select your new disk by either its assigned name or capacity, and then click **Accept**.



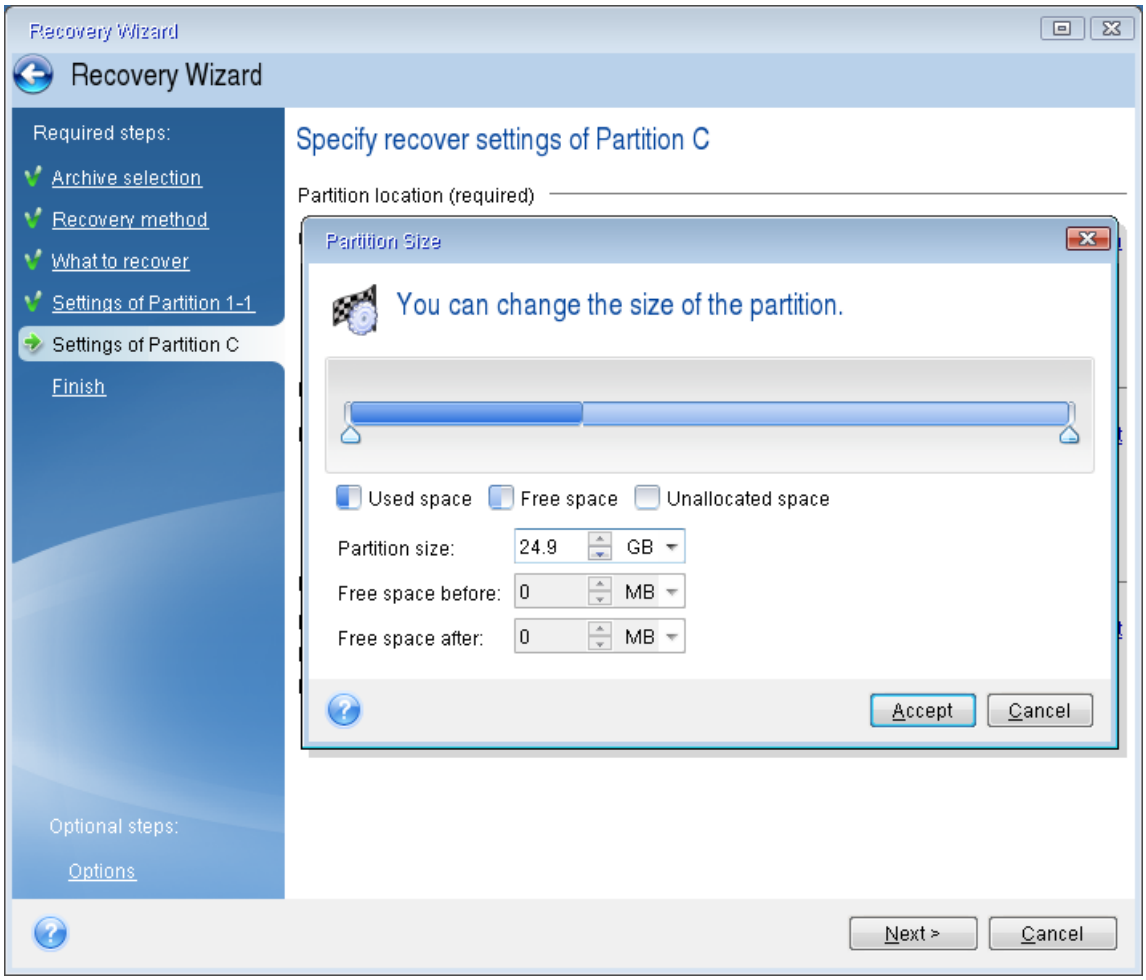

- **Type** – Check the partition type and change it, if necessary. Ensure that the System Reserved partition (if any) is primary and marked as active.
- **Size** – Click **Change default** in the Partition size area. By default the partition occupies the entire new disk. Enter the correct size in the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

### When the recovery is complete

Before you boot the computer, 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 bootable 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.

## Recovering partitions and disks

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

**Note**

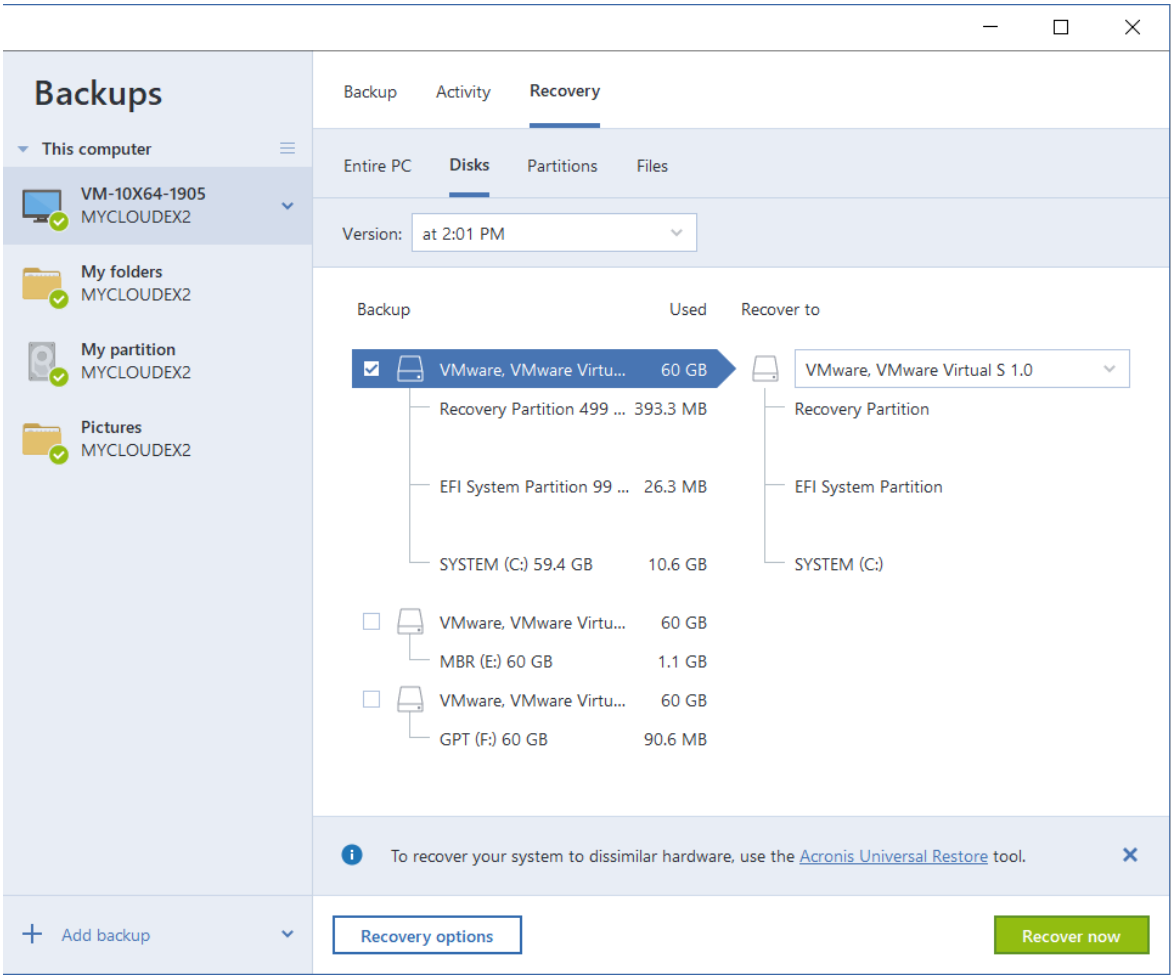
Before starting disk or partition recovery, make sure that the target disk has the same logical sector size as the original disk. Recovery to a disk with a different logical sector size is not supported and will fail. For example, older hard drives usually have a logical sector size of 512 bytes, while most modern HDDs and SSDs use 4096 bytes. For more information about verifying sector sizes, see the Support Portal article.

**Note**

Depending on your Internet connection speed, disk recovery from Acronis Cloud may take a long time.

***To recover partitions or disks***

1. Start Acronis True Image for SANDISK.
2. In the **Backup** section, select the backup which contains the partitions or disks you want to recover, then open the **Recovery** tab, 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.



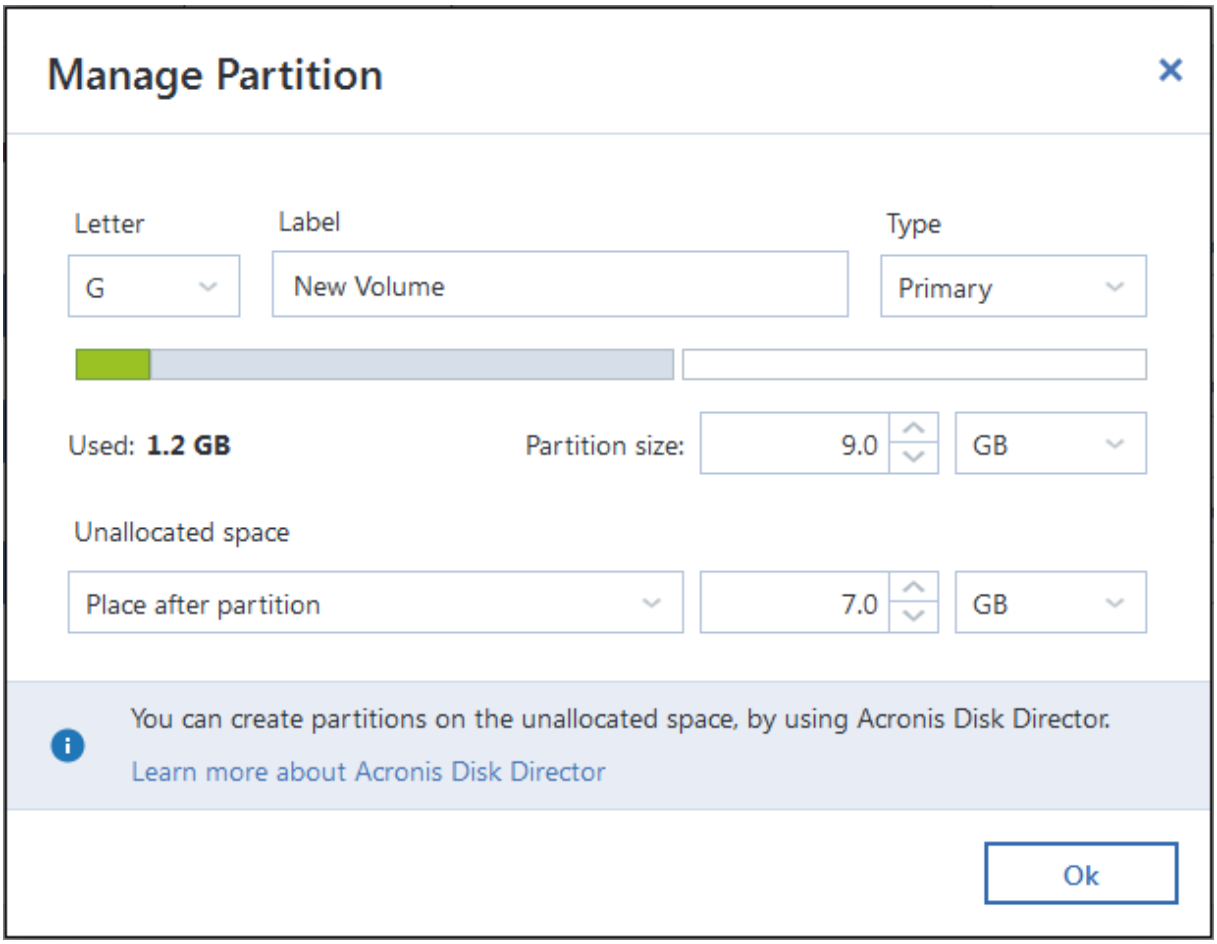
4. Select the **Disks** tab to recover disks or **Partitions** tab to recover specific partitions. Select the objects you need to recover.
5. In the recovery destination field below the partition name, select the destination partition. Unsuitable partitions are marked by a red border. Note that all data on the destination partition will be lost because it is replaced by the recovered data and file system.

   **Note**
   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] To set up additional parameters for the disk recovery process, click **Recovery options**.
7. After you finish with your selections, click **Recover now** to start recovery.
   If you are recovering the system to the same disk where Windows is installed, the computer will be restarted. After the restart, your computer will go to the Linux-based boot agent to complete the recovery process.
8. In the boot agent windows, follow the on-screen instructions.

## Partition properties

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




You can change the following partition properties:

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

# 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.**

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

  - **Original location (to the same dynamic volume).**
    The target volume type does not change.
  - **Another dynamic disk or volume.**
    The target volume type does not change. For example, when recovering a dynamic striped volume over a dynamic spanned volume the target volume remains spanned.
  - **Unallocated space of the dynamic group.**
    The recovered volume type will be the same as it was in the backup.
- **Basic volume or disk.**
  The target volume remains basic.
- **Bare-metal recovery.**
  When performing a so called "bare-metal recovery" of dynamic volumes to a new unformatted disk, the recovered volumes become basic. If you want the recovered volumes to remain dynamic, the target disks should be prepared as dynamic (partitioned and formatted). This can be done using third-party tools, for example, Windows Disk Management snap-in.

## Recovery of basic volumes and disks

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

## Partition style after recovery

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

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

| | My system is BIOS-booted (Windows or Acronis bootable media) | My system is UEFI-booted (Windows or Acronis bootable media) |
|---|---|---|
| **and my OS supports UEFI** | partition style will remain MBR, the destination disk will be bootable in BIOS. | disk bootable in UEFI. See Example of recovery to UEFI system. |
| **My source disk is GPT and my OS supports UEFI** | After operation completion, the partition style will remain GPT, the system will fail booting on BIOS, because your operating system cannot support booting from GPT on BIOS. | After operation completion, the partition style will remain GPT, the operating system will be bootable on UEFI. |

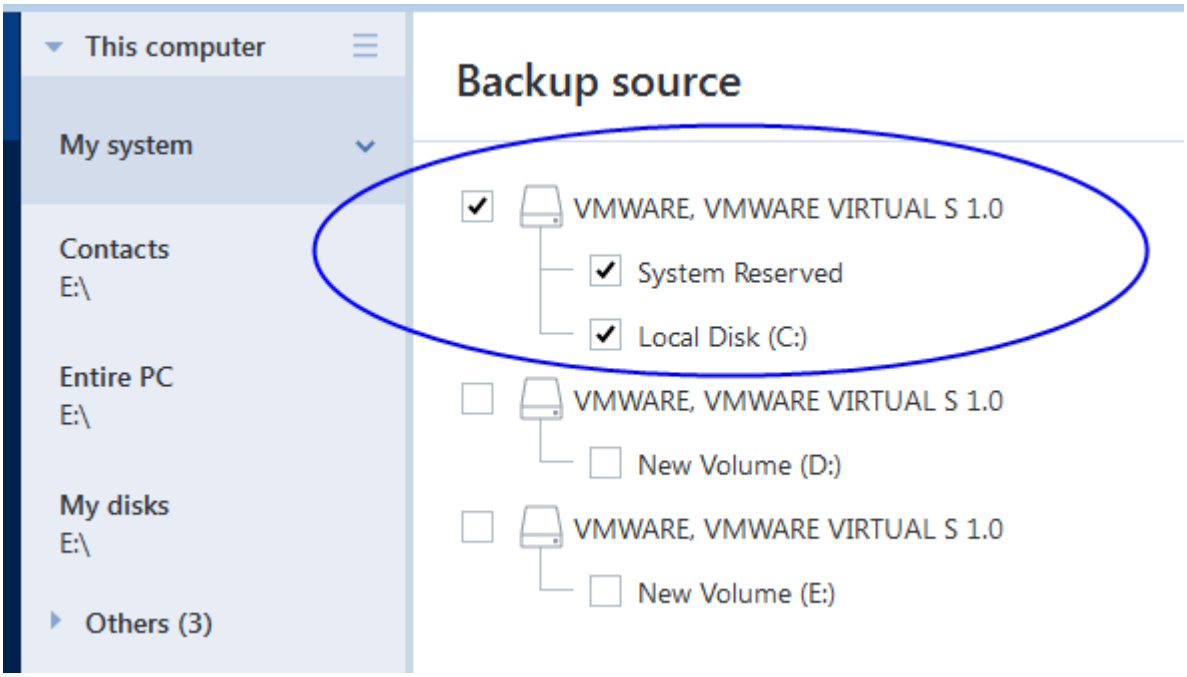
## Example of recovery to a UEFI system

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.

Before you start the procedure, ensure that you have:

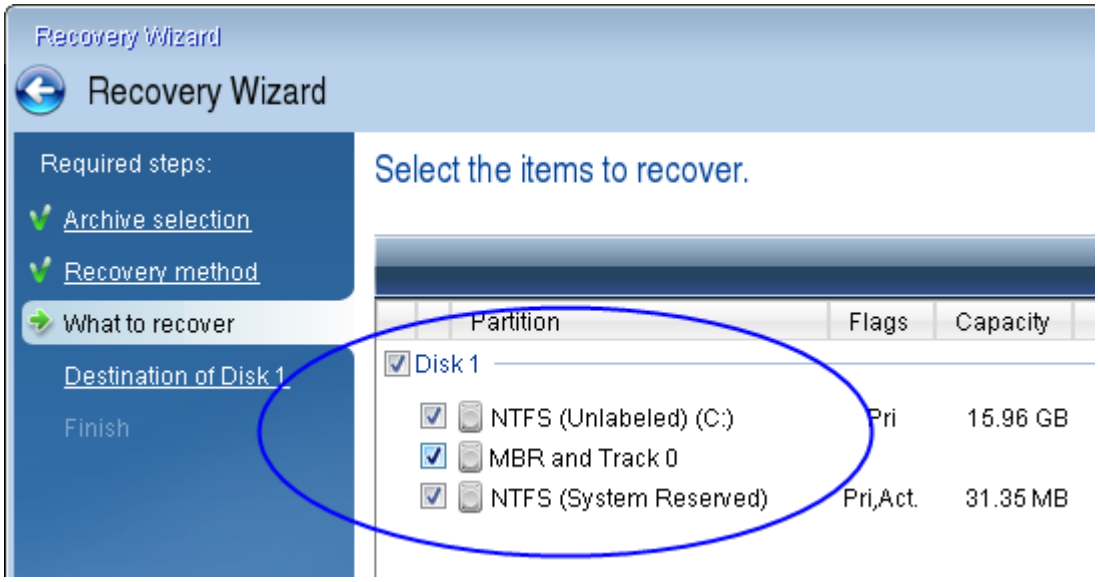
- **Acronis bootable media.**
  See Creating Acronis bootable media for details.
- **Backup of your system disk created in disk mode.**
  To create this backup, switch to disk mode, and then select the hard drive that contains your system partition. See Backing up disks and partitions for details.




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

1. Boot from the Acronis bootable media in UEFI mode and select Acronis True Image for SANDISK.
2. Run the **Recovery wizard** and follow the instructions described in Recovering your system.
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, 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.

## Arranging boot order in BIOS or UEFI BIOS

To boot your computer from Acronis bootable media, you need to arrange boot order so the media is the first booting device. The boot order is changed in BIOS or UEFI BIOS, depending on your computer firmware interface. The procedure in both cases is very similar.

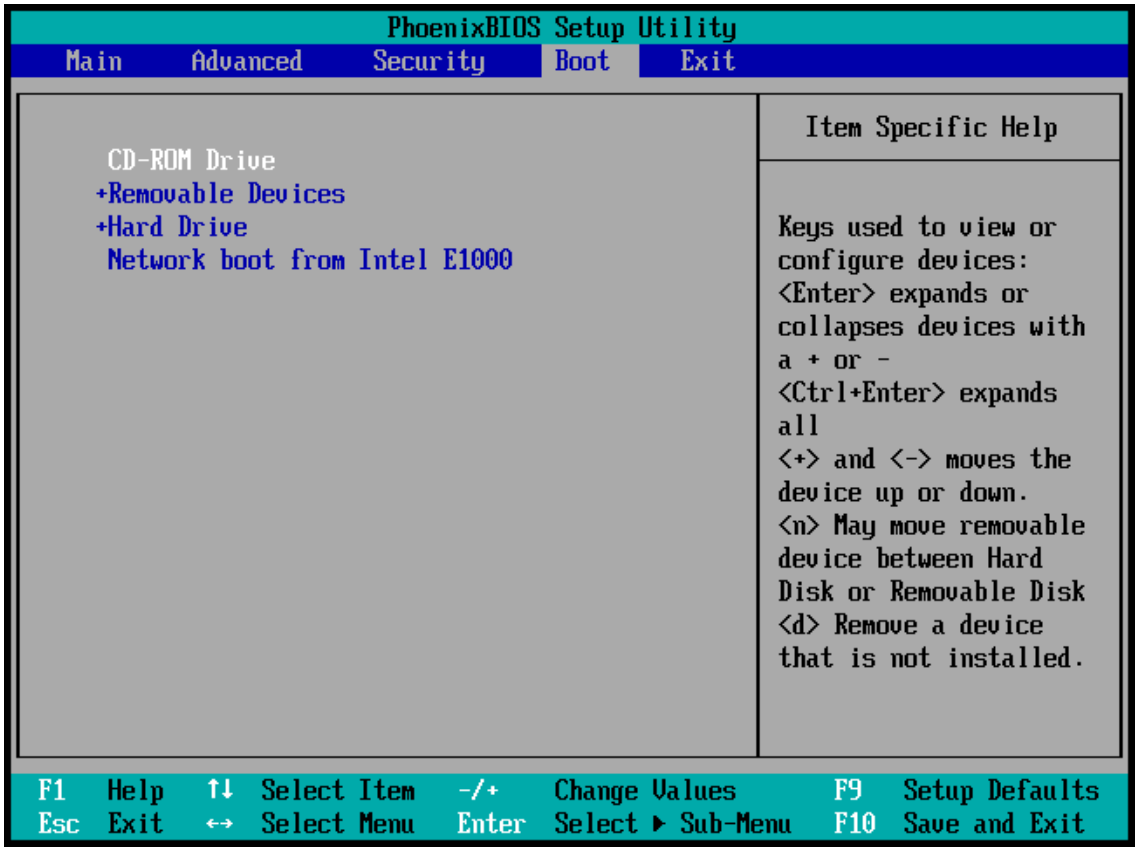
***To boot from Acronis bootable media***

1. If you use a USB flash drive or external 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 or UEFI BIOS.
3. Press the key combination (such as, **Del, F1, Ctrl+Alt+Esc, Ctrl+Esc**). The BIOS or UEFI BIOS setup utility will open. Note that utilities may differ in appearance, sets of items, names, etc.

**Note**

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 or UEFI 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 bootable media (CD, DVD or USB drive) device the first booting device:
   a. Navigate to the Boot order setting by using the arrow keys on your keyboard.
   b. 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 or UEFI BIOS and save the changes that you made. The computer will boot from Acronis bootable media.

**Note**

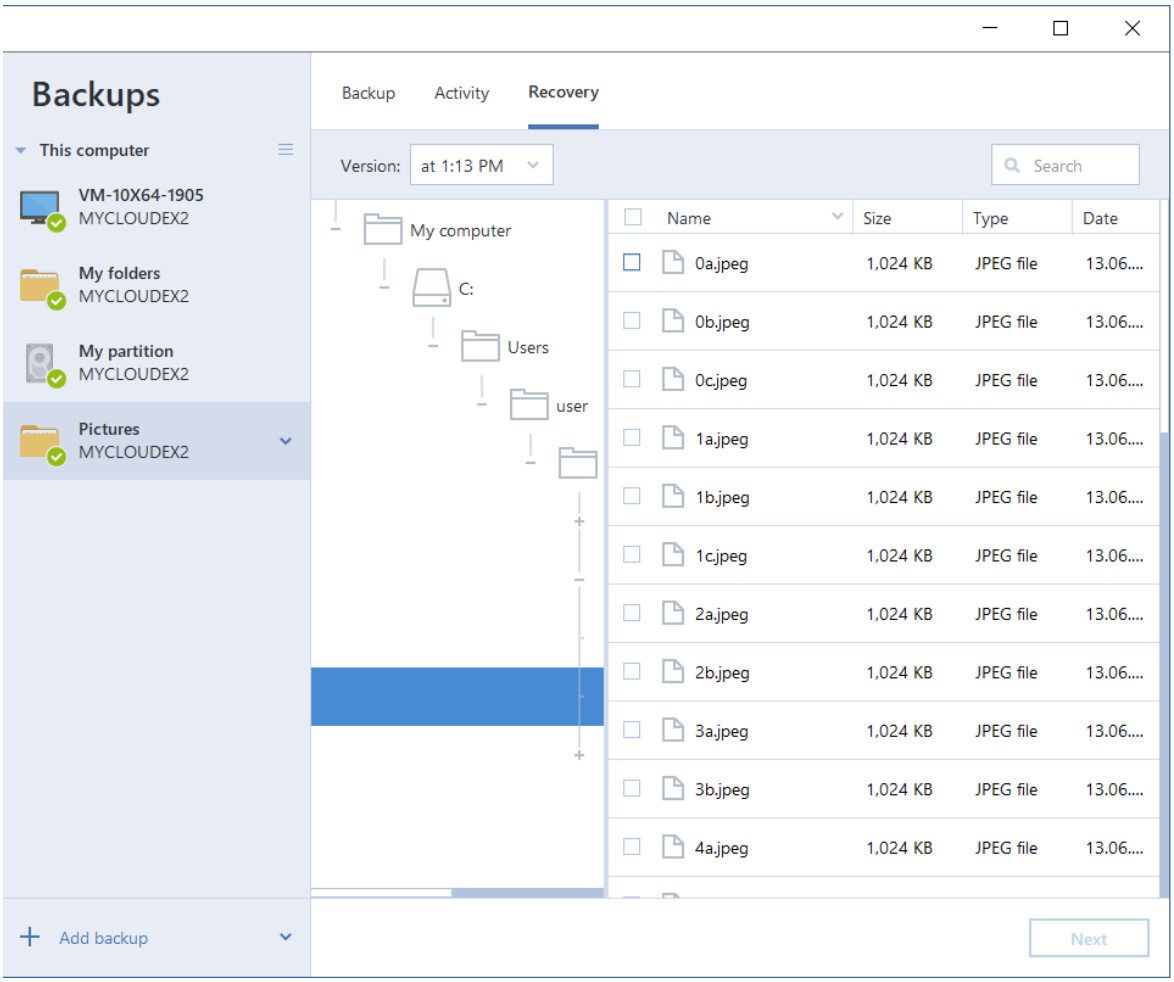
If the computer fails to boot from the first device, it tries to boot from the second device in the list, and so on.

# Recovering files and folders

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

***To recover data in Acronis True Image for SANDISK***

1. On the sidebar, click **Backup**.
2. From the backup list, select the backup which contains the files or folders that you want to recover, and then open the **Recovery** tab.
3. [Optional] On the toolbar, in the **Version** drop-down list, select the required date and time of the backup. By default, the latest backup is recovered.
4. Select the check box for the corresponding files or folders that you want to recover, and click **Next**.




5. [Optional] By default, the data is restored in the original location. To change it, click **Browse** on the toolbar, and then select the required destination folder.

**Note**
This option is available only if you have an internal or external SANDISK storage device attached to your system.

6. [Optional] Set the options for the recovery process (recovery process priority, file-level security settings, etc.). To set the options, click **Recovery options**. The options you set here will be applied only to the current recovery operation.
7. To start the recovery process, click the **Recover now** button.
   The selected file version is downloaded to the specified destination.

You can stop the recovery by clicking **Cancel**. Keep in mind that the aborted recovery may still cause changes in the destination folder.

**Note**
If you selected several files and folders, they will be placed into a zip archive.

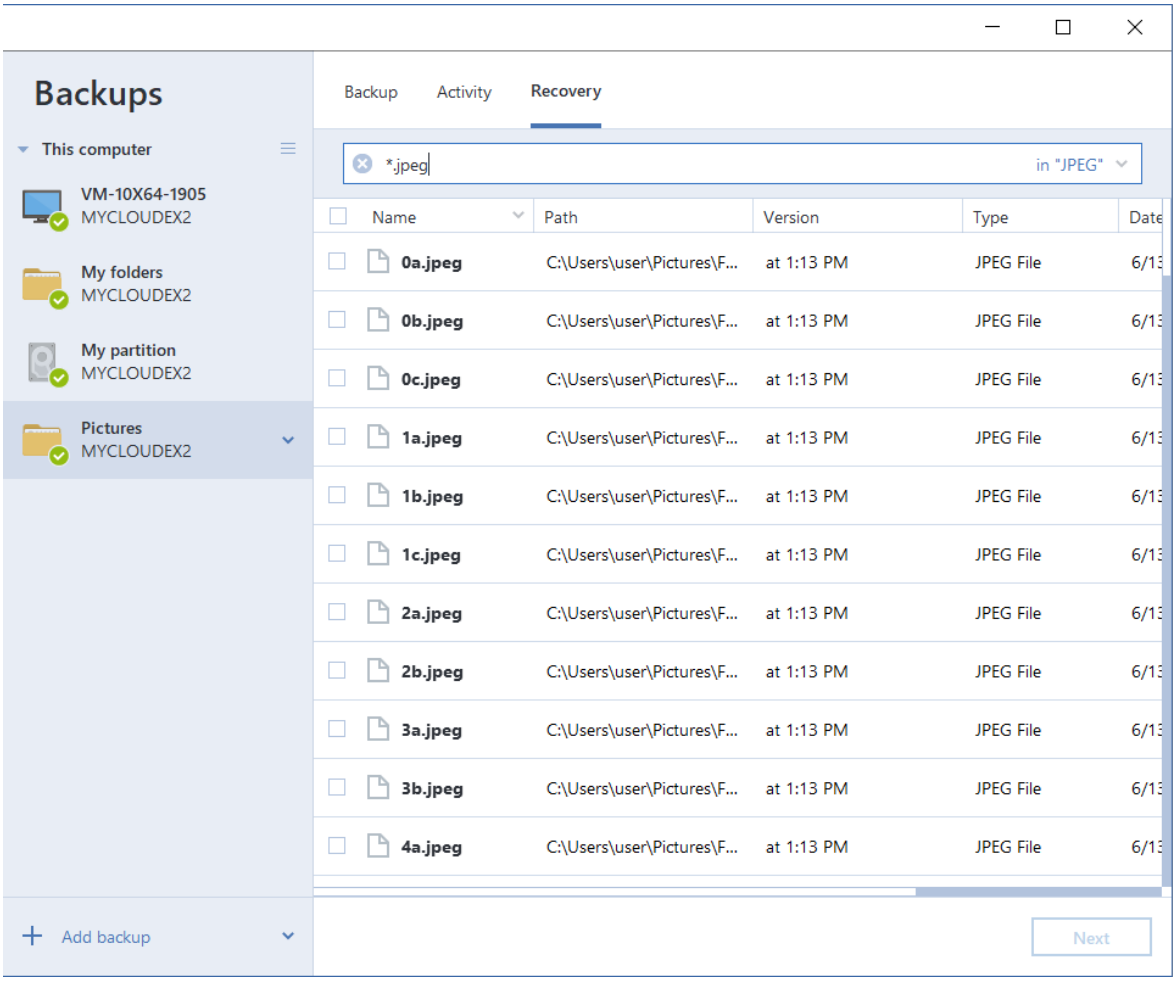
# Searching backup content

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

***To search for files and folders***

1. Start recovering data as described in Recovering partitions and disks or Recovering files and folders.
2. When selecting files and folders to recover, enter the file or folder name into the **Search** field. The program shows search results.

   You can also use the common Windows wildcard characters: * and ?. For example, to find all files with extension **.exe**, enter ***.exe**. To find all .exe files with names consisting of five symbols and starting with “my”, enter **My???.exe**.



3. By default, Acronis True Image for SANDISK searches the folder selected on the previous step. To include the entire backup in the search, click the down arrow, and then click **in entire backup**.
   To return to the previous step, delete the search text, and then click the cross icon.
4. After the search is complete, select the files that you want to recover, and then click **Next**.

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

# Recovery options

You can configure options for the disk/partition and file recovery processes. 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.

## Disk recovery mode

Location: **Recovery options** > **Advanced** > **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.

## Pre/Post commands for recovery

Location: **Recovery options** > **Advanced** > **Pre/Post commands**

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.

### 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.

## Validation option

Location: **Recovery options** > **Advanced** > **Validation**

- **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.

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

**Note**
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).

## Computer restart

Location: **Recovery options** > **Advanced** > **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.

## File recovery options

Location: **Recovery options** > **Advanced** > **File recovery options**

You can select the following file recovery options:

- **Recover files with their original security settings** - if the file security settings were preserved during backup, you can choose whether to recover them or let the files inherit the security settings of the folder where they will be recovered to. This option is effective only when recovering files from file/folder backups.
- **Set current date and time for recovered files** - you can choose whether to recover the file date and time from the backup or assign the files the current date and time. By default the file date and time from the backup will be assigned.

## Overwrite file options

Location: **Recovery options** > **Advanced** > **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.

**Note**
This option is available only while restoring files and folders (not disks and partitions).

Select the **Overwrite existing files** check box if you want to overwrite the files on the hard disk with the files from the backup. If the check box is cleared, the more recent files and folders will be kept on the disk.

If you do not need to overwrite some files:

- Select the **Hidden files and folders** check box to turn off overwriting of all hidden files and folders. This option is available for file-level backups to local destinations and network shares.
- Select the **System files and folders** check box to turn off overwriting of all system files and folders. This option is available for file-level backups to local destinations and network shares.
- Select the **More recent files and folders** check box to turn off 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. This option is available for file-level backups to local destinations and network shares.
  - To turn off overwriting of specific files, click the plus sign 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, select it in the list, and then click the minus sign.

## Performance of recovery operation

Location: **Recovery options** > **Advanced** > **Performance**

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 equal priority as other processes.
- **High** – The backup or recovery process will run faster, but the performance of other programs will be reduced. Be aware that selecting this option may result in 100% CPU usage by Acronis True Image for SANDISK.

# Notifications for recovery operation

Location: **Recovery options** > **Notifications**

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

By default all notifications are disabled.

## Free disk space threshold

You may want to be notified when the free space on the recovery storage becomes less than the specified threshold value. If after starting a backup Acronis True Image for SANDISK 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 recovery process and will immediately inform you by displaying an appropriate message. The message offers you three choices - to ignore it and proceed with the recovery, to browse for another location for the recovery or to cancel the recovery.

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

***To set the free disk space threshold***

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

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

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

**Note**
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.

**Note**
This option cannot be enabled for CD/DVD drives.

## Email notification

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

***If the test message sending fails***

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

***Additional notification settings***

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

- To send a notification with full log of operations, select the **Add full log to the notification** check box.

# Protection

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

## The Protection dashboard

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

To access the Protection dashboard, click **Protection** in the Acronis True Image for SANDISK side bar.

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

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

  **Note**
  By turning the protection off, you deactivate Active Protection.

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

## Active protection

To protect your computer from malicious software in real-time, Acronis True Image for SANDISK uses the Acronis Active Protection technology.

Active Protection constantly checks your computer while you continue working as usual. In addition to your files, Acronis Active Protection protects the Acronis True Image for SANDISK application files, your backups, and the Master Boot Records of your hard drives.

### Anti-ransomware protection

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

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

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

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

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

If Acronis True Image for SANDISK finds a good temporary copy, the file is restored from that copy.

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

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

## Configuring Active Protection

***To access Active Protection settings***

1. Click **Protection** on the sidebar, then click **Settings**, and go to the **Active Protection** tab.

***To configure Anti-ransomware Protection***

1. Switch on the **Anti-ransomware Protection** toggle to enable Anti-ransomware Protection.
   When enabled, it protects your computer from potentially harmful applications and processes that run in the background.
2. Select the options that you want to enable.
   - **Automatically recover files after blocking a process** – Though a process was blocked, there is still a possibility that your files were modified. If this check box is selected, Acronis True Image for SANDISK recovers the files as follows.
     Acronis True Image for SANDISK searches the following locations for the latest file versions to recover.
     - Temporary file copies that were preliminarily created during the process verification
     - Local backups

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

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

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

3. Click **OK**.

# Managing files in Quarantine

Quarantine is a special storage that is used to isolate blocked applications from your computer and data. When you place an application file in quarantine, the risk of potential harmful actions from the blocked application is minimized.

When Acronis True Image for SANDISK detects a suspicious process and informs you about it, you decide whether to place the corresponding application in quarantine.

A quarantine is created in the root folder of the partition where the attacked files were stored, for example C:\Acronis Active Protection Storage\Quarantine\. When you place a file in the quarantine, you can still operate it as an ordinary file – move it to another location, copy, or delete it. Be aware that Acronis True Image for SANDISK moves files to quarantine – it does not copy them. When you delete a file from quarantine, you delete it permanently, and it cannot be restored. If you place an application file in quarantine by mistake, you can still copy or move the file to its original location on your computer. The application will continue working normally.

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

***To restore or delete files from quarantine:***

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

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

1. On the **Protection** dashboard, click **Settings**, and click the **Advanced** tab.
2. In the **Quarantine** section, select the number of days to keep the quarantined items.

3. Click **OK**.

# Configuring Protection exclusions

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

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

***To remove files or folders from the Protection exclusions list***

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

# 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.
- Back up your old disk drive, and then recover it to the new one.

**See also**: Difference between Backup and Disk Clone

## Disk cloning utility

The Clone disk utility allows you to clone your hard disk drive by copying the partitions to another hard disk.

**Note**
This option is available only if you have an internal or external SANDISK storage device attached to your system.

Before you start:

- When you want to clone your system to a higher-capacity hard disk, we recommend that you 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 is especially important for laptops.

  **Note**
  It is recommended that your old and new hard drives work in the same controller mode. Otherwise, your computer might not start from the new hard drive.

  **Note**
  If you clone a disk with Windows to an external USB hard drive, you might not be able to boot from it. We recommend cloning to an internal SSD or HDD instead.

- The Clone disk utility does not support multiboot systems.
- 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 by 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.

**Note**

Please note that after cloning the disk, the used space on the original and destination drives may slightly differ for the following reasons:

- Acronis True Image for SANDISK excludes certain system files like pagefile.sys, swapfile.sys, and hiberfil.sys from cloning by default.
- If the source drive has compression and content indexing turned on, this could affect the size of the files on that drive. When cloning, these settings might not be replicated to the destination drive, leading to a difference in used space.

## Clone Disk wizard

Before you start, we recommend that you read general information about Disk cloning utility. If you use an UEFI computer and you decided to start the cloning procedure under bootable media, pay attention to the boot mode of the bootable media in UEFI BIOS. It is recommended that the boot mode matches the type of the system in the backup. If the backup contains a BIOS system, then boot the bootable media in BIOS mode; if the system is UEFI, then ensure that UEFI mode is set.

***To clone a disk***

1. Start Acronis True Image for SANDISK.
2. On the sidebar, click **Tools**, and then click **Clone disk**.
3. 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.

   **Note**

   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 **Summary** screen.

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

   **Note**

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

   Both the source and destination disks must have the same logical sector size (for example, 512 bytes or 4096 bytes). Cloning to a disk with a different logical sector size is not supported. For information about verifying these prerequisites, see the Support Portal article.

5. 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.

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

6. [This step is only available if the source disk has an OS installed]. On the **Disk Usage** step, select how you are going to use the clone.
   - **To replace a disk on this machine** – the system disk data will be copied, and the clone will be bootable. Use this clone for replacing the system disk with a new one on this PC.
   - **To use on another machine** – the system disk data will be copied, and the clone will be bootable. Use this clone to transfer all the data to another PC on a bootable disk.

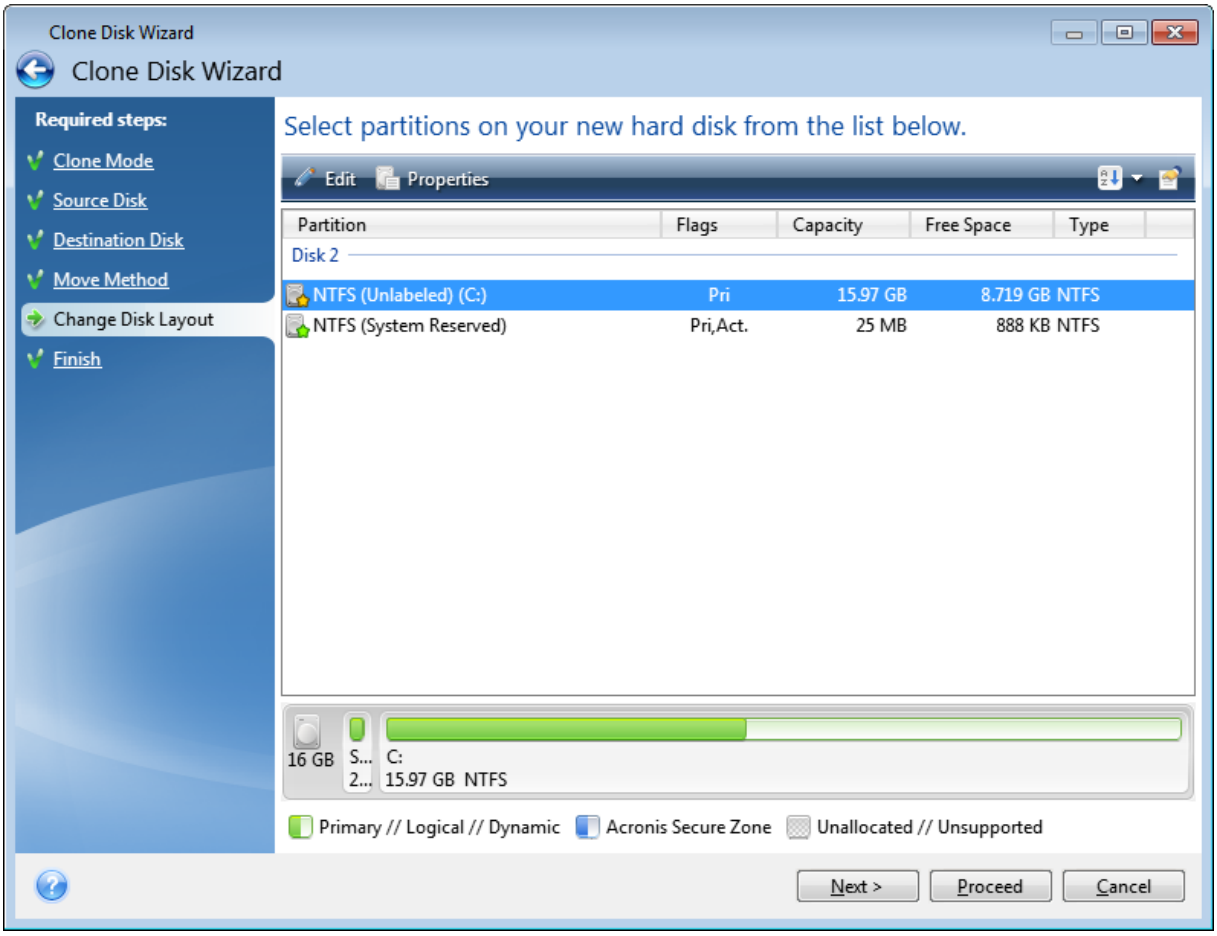
     **Note**
     The clone may not be bootable on a computer with different hardware. To make the cloned disk bootable, prepare necessary drivers and use Acronis True Image for SANDISK Universal Restore. For details, see Acronis True Image for SANDISK Active cloning in Windows.

   - **To use as a data disk** – the disk data will be copied. Use this clone as a non-bootable data drive.
7. [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.
8. [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. See Manual partitioning for details.
9. [Optional step] On the **What to exclude** step, you can specify files and folders that you do not want to clone. See Excluding items from cloning for details.
10. On the **Finish** step, ensure that the configured settings suit your needs, and then click **Proceed**.

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

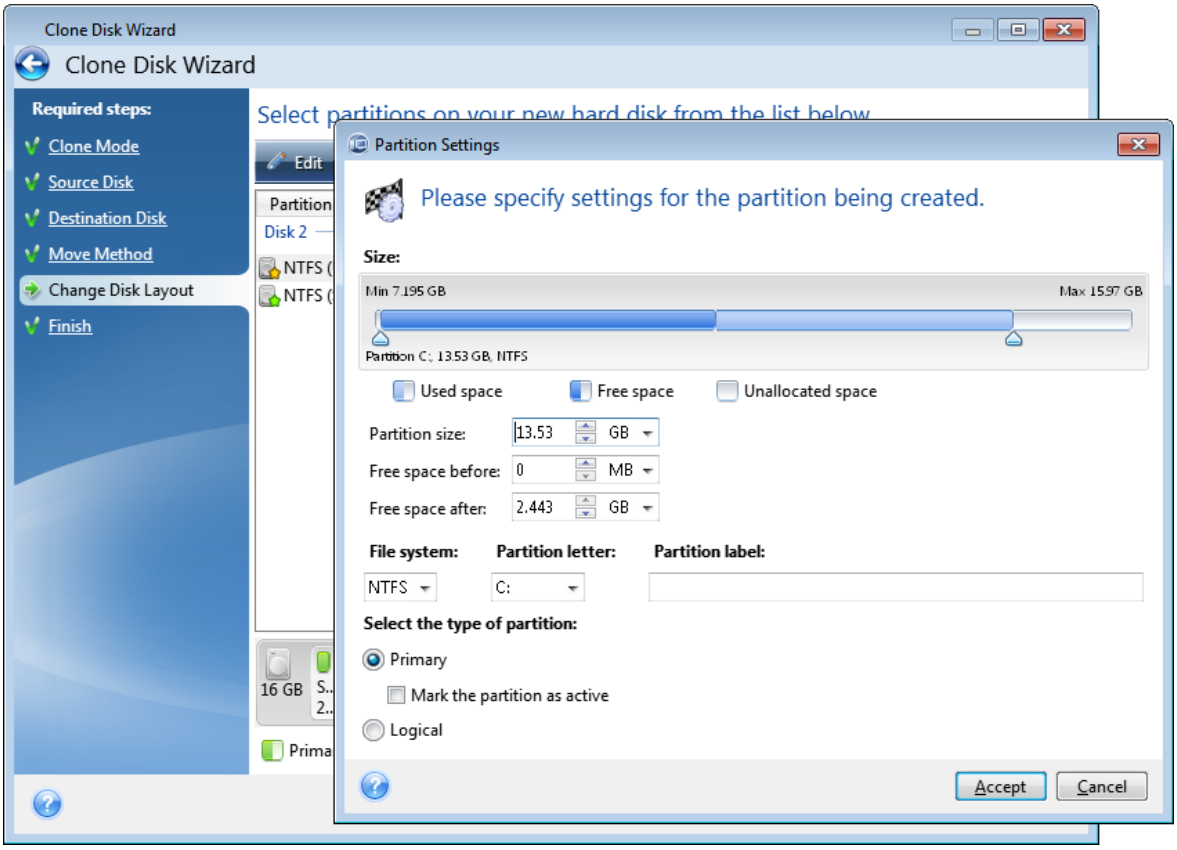
## Manual partitioning

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

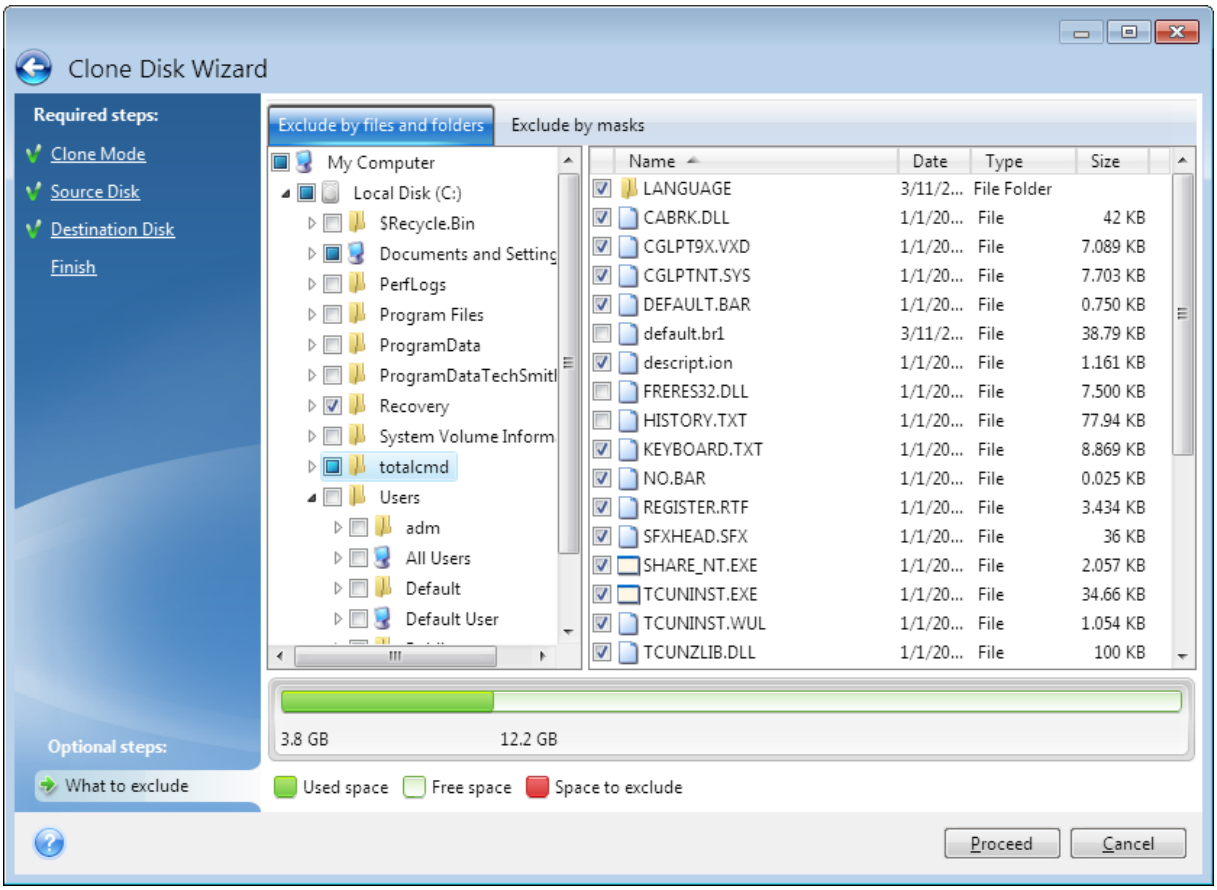
   See Partition settings for details.
3. Click **Accept**.

**Warning!**
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.

## 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.

**Note**
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.

# Migrating your system from an HDD to an SSD

First of all, make sure that Acronis True Image for SANDISK detects your new SSD both in Windows and under the Acronis bootable media. If there is a problem, see What to do if Acronis True Image for SANDISK does not recognize your SSD.

## SSD size

As SSDs usually have less capacity than HDDs, the occupied space on your old hard disk may exceed the size of your SSD. If this is the case, migration is not possible.

To reduce amount of data on your system disk, try the following:

- Move your data files from the old hard disk to another location, such as another hard disk drive, internal or external.
- Create .zip archives of data files (for example, your documents, pictures, audio files, etc.), and then delete the original files.
- Clean up the hard disk using the Windows Disk Cleanup utility.

Note that for stable operation, Windows needs to have several GB of free space on the system partition.

## Which migration method to choose

If your system disk consists of a single partition (not counting the hidden System Reserved partition), you can try to migrate to the SSD using the Clone tool. For more information see Cloning a hard disk.

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.

## What to do if Acronis True Image for SANDISK does not recognize your SSD

When you migrate your system from an HDD to an SSD, it is possible that Acronis True Image for SANDISK does not recognize your new 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 team of your SSD manufacturer.

***If the BIOS of your computer does show your new SSD***

1. Depending on your operating system, type `cmd` in the Search field or in the Run field, and then press **Enter**.
2. At the command line prompt type, enter:

   ```
   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.
3. To select the disk, run the following command:

   ```
   select disk N
   ```

   Here N is the disk number of your SSD.
4. To remove all information from the SSD and overwrite the MBR with the default one, run the command:

   ```
   clean
   exit
   exit
   ```

   **Important**
   Please pay attention that the `clean` command completely deletes all data from the selected disk. Do not perform this command if the disk contains any data. The command is applicable only for new disks that do not contain data.

Start Acronis True Image for SANDISK 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.

***To check whether your Acronis bootable media recognizes the SSD***

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

If the above suggestions do not help, try creating a WinPE-based media. This may provide the necessary drivers. For more information, see Creating Acronis bootable media.

## 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 10 and later, the system disk may have a hidden System Reserved partition.

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

***To migrate your system to an SSD***

1. Start Acronis True Image for SANDISK.
2. Create Acronis bootable 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.

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

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

# Tools

***Protection tools***

- "Acronis Media Builder" (p. 109)

***Disk cloning***

- "Disk cloning utility" (p. 100)

***Security and privacy***

- "Acronis DriveCleanser" (p. 125)

***Disk management***

- "Adding a new hard disk" (p. 120)

***Image mounting***

- "Mounting a backup image" (p. 130)
- "Unmounting an image" (p. 132)

## Acronis Media Builder

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

**You can create several types of bootable media:**

- **Acronis bootable media**
  This type is recommended for most users.
- **WinPE-based media with the Acronis plug-in**
  Running Acronis True Image for SANDISK in the preinstallation environment may provide better compatibility with your computer's hardware because the preinstallation environment uses Windows drivers.
  We recommend that you create this type of media, when Acronis bootable media did not help you boot your computer.
  To use this option, you need the following component to be installed:
  - Windows Assessment and Deployment Kit (ADK).
    This component is required for creating WinPE 4.0, WinPE 5.0, and WinPE 10.0.
- **WinRE-based media with the Acronis plug-in**
  This type of bootable media is similar to WinPE-based media, but it has an important advantage – you do not need to download ADK (formerly known as WADK or WAIK) from the Microsoft website. Windows Recovery Environment is included in supported versions of Windows (starting from Windows 10 and later). Acronis True Image for SANDISK uses these files from your system to create WinRE-based media. Similar to WinPE-based media, you can add your drivers for better

compatibility with your hardware. However, WinRE-based media can be used only on the computer where it was created or on a computer with the same Windows version and bitness (for example, Windows 10 x64).

**Notes**

- We recommend that you create a new bootable media after each Acronis True Image for SANDISK update.
- If you use non-optical media, the media must have a FAT16 or FAT32 file system.
- Acronis Media Builder supports only x64 WinPE 4.0, WinPE 5.0, and WinPE 10.0.
- Your computer must have:
  - For WinPE 4.0 – at least 512 MB RAM
  - For WinPE 5.0 – at least 1 GB RAM
  - For WinPE 10.0 – at least 512 MB RAM
- If Acronis Media Builder does not recognize your USB flash drive, you can try using the procedure described in the Support Portal article.
- When booting from the bootable media, you cannot perform backups to disks or partitions with Ext2/Ext3/Ext4, ReiserFS, and Linux SWAP file systems.
- When booting from the bootable media and using a standalone version of Acronis True Image for SANDISK, you cannot recover files and folders encrypted with the encryption available in Windows operating systems. However, backups encrypted using the Acronis True Image for SANDISK encryption feature can be recovered.

## Creating Acronis bootable media

1. Plug in a USB flash drive, or an external drive (HDD/SSD), or insert a blank CD or DVD.
2. Start Acronis True Image for SANDISK.
3. In the **Tools** section, click **Bootable Rescue Media Builder**.
4. Choose a creation method.
   - **Simple** – This is the easiest option. Acronis True Image for SANDISK will choose the optimal media type for your computer. If you use Windows 10 or a later version, WinRE-based media will be created.
   - **Advanced** – This option allows you to choose a media type. This means you can create the bootable media not only for your computer, but for a computer running a different Windows version. See Acronis Media Builder for details.

     If you select a Linux-based media, choose Acronis True Image for SANDISK components to be placed on the media. Ensure that the components that you select are compatible with the target computer architecture.

     If you select a WinRE-based or WinPE-based media, then:
     - Select an architecture type of the media – 32-bit or 64-bit. Note that 32-bit bootable media can work only on 32-bit computers, and 64-bit media is compatible with both 32-bit and 64-bit computers.

- Select a toolkit that you want to be used for creating the bootable media. If you choose WAIK or WADK and you do not have the selected kit installed on your computer, then you first need to download it from the Microsoft website, and then install the required components – Deployment Tools and Windows Preinstallation Environment (Windows PE).

  If you already have WinPE files on your computer and they are stored in a non-default folder, then just specify their location and the Acronis plug-in will be added to the existing WinPE image.
- For better compatibility with your hardware, you can select drivers to be added to the media. Acronis True Image for SANDISK searches for and suggests drivers suitable for your system.

  If the search process takes too long, you can stop it by clicking the **Cancel search** button and confirming your choice.

5. Select a destination for the media:
   - **CD**
   - **DVD**
   - **External drive**
   - **USB flash drive**

     If your drive has an unsupported file system, Acronis True Image for SANDISK will suggest formatting it to FAT file system.

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

     **Note**
     Most hardware cannot correctly handle USB flash drives with more than 32 GB of capacity, which can lead to bootability issues. Avoid using USB flash drives larger than 32 GB. Common sizes, such as 8 GB or 16 GB, are sufficient for these tasks.

   - **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 10 and later, you can do this by using a built-in burning tool. In File Explorer, double-click the created ISO image file, and then click **Burn**.
   - **WIM image file** (available only for WinPE-based media)

     Acronis True Image for SANDISK adds the Acronis plug-in to the .wim file from 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. See Creating an .iso file from a .wim file for details.
6. Click **Proceed**.

## Acronis bootable media startup parameters

Here, you can set Acronis bootable media startup parameters in order to configure the 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 Acronis bootable media, it may be best to contact the Acronis Support team.

***To add startup parameters***

1. Enter a command into the **Parameters** field. You can type several commands, separated by spaces.
2. 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 True Image for SANDISK 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.

## Adding drivers to an existing .wim image

Sometimes a basic WinPE disk with Acronis plug-in does not have drivers for your specific hardware, for example, for storage device controllers. The easiest way to add them is to select the Advanced mode in Acronis Media Builder and specify the drivers to add. You can add the drivers manually to an existing .wim file before creating an ISO file with Acronis plug-in.

**Warning!**
Attention! You can only add drivers which have the .inf filename extension.

The following procedure is based on an MSDN article that can be found at https://technet.microsoft.com/.

***To create a custom Windows PE image***

1. If you don't have the .wim file with the Acronis plug-in, start Acronis Media Builder and create it by choosing **WIM file** as a destination for the WinPE-based media. See Creating Acronis bootable media for details.
2. Depending on your version of Windows AIK or Windows ADK, do one of the following:

- In the **Start** menu, click **Microsoft Windows AIK**, right-click **Windows PE Tools Command Prompt**, and then select **Run as administrator**.
- In the **Start** menu, click **Microsoft Windows AIK**, right-click **Deployment Tools Command Prompt**, and then select **Run as administrator**.
- In the **Start** menu, click **Windows Kits**, click **Windows ADK**, right-click **Deployment and Imaging Tools Environment**, and then select **Run as administrator**.

3. Run the Copype.cmd script to create a folder with Windows PE files. For example, from a command prompt, type:

```
copype amd64 C:\winpe_x64
```

4. Copy your .wim file, for example, to folder C:\winpe_x64\. By default, this file is named AcronisBootablePEMedia.wim.
5. Mount the base image to a local directory by using the DISM tool. To do this, type:

```
Dism /Mount-Wim /WimFile:C:\winpe_x64\AcronisBootablePEMedia.wim /index:1
/MountDir:C:\winpe_x64\mount
```

6. Add your hardware driver, by using the DISM command with the Add-Driver option. For example, to add the Mydriver.inf driver located in folder C:\drivers\, type:

```
Dism /image:C:\winpe_x64\mount /Add-Driver /driver:C:\drivers\mydriver.inf
```

7. Repeat the previous step for each driver that you need to add.
8. Commit the changes by using the DISM command:

```
Dism /Unmount-Wim /MountDir:C:\winpe_x64\mount /Commit
```

9. Create a PE image (.iso file) from the resulting .wim file. Refer to Creating an .iso file from a .wim file for details.

## Creating an .iso file from a .wim file

To create a bootable media by using a .wim file, you need to convert it to an .iso file first.

***To create a PE image (.iso file) from the resulting .wim file***

1. Depending on your version of Windows AIK or Windows ADK, do one of the following:
   - In the **Start** menu, click **Microsoft Windows AIK**, right-click **Windows PE Tools Command Prompt**, and then select **Run as administrator**.
   - In the **Start** menu, click **Microsoft Windows AIK**, right-click **Deployment Tools Command Prompt**, and then select **Run as administrator**.
   - In the **Start** menu, click **Windows Kits**, click **Windows ADK**, right-click **Deployment and Imaging Tools Environment**, and then select **Run as administrator**.
2. Run the Copype.cmd script to create a folder with Windows PE files. For example, from a command prompt, type:

```
copype amd64 C:\winpe_x64
```

3. Replace the default boot.wim file in your Windows PE folder with the newly created .wim file (for example, AcronisBootablePEMedia.wim). If the AcronisBootablePEMedia.wim file is located on c:\, then:

   For WinPE 3.0, type:

   ```
   copy c:\AcronisBootablePEMedia.wim c:\winpe_x64\ISO\sources\boot.wim
   ```

   For WinPE 4.0, WinPE 5.0 or WinPE 10.0, type:

   ```
   copy "c:\AcronisBootablePEMedia.wim" c:\winpe_x64\media\sources\boot.wim
   ```

4. Use the **Oscdimg** tool. To create an .iso file, type:

   ```
   oscdimg -n -bc:\winpe_x64\etfsboot.com c:\winpe_x64\ISO c:\winpe_x64\winpe_x64.iso
   ```

   Alternatively, to make the media bootable on both BIOS and UEFI computers, type:

   ```
   oscdimg -m -o -u2 -udfver102 -bootdata:2#p0,e,bc:\winpe_
   x64\fwfiles\etfsboot.com#pEF,e,bc:\winpe_x64\fwfiles\efisys.bin c:\winpe_x64\media
   c:\winpe_x64\winpe_x64.iso
   ```

5. Burn the .iso file to a CD by using a third-party tool, and you will have a bootable Windows PE disc with Acronis True Image for SANDISK.

# Making sure that your bootable 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 bootable media. In addition, you must check that the bootable media recognizes all of your computer's devices, such as the hard drives, mouse, keyboard, and network adapter.

If you purchased a boxed version of the product that has a bootable CD and you did not update Acronis True Image for SANDISK, you can test this CD. Otherwise, create a new bootable media. See Creating Acronis bootable media for details.

***To test the bootable media***

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

1. Configure your computer to enable booting from the bootable media. Then, make your bootable media device (CD-ROM/DVD-ROM or USB drive) the first boot device. See Arranging boot order in BIOS for details.

2. If you have a bootable CD, press any key to start booting from the CD, when you see the "Press any key to boot from CD" prompt. If you do not press a key within five seconds, you will need to restart the computer.
3. After the boot menu appears, choose **Acronis True Image for SANDISK**.

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

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

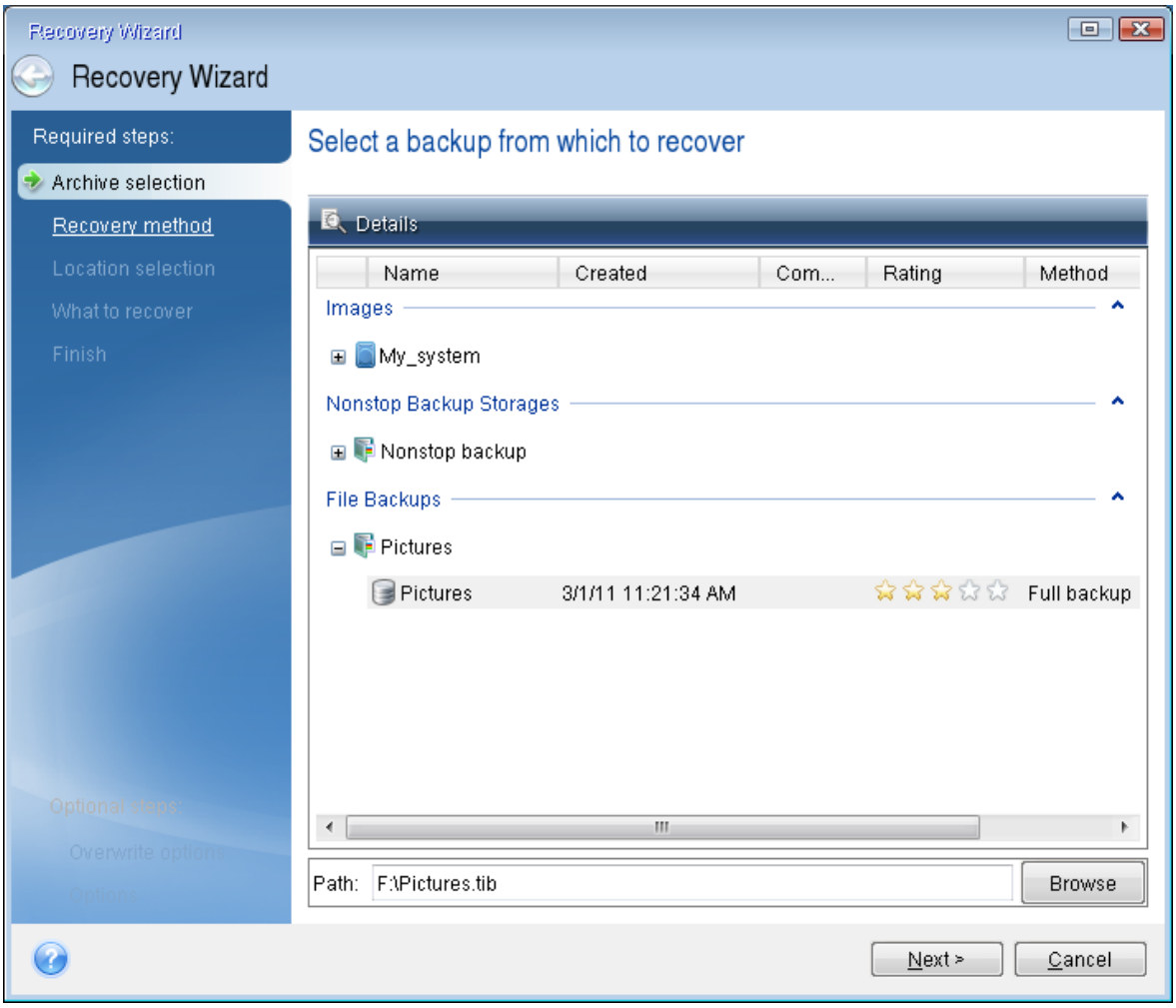
> **Note**
> If you have a spare hard drive, we strongly recommend that you try a test recovery of your system partition to this hard drive.

***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.

> **Note**
> 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**.

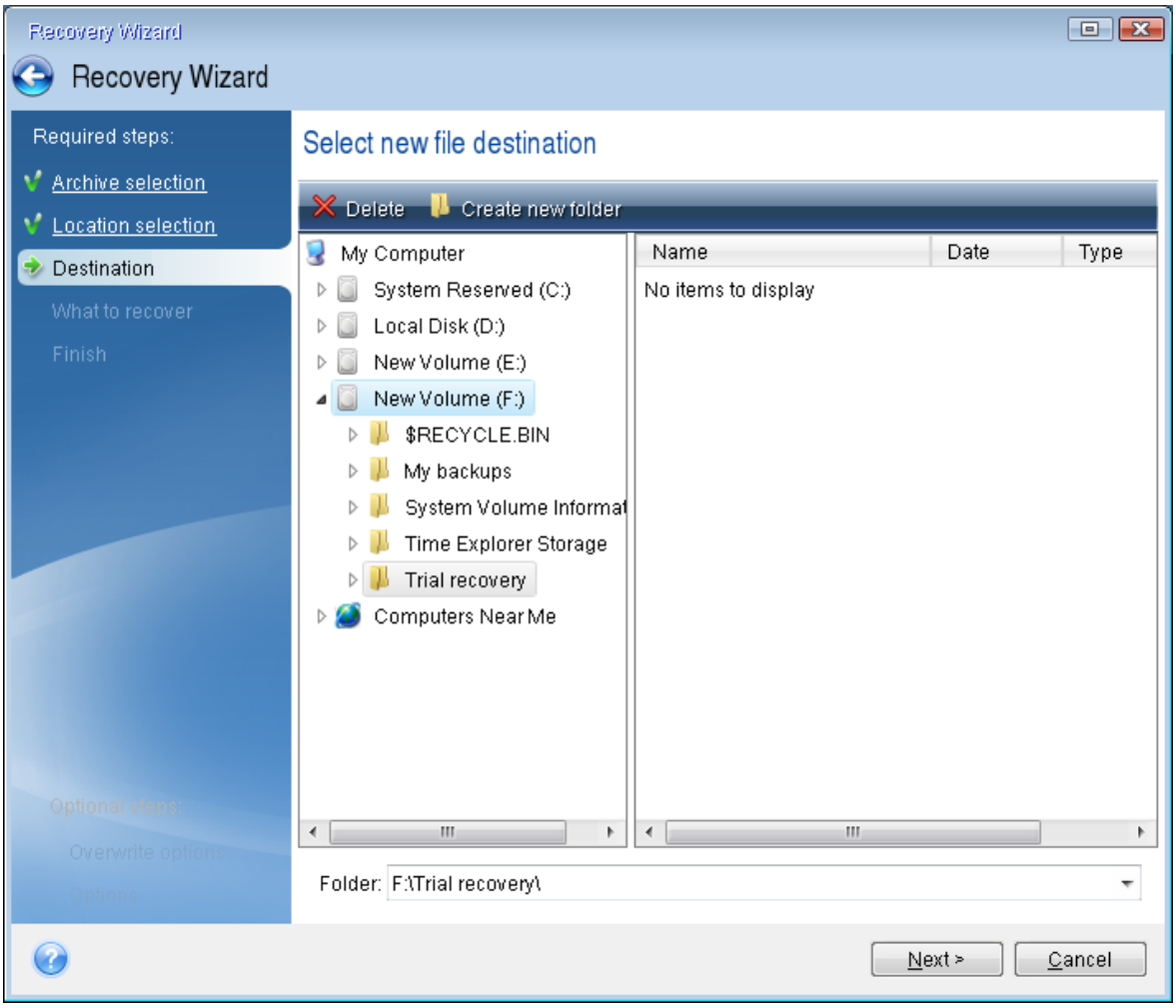



3. When recovering files with the bootable CD, you are able to select only a new location for the files to be recovered. Therefore, just click **Next** at the **Location selection** step.
4. After the **Destination** window opens, check that all of your drives are shown under **My Computer**.

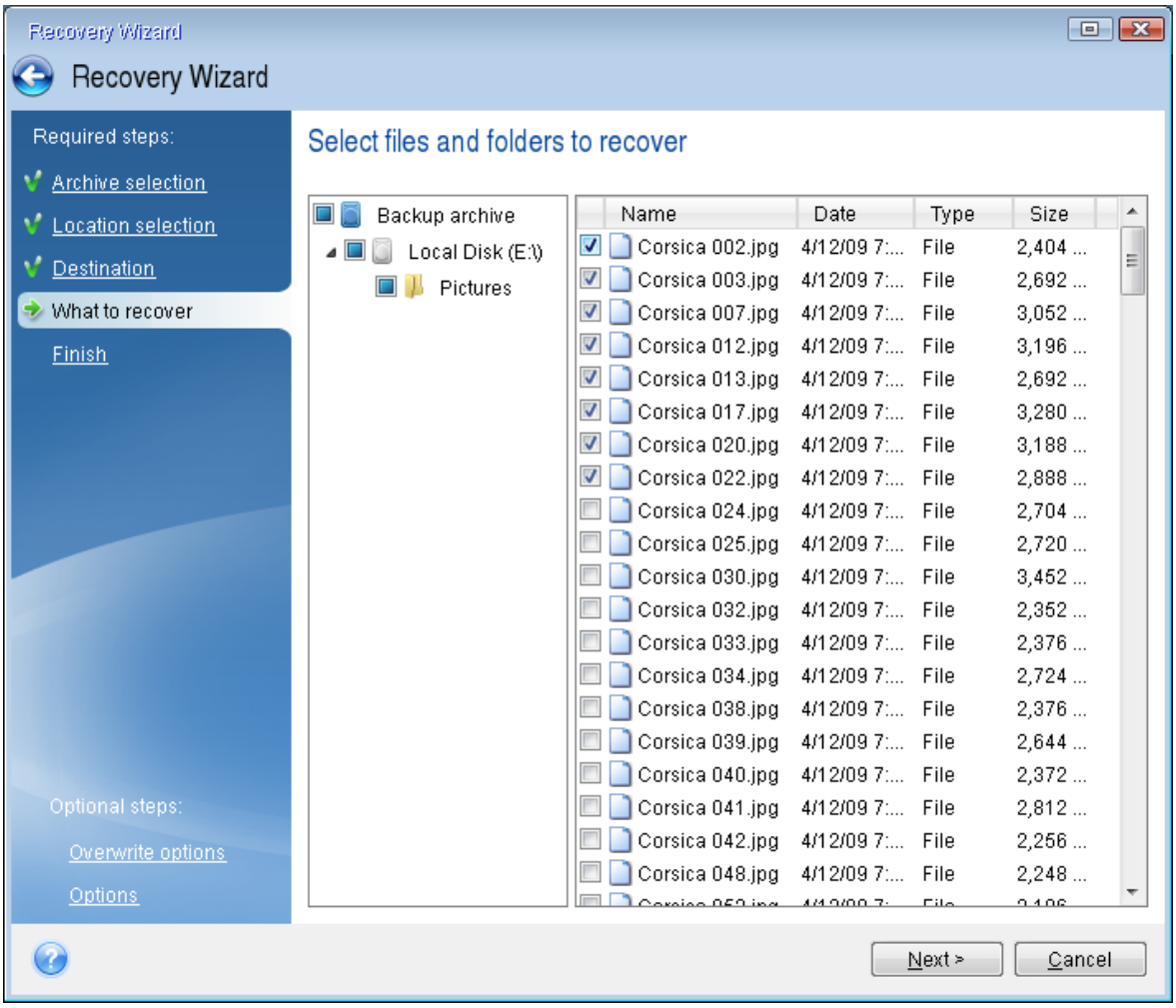
**Note**
If you store your backups on the network, verify that you can access the network.

**Note**
If no computers are visible on the network, but the **Computers Near Me** icon is found under **My Computer**, specify the network settings manually. To do this, open the window available at **Tools & Utilities** > **Options** > **Network adapters**.

**Note**
If the **Computers Near Me** icon is not available under **My Computer**, there may be problems either with your network card or with the card driver provided with Acronis True Image for SANDISK.




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**.



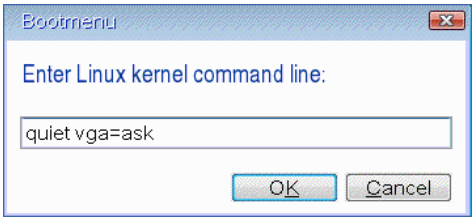

7. Click **Proceed** on the Summary window to start recovery.
8. After the recovery finishes, exit the standalone Acronis True Image for SANDISK.

Now, you can be reasonably sure that your bootable CD will help you when you need it.

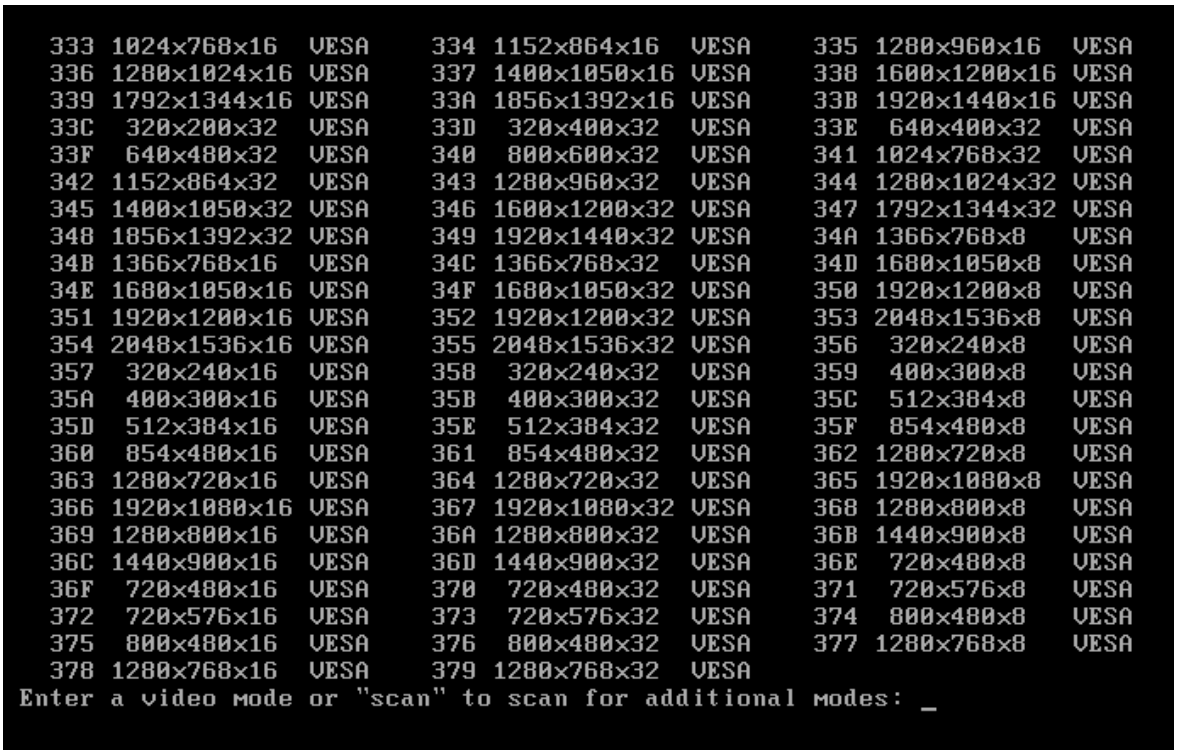
## Selecting video mode when booting from the bootable media

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

1. Start booting from the bootable media. When the boot menu appears, hover the mouse over **Acronis True Image for SANDISK** item and press the F11 key.
2. When the command line appears, type **vga=ask** and click **OK**.



3. Select **Acronis True Image for SANDISK** in the boot menu to continue booting from the bootable media. To see the available video modes, press the Enter key when the appropriate message appears.
4. Choose a video mode you think best suitable for your monitor and type its number in the command line. For instance, typing 338 selects video mode 1600x1200x16 (see the below figure).




5. Wait until Acronis True Image for SANDISK starts and make sure that the quality of the Welcome screen display on your monitor suits you.

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

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

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

# 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***

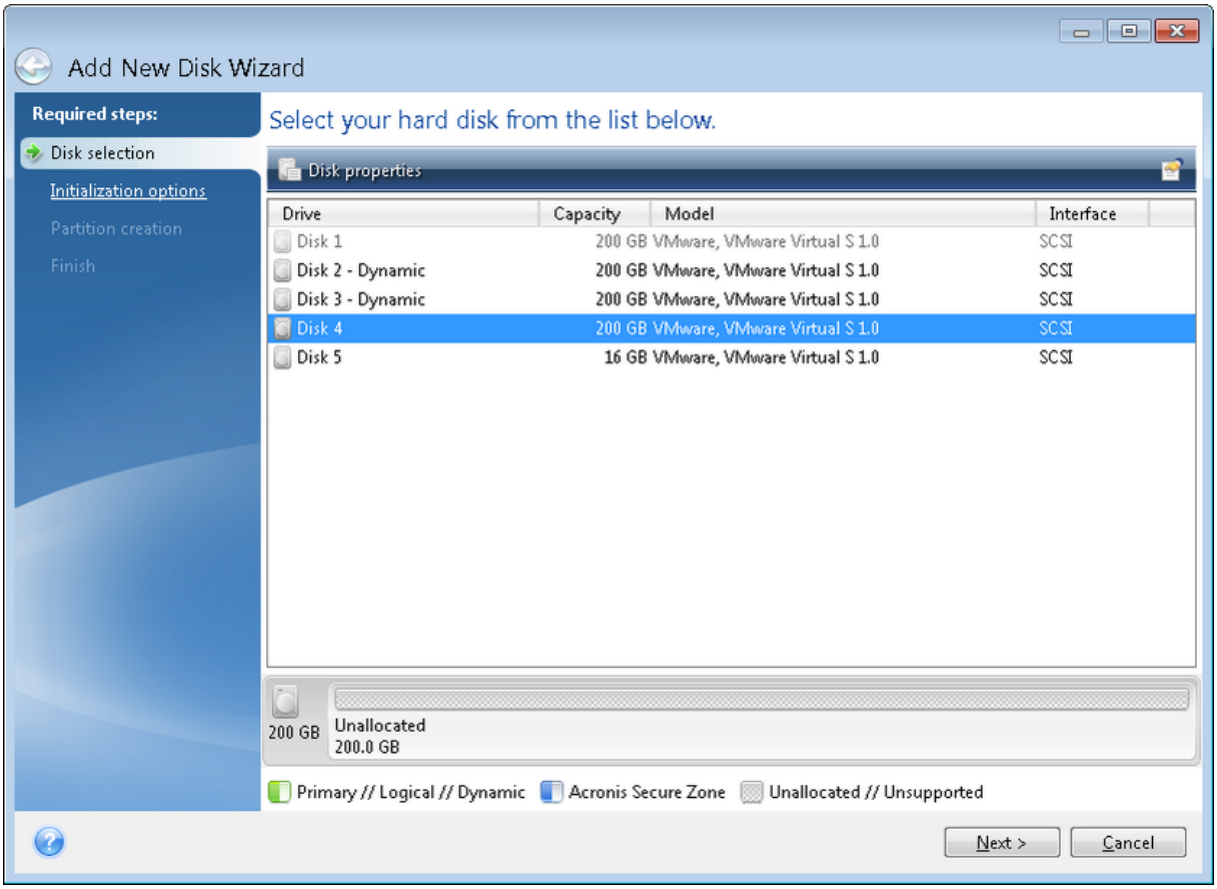
1. Shut down your computer, and then install the new disk.
2. Turn on your computer.
3. Click the **Start** button > **Acronis** (product folder) > **Add New Disk**.

4. Follow the wizard steps.
5. On the **Finish** step, ensure that the configured disk layout suits your needs, and then click **Proceed**.

## Selecting a hard disk

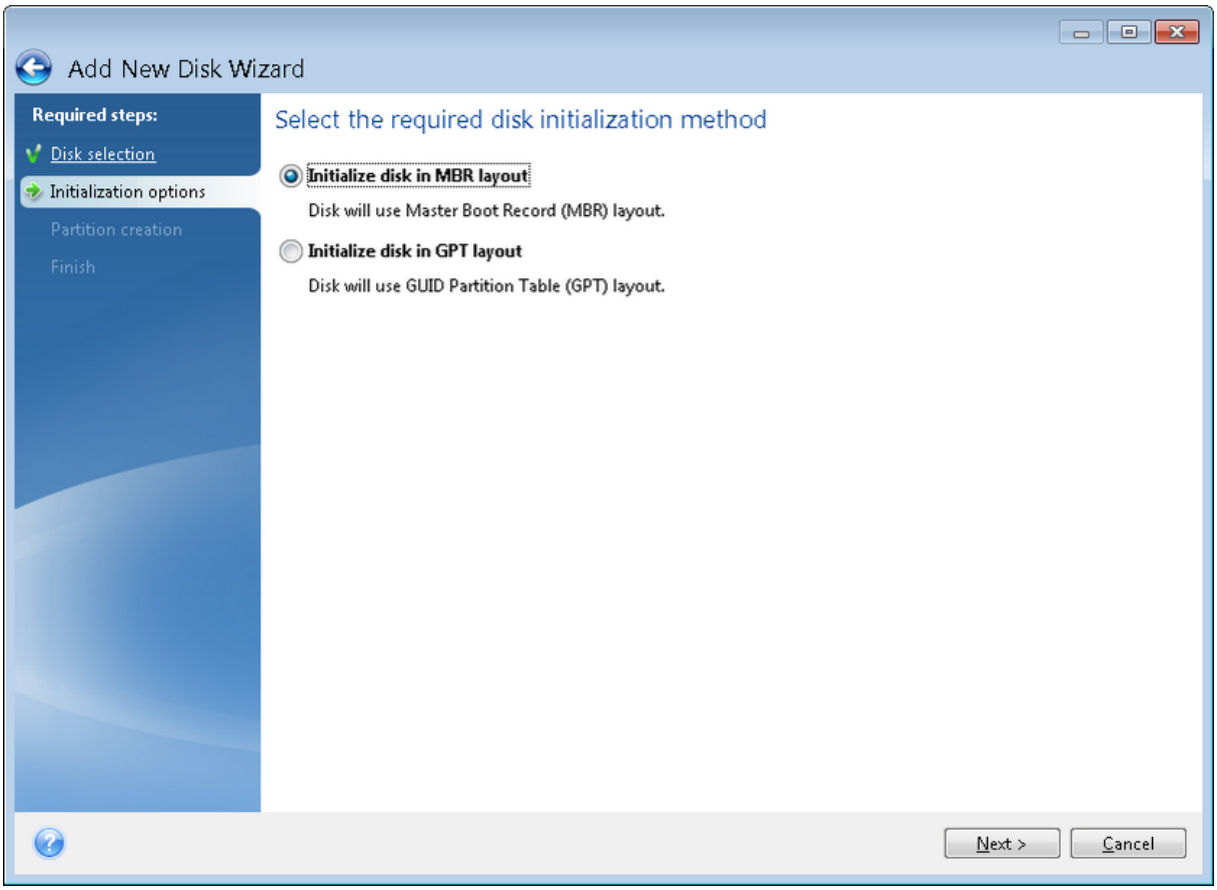
Select the disk that you have added to the computer. If you have added several disks, select one of them and click **Next** to continue. You can add the other disks later by restarting the Add New Disk Wizard.

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




## Selecting initialization method

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




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

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

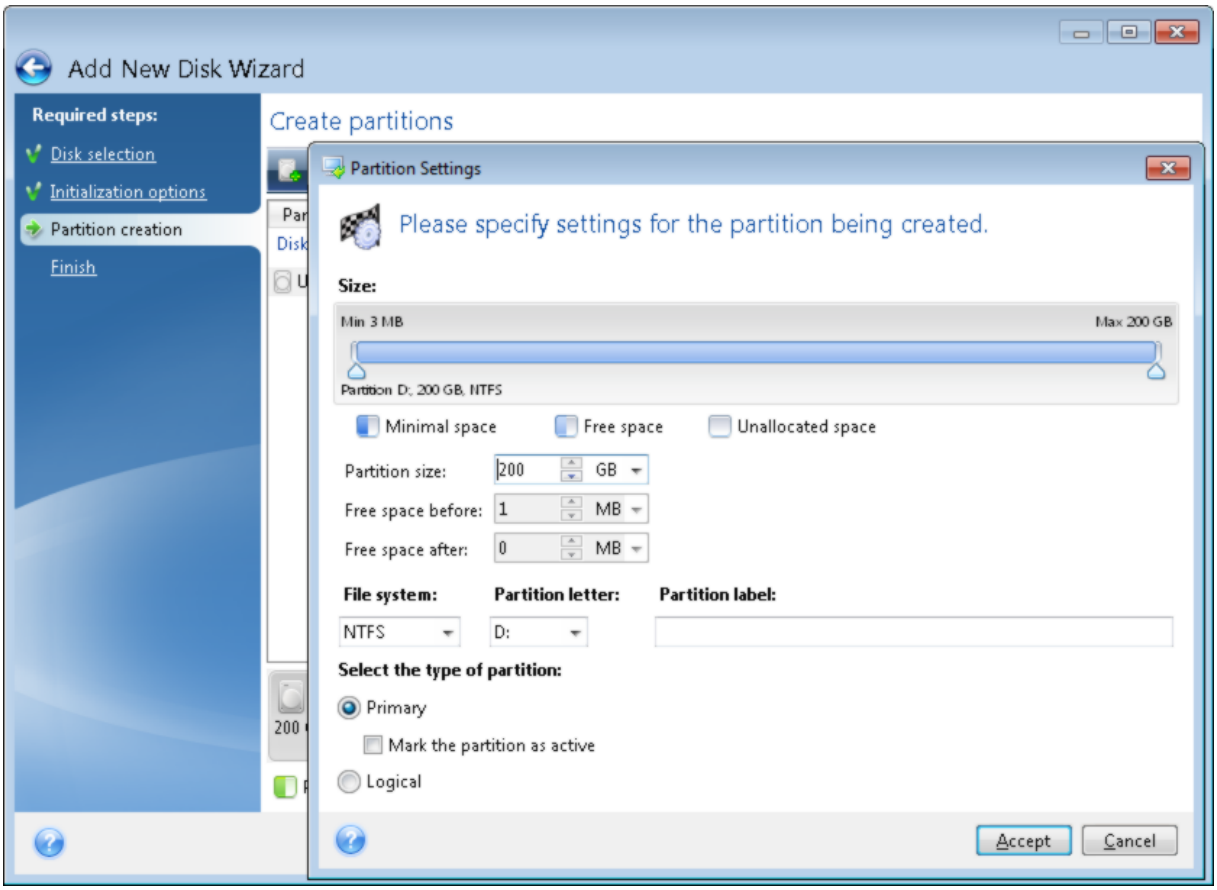
## Creating new partitions

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

   See Partition settings for details.
3. Click **Accept**.




# Partition settings

## Size

***To resize the partition, do 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.

**Note**
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 native file system for Windows NT, Windows 2000, Windows XP, and later operating systems. 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.

# Security and Privacy Tools

## 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. See Algorithm selection 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) > **Acronis DriveCleanser**.
   The Acronis DriveCleanser wizard opens.
2. On the **Source selection** step, select the disks and partitions that you want to wipe. See Source selection for details.
3. On the **Algorithm selection** step, select an algorithm that you want to use for the data destruction. See Algorithm selection for details.
4. [optional step] You can create your own algorithm. See 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. See Post-wiping actions 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**.

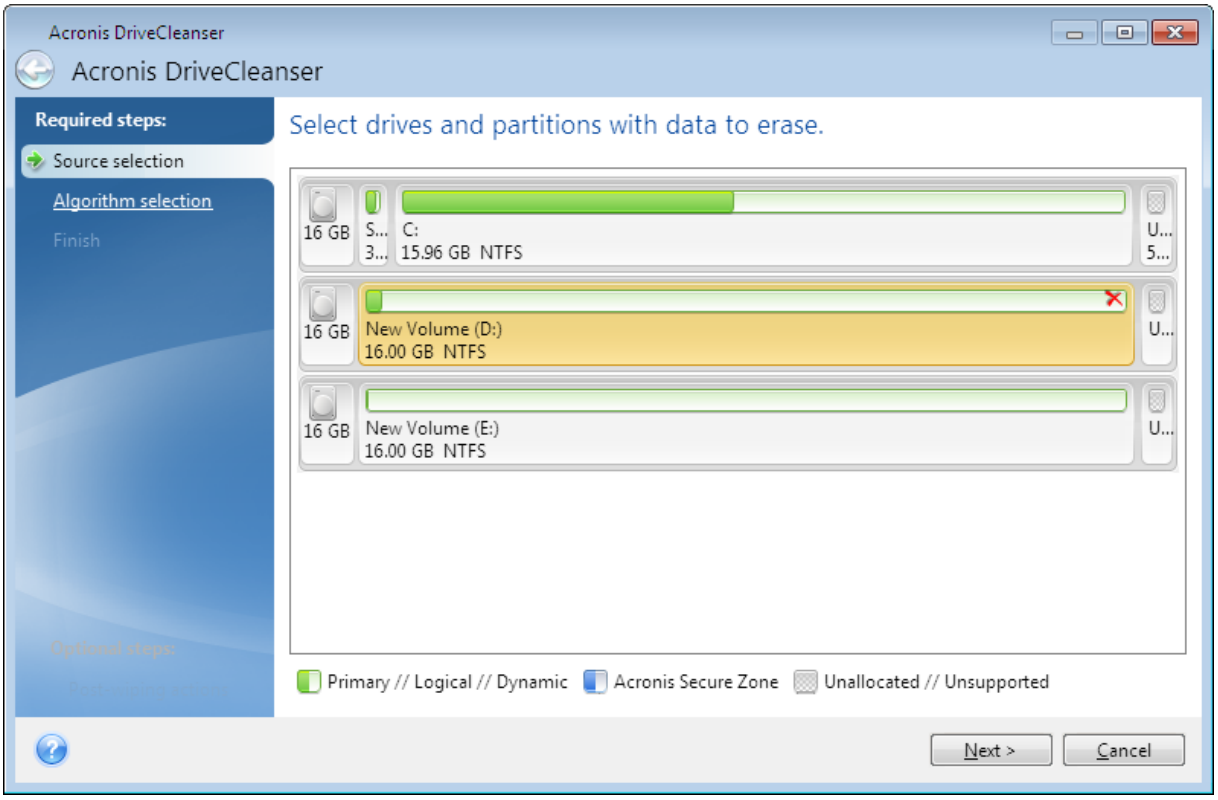
**Warning!**
Be aware that, depending on the total size of selected partitions and the selected data destruction algorithm, the data destruction may take many hours.

### 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 ( ).

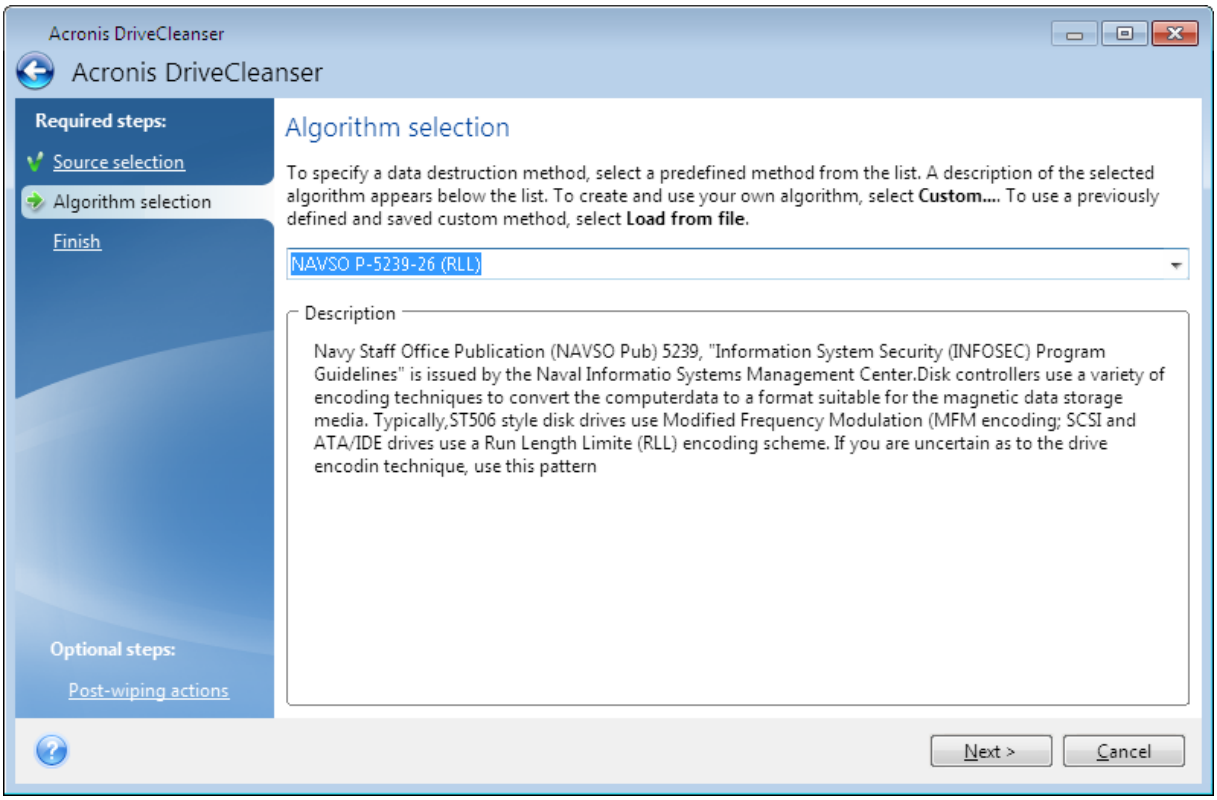



**Note**
Acronis DriveCleanser cannot wipe partitions on dynamic and GPT disks, so they will not be shown.

## Algorithm selection

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

- To use one of the preset algorithms, select the desired algorithm. See Hard Disk Wiping Methods 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.




## Hard Disk Wiping methods

Information removed from a hard disk drive by non-secure means (for example, by simple Windows delete) can easily be recovered. Utilizing specialized equipment, it is possible to recover even repeatedly overwritten information.

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***

The detailed theory of guaranteed information wiping is described in an article by Peter Gutmann. See "Secure Deletion of Data from Magnetic and Solid-State Memory" at https://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html.

| No. | Algorithm (writing method) | Passes | Record |
|---|---|---|---|
| 1. | United States Department of Defense 5220.22-M | 4 | 1 pass – randomly selected symbols to each byte of each sector, 2 – complementary to written during the first pass; 3 – random symbols again; 4 – writing verification. |

| No. | Algorithm (writing method) | Passes | Record |
|---|---|---|---|
| 2. | United States: NAVSO P-5239-26 (RLL) | 4 | 1 pass – 0x01 to all sectors, 2 – 0x27FFFFFF, 3 – random symbol sequences, 4 – verification. |
| 3. | United States: NAVSO P-5239-26 (MFM) | 4 | 1 pass – 0x01 to all sectors, 2 – 0x7FFFFFFF, 3 – random symbol sequences, 4 – verification. |
| 4. | German: VSITR | 7 | Passes 1 – 6 – alternate sequences of: 0x00 and 0xFF; pass 7 – 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 the sixth to fourth security level systems.<br>Randomly selected symbols (numbers) to each byte of each sector for the third to first 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 pass – 0xFF, 2 – 0x00, and then five times with a cryptographically secure pseudo-random sequence. |
| 8. | Fast | 1 | Logical zeros (0x00 numbers) to all sectors to wipe. |

## Creating custom algorithms

### Algorithm definition

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

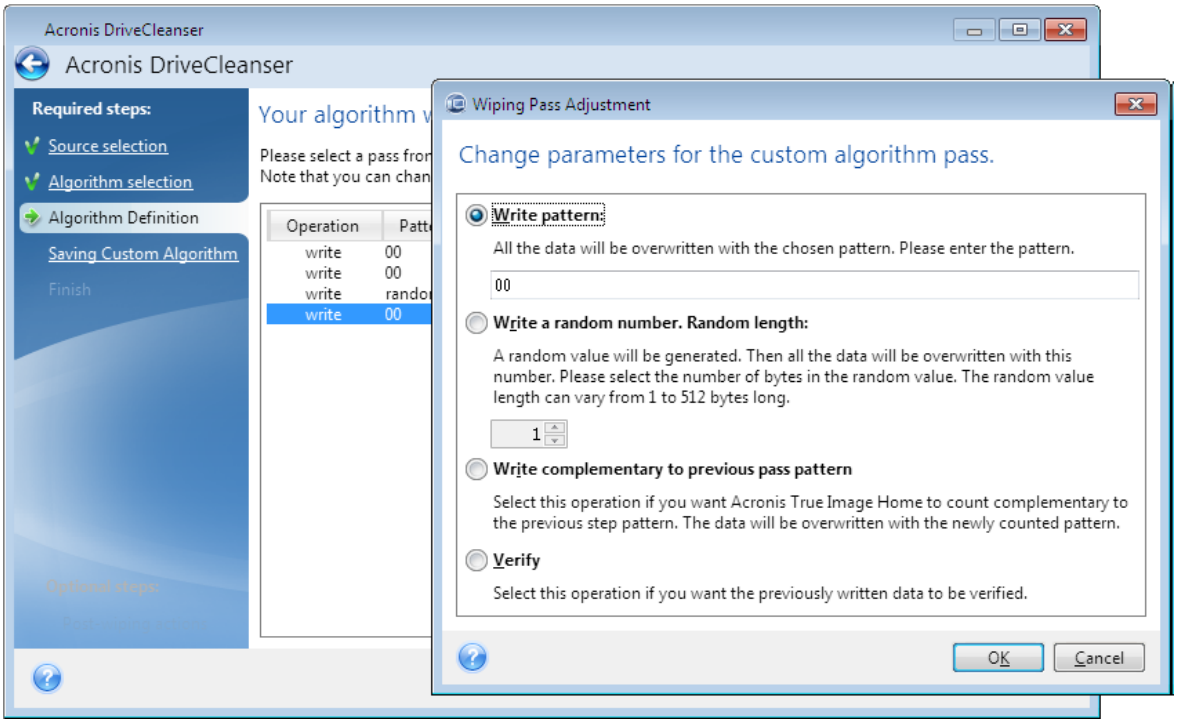
The table has the following legend:

- 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).

     **Note**

     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**

     Acronis True Image for SANDISK adds a complementary value to the one written to disk during the previous pass.
   - **Verify**

     Acronis True Image for SANDISK 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**.

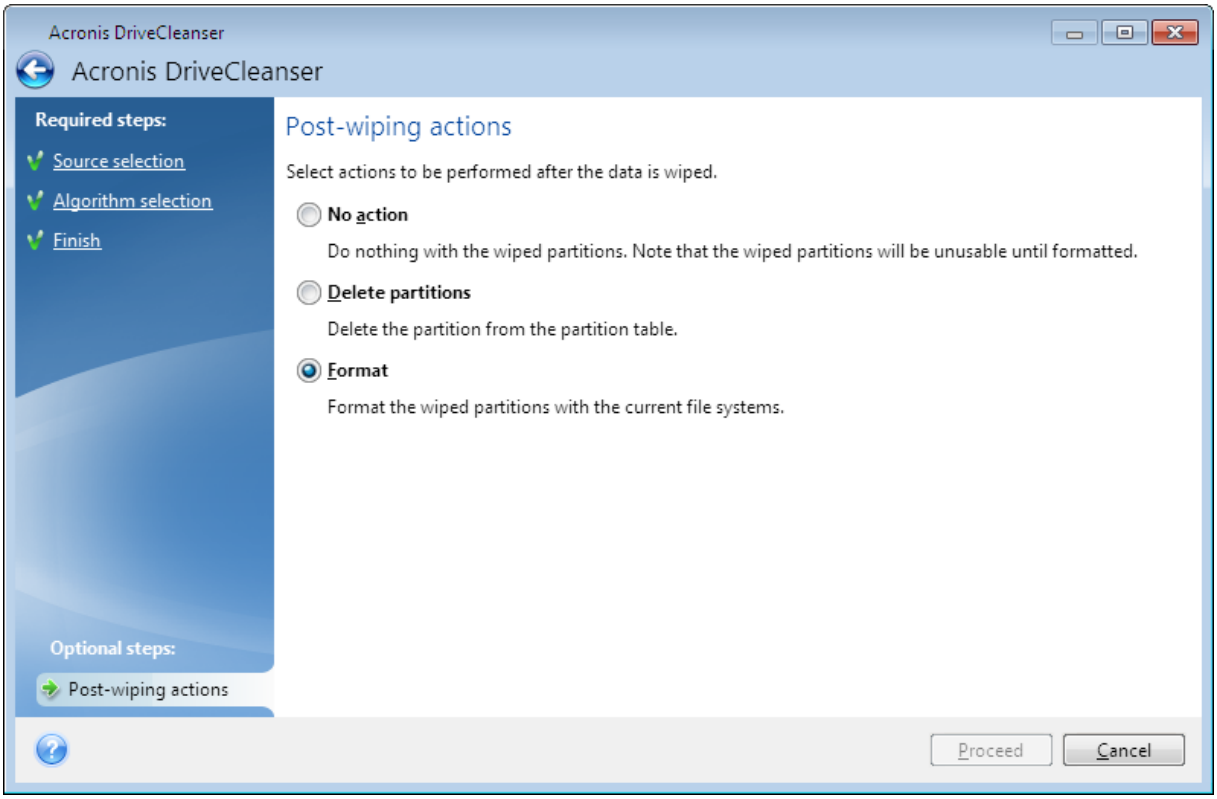
### Saving algorithm to a file

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**.

## 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).




# Mounting a backup image

**Note**
The mounting option is only available for the backups of entire machines, disks, and partitions. It is not available for file and folder backups.

Mounting images as virtual drives lets you access them as though they were physical drives. You can mount local backups that contain partitions or entire disk drives, and then select which partitions to mount. After mounting:

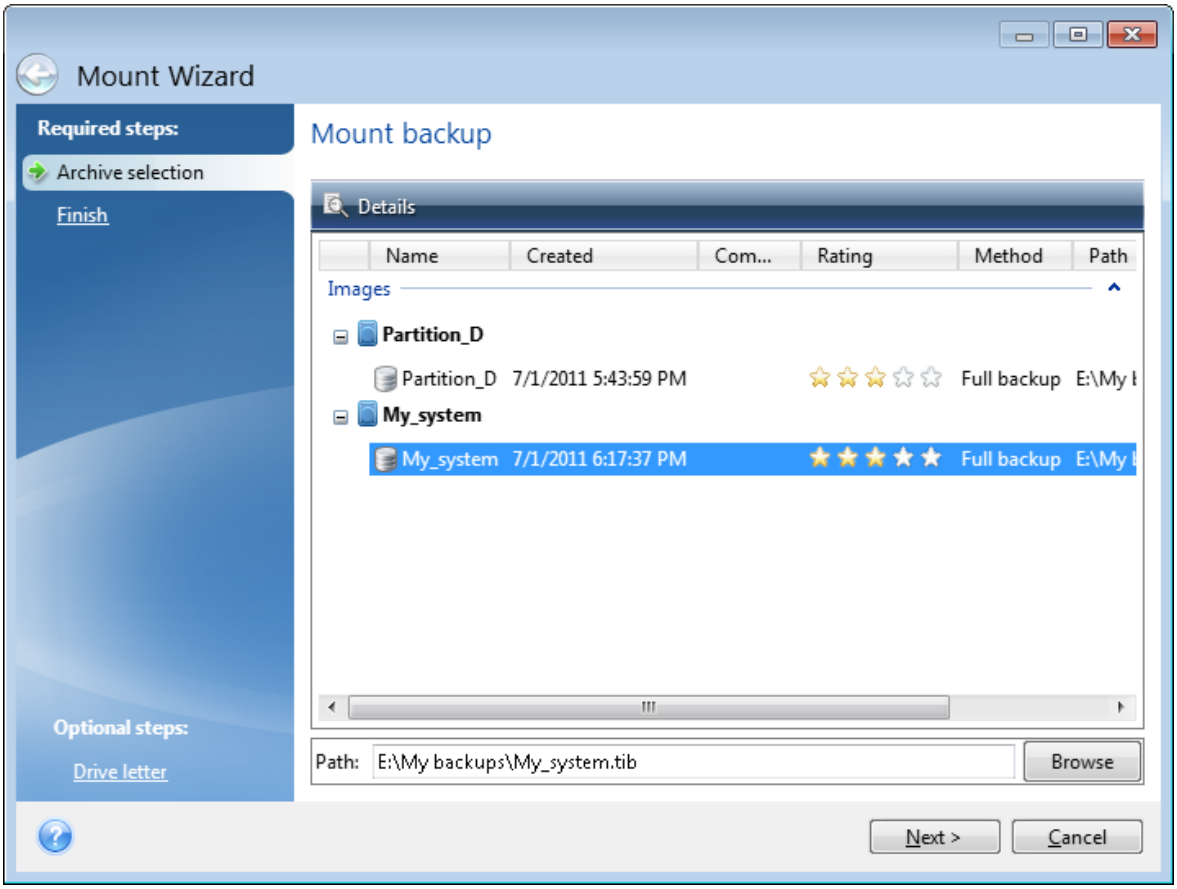
- A new disk appears in your system for every mounted partition.
- You can view the image contents in File Explorer and other file managers in read-only mode.

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

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

## How to mount an image

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




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 File Explorer, showing its contents.

# 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***

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

# Working with .vhd(x) files

Acronis backups (.tibx files) of disks or partitions can be converted to virtual hard disks (.vhd(x) files).

## How to use .vhd(x) files

- You can boot your computer from the converted .vhd(x) file to test whether the backup is valid and can be recovered to a bootable operating system.
- You can keep a converted .vhd(x) file for emergency situations. For example, if your computer cannot start and you need to run it right away, you can boot from the .vhd(x) file.
- In Windows 10 or later, you can mount a .vhd(x) file as an additional drive. The .vhd(x) file may contain any partitions – system or non-system.
- You can run a converted .vhd(x) file as a virtual machine.

## Limitations and additional information

- A file backup cannot be converted to a .vhd(x) file.
- To boot from a converted .vhd(x) file, it must contain:
  - System partition of the same computer. You cannot boot other computers using the same .vhd(x) file.
  - Windows 10 or later operating system.
- Any changes you make to a booted or mounted .vhd(x) file are saved to it. If you boot from a .vhd(x) file and make changes to the data that was not backed up, these changes will affect your live system.
- The standalone versions of Acronis True Image for SANDISK that start when booting from the bootable media do not support conversion operations.
- Acronis True Image for SANDISK cannot convert .tibx files that contain dynamic volumes which were originally located on more than one disk drive (for example, spanned or striped dynamic volumes).

## Converting Acronis backup

Users of the Enterprise and Ultimate editions of Windows 10 and later Windows versions can convert a .tibx image of the system partition into the .vhd(x) format if they want to use the converted .vhd(x) file for booting the operating system. Or, they may want to get the ability to mount images without using Acronis True Image for SANDISK.

***To convert an Acronis disk image (.tibx file) to a Windows backup (.vhd(x) file)***

1. Start Acronis True Image for SANDISK.
2. Go to the **Backup** section.
3. In the backup list, click the down arrow icon next to the backup that you want to convert, and then click **Convert to VHD**.
4. Select the backup version that you want to convert.

   Converting an incremental backup requires all the previous incremental backups and the original full backup. Converting a differential backup requires the original full backup. The result of conversion is always a full backup.
5. Specify the path to the file to be created.

   The file can be directed to any local storage supported by Acronis True Image for SANDISK (except the Acronis Secure Zone and CD/DVD). In addition, it can be directed to an SMB share.
6. [Optional step] While the backup is being converted, you can select the **Start virtual machine after completion** check box. If it is selected, Acronis True Image for SANDISK will restart your computer and run Hyper-V virtual machine by using the created .vhd(x) file.

When a .tibx image selected for conversion contains partitions (for example, from two physical hard disk drives) the program will create two .vhd(x) files corresponding to those physical drives.

# Importing and exporting backup settings

Acronis True Image for SANDISK allows you to import and export the settings of your backups. This may be desirable if you need to transfer the settings to a new PC after installing Acronis True Image for SANDISK on that computer. Saving the settings may also be useful if you later decide to upgrade to the next Acronis True Image for SANDISK version.

Such transfer will make configuring backups on the new PC much easier. You only need to export the settings and then import them to the other PC. The settings are exported in the form of script files.

The settings content can be different depending on a backup type. In case of "classic" disk and file type backups the settings consist of the following items:

- list of items for backup
- backup options
- backup location
- schedule

- backup scheme
- automatic clean-up rules
- backup version naming rules

The settings of Nonstop Backup are as follows:

- list of items for nonstop protection
- Nonstop Backup data storage location (a list of locations, if there are several)

**Note**
You cannot import online backup settings from one computer to another.

***To export the backup settings***

1. Start Acronis True Image for SANDISK.
2. On the sidebar, click **Settings** > **Backup settings transfer**, click **Save settings to file**, and then browse for the destination to save the script files with the settings.

***To import the backup settings***

1. Start Acronis True Image for SANDISK on another computer.
2. On the sidebar, click **Settings** > **Backup settings transfer**, click **Import settings from file**, and then show the path to the script files with the settings.

After importing the settings you may need to change some of them to suit the new environment. For example, it may be necessary to change the list of items for backup, backup destination, etc.

If you want to copy some of your backups to another computer, it is recommended to export the settings of those backups too. Thus you will not lose some of the copied backup's functionality.

# Troubleshooting

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

## Resolving the most frequent issues

Here is the list of the most frequent issues that users encounter in Acronis True Image for SANDISK. You can read the corresponding solutions in the Acronis Support Portal.

- **Signing in at program start fails**
- **Error "You've exceeded the maximum number of activations for this serial number"**
- **Error "This serial number is already registered to another account"**
- **Files and folders are not shown when browsing backups in File Explorer**
- **Error "Plug in external drive"**
- **Blue Screen of Death (BSOD) after recovery to new hardware and error "Stop 0x0000007B" due to missing drivers**

See the full list of popular solutions at https://care.acronis.com/s/support-portal/acronis-true-image-known-solutions.

## Acronis System Report

The **Generate System Report** tool creates a System Report that contains all the necessary technical information and allows you to save the information to a file. When it's necessary, you can attach the created file to your problem description and send it to the 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 sidebar, click **Help**, and then click **Generate System Report**.
- Press **CTRL+F7**. Note that you can use this key combination even when Acronis True Image for SANDISK is performing any other operation.
- If you use Windows 11, click **All apps** > **Acronis** > **Acronis System Report**.
- If you use Windows 10, in the **Start** menu, click **Acronis** > **Acronis System Report**.

***After the report is generated***

- To save the generated System Report, 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 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 for SANDISK. Simply plug in a USB flash drive and click the **Acronis System Report** icon. The generated report will be saved on the USB flash drive.

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

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

**Creating a System Report from the command line prompt**

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

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

3. To create the System Report file, enter:

   ```
   SystemReport
   ```

   The file SystemReport.zip will be created in the current folder.

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

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

***To generate a System Report under bootable media***

1. Create Acronis bootable media, if you do not have it. See Acronis Media Builder for details.
2. Arrange the boot order in BIOS so that your bootable media device (CD, DVDs or USB drive) is the first boot device. See Arranging boot order in BIOS for details.
3. Boot from the Acronis bootable media and select **Acronis True Image for SANDISK**.

   **Note**
   Instead of clicking **Acronis True Image for SANDISK**, you can plug in a USB flash drive and click **Acronis System Report**. In this case, the program generates a report and automatically saves it to the flash drive.

4. Click the arrow next to the Help icon (  ), and then select **Generate System Report**.
5. After the report is generated, click **Save** and in the opened window specify a location for the created file.

   The program will archive the report into a zip file.

# Acronis Smart Error Reporting

When an issue is caused by an error in the program's operation, Acronis True Image for SANDISK displays an appropriate error message. The error message contains an event code and a short description of the error.

## When you have an Internet connection

To view the Acronis Support Portal article suggesting a solution(s) for correcting the error, click the **Knowledge Base** button.

This will open a confirmation window that lists the information to be sent via Internet to the Acronis Support Portal. Click **OK** to permit sending the information.

If in future you would like to send such information without confirmation, select the **Always send without confirmation** check box.

## When you do not have an Internet connection

1. In the error message window, click **More details** and write down the event code. The code may look like this:

   0x000101F6 - example of an ordinary event code.

   0x00970007+0x00970016+0x00970002 - example of a composite event code. A code of this kind may appear when an error occurred in a low-level program module and then propagated to higher-level modules, resulting in errors in those modules as well.
2. When you establish Internet connection or if you can use another computer where Internet connection is available, enter the event code at Acronis Smart Error Reporting.

If the event code is not recognized in the Knowledge Base, the base does not yet contain an article to resolve the issue. In such cases, open a trouble ticket with Acronis Customer Center.

# How to collect crash dumps

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

***If Acronis True Image for SANDISK crashes, please provide the following information***

1. A description of the exact sequence of steps performed before you encountered the issue.
2. A crash dump. For information on how to collect such a dump, see Creating process dumps with ProcDump.

***If Acronis True Image for SANDISK causes a Windows crash***

1. A description of the exact sequence of steps performed before you encountered the issue.
2. A Windows dump file. For information on how to collect such a dump, see Creating Windows Memory Dumps.

***If Acronis True Image for SANDISK hangs***

1. A description of the exact sequence of steps performed before you encountered the issue.
2. A userdump of the process. See Creating a Userdump.
3. The Procmon log. See Collecting Process Monitor log.

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

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

# Index

**I**



**L**



**M**



**N**



**O**



**P**

**R**



**S**



**T**



**U**



**V**

**W**