

Acronis

[acronis.com](https://www.acronis.com)

Acronis True Image for Kingston

Table of contents

| | |
|---|-----------|
| Introduction | 7 |
| What is Acronis True Image for Kingston? | 7 |
| System requirements and supported media | 7 |
| Minimum system requirements | 7 |
| Supported operating systems | 8 |
| Supported file systems | 8 |
| Supported storage media | 9 |
| Installing and uninstalling Acronis True Image for Kingston | 9 |
| Upgrading Acronis True Image for Kingston | 10 |
| Built-in store | 10 |
| Acronis True Image advanced features | 10 |
| Technical Support | 12 |
| Getting started | 13 |
| User interface language | 13 |
| Protecting your system | 13 |
| Backing up your computer | 13 |
| Creating Acronis bootable media | 14 |
| Backing up all data on your PC | 15 |
| Cloning your hard drive | 15 |
| Why do I need it? | 15 |
| Before you start | 16 |
| Cloning a disk | 16 |
| Recovering your computer | 17 |
| Two-factor authentication (2FA) | 18 |
| Basic concepts | 21 |
| The difference between file backups and disk/partition images | 22 |
| Full backup | 23 |
| Deciding where to store your backups | 23 |
| Preparing a new disk for backup | 24 |
| FTP connection | 24 |
| Authentication settings | 25 |
| Backup file naming | 25 |
| Wizards | 26 |
| FAQ about backup, recovery and cloning | 27 |
| Backing up data | 29 |

| | |
|---|-----------|
| Backing up disks and partitions | 29 |
| Backup options | 30 |
| Backup schemes | 30 |
| Notifications for backup operation | 32 |
| Image creation mode | 34 |
| Pre/Post commands for backup | 34 |
| Backup splitting | 35 |
| Backup validation option | 36 |
| Backup reserve copy | 36 |
| Error handling | 37 |
| Computer shutdown | 38 |
| Performance of backup operation | 38 |
| Laptop power settings | 40 |
| Operations with backups | 41 |
| Backup operations menu | 41 |
| Backup activity and statistics | 41 |
| Sorting backups in the list | 43 |
| Validating backups | 44 |
| Backup to various places | 44 |
| Adding an existing backup to the list | 45 |
| Deleting backups | 45 |
| Cleaning up backups and backup versions | 46 |
| Recovering data | 48 |
| Recovering disks and partitions | 48 |
| Recovering your system after a crash | 48 |
| Recovering partitions and disks | 58 |
| About recovery of dynamic/GPT disks and volumes | 60 |
| Arranging boot order in BIOS or UEFI BIOS | 63 |
| Recovering files and folders | 64 |
| Searching backup content | 65 |
| Recovery options | 66 |
| Disk recovery mode | 66 |
| Pre/Post commands for recovery | 66 |
| Validation option | 67 |
| Computer restart | 67 |
| File recovery options | 67 |
| Overwrite file options | 68 |

| | |
|---|------------|
| Performance of recovery operation | 68 |
| Notifications for recovery operation | 69 |
| Protection | 71 |
| The Protection dashboard | 71 |
| Active protection | 71 |
| Anti-ransomware protection | 71 |
| Configuring Active Protection | 72 |
| Managing files in Quarantine | 73 |
| Configuring Protection exclusions | 73 |
| Tools | 75 |
| Acronis Media Builder | 75 |
| Creating Acronis bootable media | 75 |
| Acronis bootable media startup parameters | 76 |
| Making sure that your bootable media can be used when needed | 78 |
| Selecting video mode when booting from the bootable media | 81 |
| Adding a new hard disk | 82 |
| Selecting a hard disk | 83 |
| Selecting initialization method | 83 |
| Creating new partitions | 84 |
| Security and Privacy Tools | 87 |
| Acronis DriveCleanser | 87 |
| Mounting a backup image | 92 |
| How to mount an image | 93 |
| Unmounting an image | 94 |
| Disk cloning and migration | 95 |
| Disk cloning utility | 95 |
| Clone Disk wizard | 95 |
| Manual partitioning | 97 |
| Excluding items from cloning | 98 |
| Migrating your system from an HDD to an SSD | 100 |
| SSD size | 100 |
| Which migration method to choose | 100 |
| What to do if Acronis True Image for Kingston does not recognize your SSD | 100 |
| Migrating to SSD using the backup and recovery method | 101 |
| Troubleshooting | 103 |
| Resolving the most frequent issues | 103 |
| Acronis System Report | 103 |

| | |
|----------------------------------|------------|
| How to collect crash dumps | 105 |
| Glossary | 106 |
| Index | 109 |

Copyright statement

© Acronis International GmbH, 2003-2023. All rights reserved.

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

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

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

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

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

Acronis patented technologies

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

Introduction

What is Acronis True Image for Kingston?

Acronis True Image for Kingston is a complete cyber protection solution that ensures the security of all your information. It can back up your documents, photos, emails, 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 and security features.

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:

- [Acronis bootable media](#)
- [Hard disk cloning](#)
- [Security and privacy tools](#)

Learn how to protect your computer: "[Protecting your system](#)".

System requirements and supported media

Minimum system requirements

Acronis True Image for Kingston requires the following hardware.

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

Warning!

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

Other requirements

- An internet connection is required for the product activation and for downloading protection updates.
- You need to have administrator privileges to run Acronis True Image for Kingston.

Supported operating systems

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

- Windows 11
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7 SP1 (all editions)
- Windows Home Server 2011

Note

- Beta builds are not supported. See <https://kb.acronis.com/content/60589>.
- Windows Embedded, IoT editions, Windows 10 LTSC, Windows 10 LTSC, and Windows 10 in S mode are not supported.
- To use Acronis True Image for Kingston on Windows 7, Windows 8, and Windows 8.1, you will need the following security updates from Microsoft: KB4474419 and KB4490628. See <https://kb.acronis.com/content/69302>.

Acronis True Image for Kingston 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 SWAP²
- HFS+/HFSX³
- FAT16/32/exFAT⁴

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

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

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

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

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

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)
- FTP servers

Note

The FTP server must allow passive mode file transfers. Acronis True Image for Kingston 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 1.1 / 2.0 / 3.0, USB-C, eSATA, FireWire (IEEE-1394), SCSI, and PC card storage devices

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 Kingston

To install Acronis True Image for Kingston

1. Run the setup file.
2. Select the installation mode:
 - Click **Install** for the default installation.Acronis True Image for Kingston 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 Kingston and Bonjour.
Bonjour software will be installed on your computer for advanced support of NAS devices. You can uninstall the software at any time.

To uninstall Acronis True Image for Kingston completely

- If you use Windows 11, click **Start > Settings > Apps > Acronis True Image for Kingston > Uninstall**.

- If you use Windows 10, click **Start > Settings > Apps > Acronis True Image for Kingston > Uninstall**.
- If you use Windows 8, click the **Settings** icon, then select **Control Panel > Uninstall a program > Acronis True Image for Kingston > Uninstall**.
- If you use Windows 7, click **Start > Control Panel > Uninstall a program > Acronis True Image for Kingston > Uninstall**.

Then follow the instructions on the screen. You may have to restart your computer afterwards to complete the task.

Upgrading Acronis True Image for Kingston

You can upgrade Acronis True Image for Kingston to Acronis Cyber Protect Home Office.

Your backups created with a previous version of Acronis True Image for Kingston are completely compatible with the newer version of Acronis Cyber Protect Home Office. 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 Kingston.
2. On the sidebar, click **Account**, and then click **Upgrade**. The built-in store opens.
3. Select the license that you want to buy, and then click **Buy now**.
4. Provide your payment information.

Built-in store

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

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

Acronis True Image advanced features

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

- **Online Backup**
Online Backup allows you to store your files and disks on Acronis Cloud. Your data will be protected even if your computer is lost, stolen, or destroyed, and your data can be entirely recovered onto a new device, if needed.
- **File backup**
Instead of backing up entire partitions and disks, you can back up specific files and folders, both to a local storage and Acronis Cloud.

- **Cloud archiving**
Data archiving is a tool that allows you to move your big or rarely used files to Acronis Cloud. Every time you run this tool, it analyzes the data in the selected folder and suggests uploading the found files to Acronis Cloud. You can select the files and folders that you want to archive. After uploading, the local copies of these files will be deleted. Afterwards, when you need to open or change an archived file, you can download it back to your local storage device or access and manage it right in Acronis Cloud.
- **Local archiving**
When you archive your old, large, or rarely used files, Acronis Cloud is not the only possible destination. You can also select local storage, including NAS, an external hard drive, or a USB flash drive. Your local archives are placed into Acronis Archive, which can be accessed in File Explorer under Favorites, along with your cloud archive.
- **Family data protection**
Family data protection is a unified cross-platform solution that allows you to track and control the protection status of all computers, smartphones, and tablets sharing the same Acronis account. Since users of these devices must be signed in to the same account, usually they are members of the same family. In general, each of them can use this feature, but there is often a family member who is more experienced in technology than the others. So, it's reasonable to make that person responsible for protection of the family data. To track and control the protection status of your family's devices, use the web-based Online Dashboard, which is accessible from any computer connected to the Internet.
- **Data synchronization**
You can have the same data - documents, photos, videos, etc. - on all of your computers. Your data is within easy reach anywhere and anytime. No more emailing files to yourself or carrying an USB drive all the time.
You can create as many syncs as you need and store your synced files and versions of those files on Acronis Cloud. This lets you roll back to a previous file version whenever you need it. You can also access the Cloud using a web browser, without having to install the application.
- **Acronis Survival Kit**
To recover your computer in case of a failure, you need to have two crucial components—a backup of your system disk and Acronis bootable media. Acronis Survival Kit is an external hard disk drive that contains both components so that you could have a single device that has everything that you need to recover your computer.
- **Acronis Universal Restore**
Acronis Universal Restore allows you to create a bootable system clone on different hardware. Use this utility when recovering your system disk to a computer with a dissimilar processor, different motherboard or a different mass storage device than in the system you originally backed up. This may be useful, for example, after replacing a failed motherboard or when deciding to migrate the system from one computer to another.
- **Acronis Mobile**
Acronis Mobile allows you to back up your mobile data to Acronis Cloud or local storage, and then recover it in case of loss or corruption. You can install Acronis Mobile on any mobile devices that

runs either iOS (iPhone, iPad, iPod) or the Android (mobile phones and tablets) operating systems.

- Try&Decide

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

- Acronis Secure Zone

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

- System Clean-up

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

See the full feature list at <https://acronis.com/promotion/b-oem-ssd/>.

Technical Support

If you need assistance with Acronis True Image for Kingston, refer to the official support resources of your vendor.

Getting started

User interface language

Before you start, select a preferred language for the Acronis True Image for Kingston 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 Kingston.
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 Kingston 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. Refer to [Backing up disks and partitions](#) for details.

To back up your computer

1. Start Acronis True Image for Kingston.
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**.

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 Kingston 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 Kingston.
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.
Refer to [Arranging boot order in BIOS](#) for details.
3. Boot your computer from the bootable media and select **Acronis True Image for Kingston**.
Once Acronis True Image for Kingston is loaded, you can use it to recover your computer.

Refer to [Acronis Media Builder](#) for details.

Backing up all data on your PC

What is an Entire PC backup?

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

When you select Entire PC as a backup type, Acronis True Image for Kingston 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 Kingston recovers all data from the backup to the original location. Note that you cannot select specific disks or partitions to recover and you cannot change the default destination. If you need to avoid these limitations, we recommend that you back up your data with an ordinary disk-level backup method. Refer to [Backing up disks and partitions](#) for details.

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

To create an Entire PC backup

1. Start Acronis True Image for Kingston.
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**.

Cloning your hard drive

Why do I need it?

When you see that the free space on your hard drive is not enough for your data, you might want to buy a new, larger hard drive and transfer all your data to the new drive. The usual copy operation does not make your new hard drive identical to the old one. For example, if you open 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.

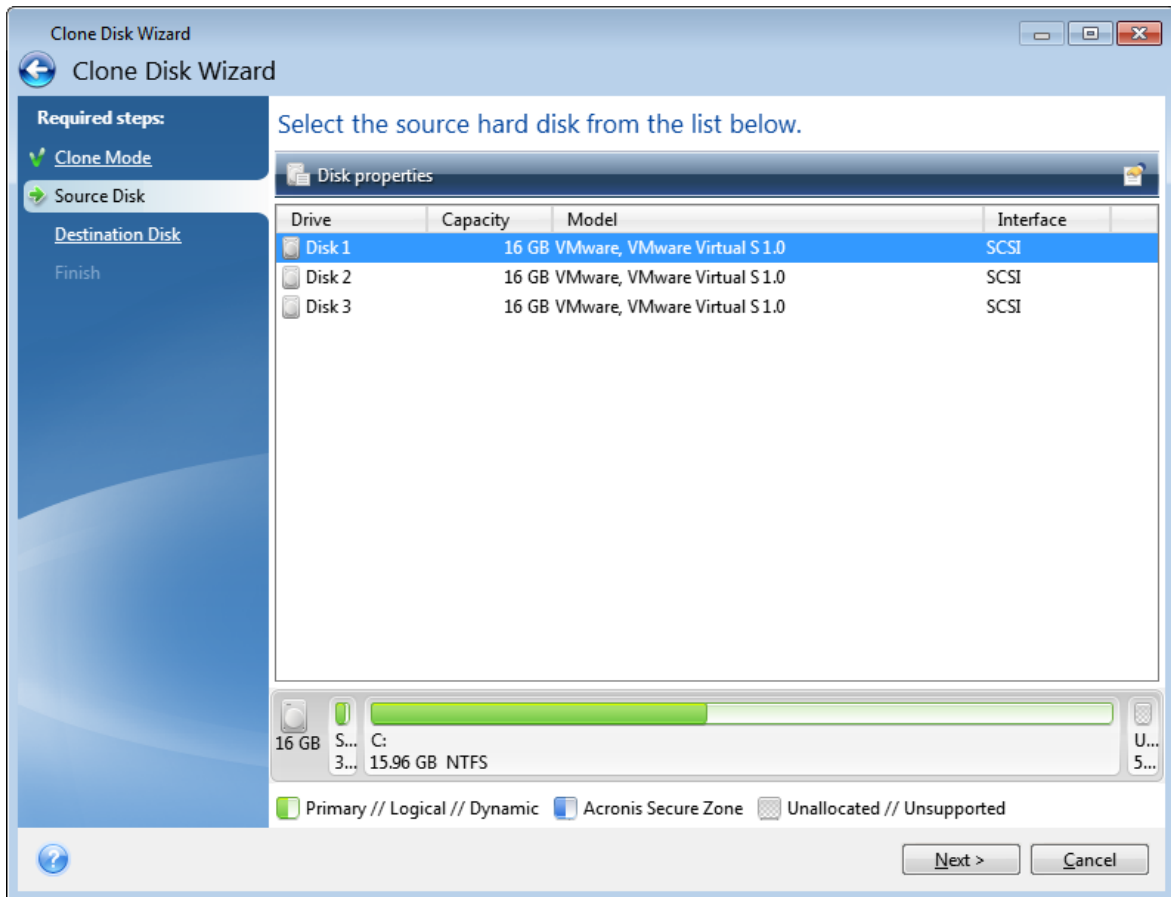
Cloning a disk

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. Refer to [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 Kingston 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 Kingston.
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 Kingston.
2. On the sidebar, click **Backup**.
3. From the backup list, select the backup that contains your system disk.
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 Kingston 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 Kingston.
Refer to [Step 2 Creating Acronis bootable media](#) and [Arranging boot order in BIOS](#) for details.
2. On the Welcome screen, select **My disks** below **Recover**.
3. Select the system disk backup to be used for recovery. Right-click the backup and choose **Recover**.
When the backup is not displayed, click **Browse** and manually specify the path to the backup.
4. At the **Recovery method** step, select **Recover whole disks and partitions**.
5. Select the system partition (usually C) on the **What to recover** screen. Note that you may distinguish the system partition by the Pri, Act flags. Select the System Reserved partition (if any), as well.
6. You may leave all settings of the partitions without changes and click **Finish**.
7. Check the summary of operations, and then click **Proceed**.
8. When the operation finishes, exit the standalone version of Acronis True Image for Kingston, 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.

Two-factor authentication (2FA)

When the two-factor authentication is set up, you are required to enter your password (the first factor) and a one-time password (the second factor) to log in to the Online Dashboard. The one-time code is generated by an authenticator app that must be installed on your mobile phone or another device that belongs to you. Even if someone finds out your login and password, they still will not be able to log in without access to your second-factor device.

Prerequisites

Before enabling 2FA, make sure you installed a compatible version. 2FA is compatible with the following versions:

- Acronis True Image for Kingston build 40561 and later.

To see the build number:

In the left sidebar, click **Help**, and then select the **About** option.

- Acronis Mobile for Android app version 6.2
- Acronis Mobile for iOS app version 6.2

To set up two-factor authentication for your account

1. Open Online Dashboard at: <https://cloud.acronis.com>.
2. Click on the **Account** tab. The **Two-factor authentication (2FA)** section is displayed in the **Account** window.
3. Use the toggle to enable two-factor authentication for your account. The **Set up two-factor authentication (2FA)** window is displayed.
4. Install an authenticator app on your mobile device.
Examples of authenticator apps:
 - Twilio Authy
 - Microsoft Authenticator
 - Google Authenticator
5. Scan the QR code by using your authenticator app, and then enter the 6-digit code displayed on the authenticator app in the **Set up two-factor authentication (2FA)** window.
6. Click **Next**. The instructions are displayed for restoring access to your account if you lose your 2FA device or uninstall the authenticator app.
7. Save or print the PDF file.

Note

Make sure to save it in a safe place or print it for further reference. This is the best way to restore your access.

To make sure you will be able to restore your 2FA

- Save or print the PDF file containing an alpha-numeric code that can be used as a replacement of the QR code.
- Make backup of authenticator account if the mobile app supports it.
- Use a mobile app that supports accounts.

To restore two-factor authentication on a new device (2FA)

If you have access to the previously set-up mobile authentication app:

1. Install an authenticator app on your new device.
2. Use the PDF file that you saved when you set up 2FA on your device. This file contains the 32-digit code that you need to enter in the authenticator app to link the authenticator app again to your Acronis account.

Important

If the code is correct but it is not working, ensure that the time in the authenticator mobile app it is synced with your device.

3. If you missed saving the PDF file during the setup:
 - a. Click **Reset 2FA**, and then enter the one-time password shown in the mobile authenticator app.
 - b. Follow the on-screen instructions.

If you have no access to previously set-up mobile authenticator app:

Variation 1: Use the stored PDF file to link a new device. The default name of the file is cyberprotect-2fa-backupcode.pdf.

Variation 2: Restore access to your account from backup. Ensure that backups are supported by your mobile app.

Variation 3: Open the app under the same account from another mobile device if it's supported by the app.

Basic concepts

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

Note

Certain features and functionalities may be unavailable in the edition that you use.

Backup and recovery

Backup refers to the making copies of data so that these additional copies may be used to **recover** the original after a data loss event.

Backups are useful primarily for two purposes:

- To recover an operating system when it is corrupted or cannot start (called disaster recovery). Refer to [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 Kingston does both by creating disk (or partition) images and file-level backups respectively.

Backup versions

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

Acronis True Image for Kingston 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 Kingston 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 Kingston only stores the hard disk sectors that contain data.

Acronis True Image for Kingston 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 Kingston copies all hard disk sectors, and not only those that contain data.

Full backup

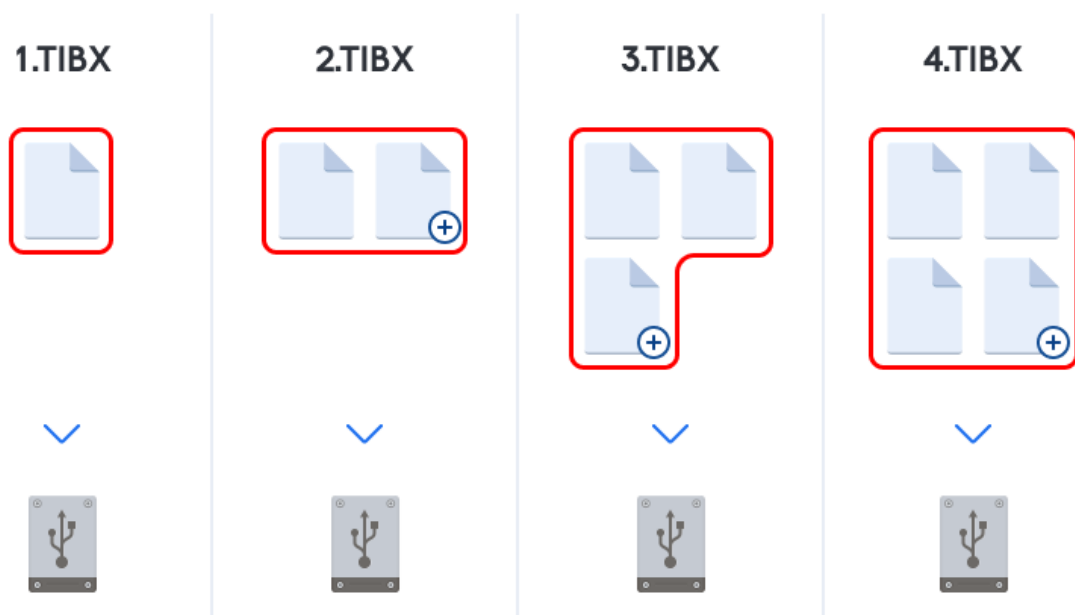
Note

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

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 Kingston 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.

Deciding where to store your backups

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

Preparing a new disk for backup

A new internal or external hard drive may not be recognized by Acronis True Image for Kingston. 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.

FTP connection

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

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

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

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

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

Note

The mere opening of an FTP server's root folder does not bring you to your home directory.

Note

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

Note

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

Note

An FTP server must allow passive mode file transfers.

Note

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

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

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

Backup file naming

A TIB backup file name has the following attributes:

- Backup name
- Backup method (full, inc, diff: full, incremental, differential)

- Number of backup chain¹ (in the form of b#)
- Number of backup version² (in the form of s#)
- Number of volume (in the form of v#)

For example this attribute changes when you split a backup into several files. Refer to [Backup splitting](#) 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.

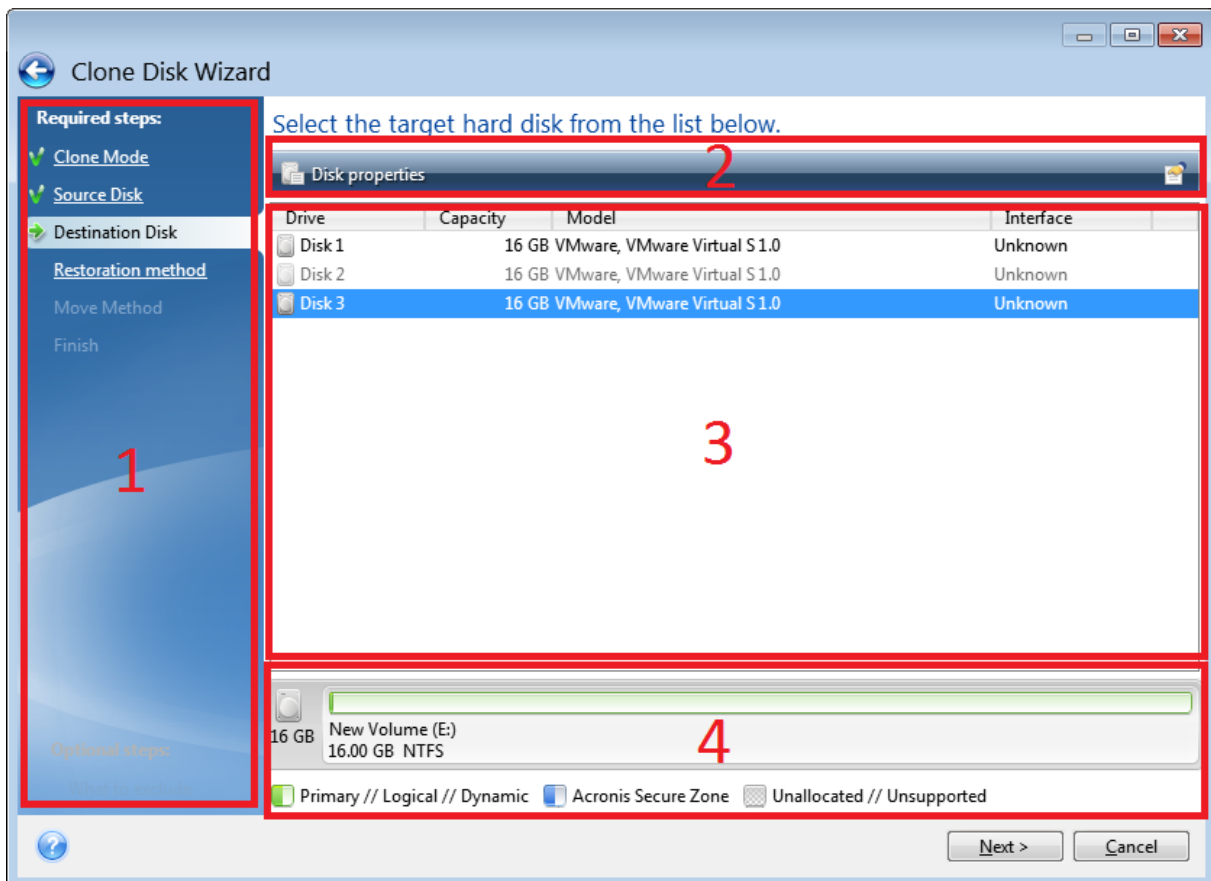
Wizards

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

For example, see the screenshot below.

¹Sequence 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).

²The 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 Kingston have a .tibx extension. The TIBX files resulting from consolidation of backup versions are also called backup versions.



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 Kingston include in a backup?**—By default, Acronis True

Image for Kingston 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 Kingston?**—Yes, Acronis True Image for Kingston 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 Kingston support RAID?**—Acronis True Image for Kingston 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

Note

Certain features and functionalities may be unavailable in the edition that you use.

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

To back up partitions or disks

1. Start Acronis True Image for Kingston.
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**.

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:
 - **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 Kingston 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.

8. [optional step] Click **Options** to set the options for the backup. For more information see [Backup options](#).
9. [optional step] 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**.

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**.

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>.

Backup schemes

Note

Certain features and functionalities may be unavailable in the edition that you use.

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:

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

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

- **Single version scheme**—Select this scheme if you want to use the smallest backup storage.
- **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 Kingston 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

The program creates a full backup version and overwrites it every time 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!

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

Required storage space: minimal.

Custom schemes

With Acronis True Image for Kingston 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 backup method. To do this, under **Backup method**, select **Full**.

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.
 - **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.

Notifications for backup operation

Location: **Options > Notifications**

Sometimes a backup or recovery procedure can last an hour or longer. Acronis True Image for Kingston 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 Kingston 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 Kingston 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 Kingston. 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.

Pre/Post commands for backup

Location: **Options > Advanced > Pre/Post commands**

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

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

To specify commands (batch files)

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

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

Edit user command for backup

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

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

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

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

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

Backup splitting

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

Note

Acronis True Image for Kingston 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 Kingston will act as follows.

When backing up to a hard disk:

- If the selected disk has enough space and its file system allows the estimated file size, the program will create a single backup file.
- If the storage disk has enough space, but its file system does not allow the estimated file size, the program will automatically split the image into several files.

- If you do not have enough space to store the image on your hard disk, the program will warn you and wait for your decision as to how you plan to fix the problem. You can try to free some additional space and continue or select another disk.

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

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

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

Note

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

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**

Backup reserve copy

Location: **Options > Advanced > Backup reserve copy**

Backup reserve copy is an independent full backup version created immediately after a normal backup. Even when you create an incremental or differential backup version containing only data changes, the reserve copy will contain all the data selected for the normal backup. You can save reserve copies of your backups on the file system, a network drive, or a USB flash drive.

Note

CD/DVDs are not supported as locations for reserve copies.

To make a reserve copy

1. Select the **Create a reserve copy of my backups** check box.
2. Specify a location for the backup copies.
3. Select the reserve copy format. You can create it as an Acronis backup (.tibx files) or just copy the source files to the selected location as is, without any modification.
4. [Optional step] Protect the reserve copy with a password.
All other backup options will be inherited from the source backup.

Error handling

When Acronis True Image for Kingston 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 Kingston 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.

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 Kingston 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 Kingston automatically stops all its current operations before shutdown. This may take about two minutes. The next time you run Acronis True Image for Kingston, 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:

- **None**—The data will be copied without any compression, which may significantly increase the backup file size.
- **Normal**—The recommended data compression level (set by default).
- **High**—Higher backup file compression level, takes more time to create a backup.
- **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 the equal priority with other processes.
- **High**—The backup or recovery process will run faster, but the performance of other programs will be reduced. Be aware that selecting this option may result in 100% CPU usage by Acronis True Image for Kingston.

Network connection transfer rate

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

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

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

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 Kingston 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 Kingston 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 Kingston.
- **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 menu

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

The backup operations menu can contain the following items:

- **Rename** (not available for backups to Acronis Cloud)—Set a new name for a backup in the list. The backup files will not be renamed.
- **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.
- **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.

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

To view a 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**.

| | | | | |
|---|--|----------------|-----------------|--------|
|  | Successfully backed up today at 12:04 PM | | | |
| Backed up | Speed | Time spent | Data to recover | Method |
| 1.6 GB | 180.4 Mbps | 2 mins 28 secs | 1.6 GB | Full |

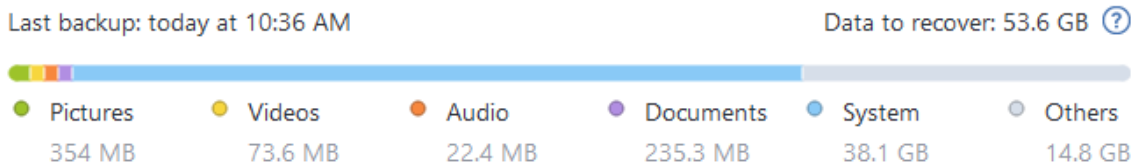
What you can view and analyze:

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

For more information, refer to the Knowledge Base article: <https://kb.acronis.com/content/60104>.

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. To reverse the order, select Z → A . |
| | Date created | This command sorts all backups from newest to oldest. 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. To reverse the order, select Least recent on top . |
| | Size | This command sorts all backups by size, from biggest to smallest. 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 Kingston, 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 Kingston (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 Kingston 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.

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 Kingston 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 Kingston.

Acronis True Image for Kingston 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 Kingston

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 Kingston. 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 Kingston, the backup files remain in their current location and you will be able to add the existing backup to Acronis True Image for Kingston 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 Kingston. If you want to delete backup files that you see locally, but not in Acronis True Image for Kingston, try adding this existing backup to Acronis True Image for Kingston. After that, you can completely delete this backup and its files by using Acronis True Image for Kingston.

To delete an entire backup by using Acronis Cloud

1. On the **Backups** tab, click the size of the backup that you want to delete. Then, the detailed view will appear.

2. Click **Delete** in the detailed view.

Note

The backup will be deleted from Acronis Cloud, but all of its settings and schedule will remain in the Acronis True Image for Kingston application.

See also

"Cleaning up backups and backup versions" (p. 46)

Cleaning up backups and backup versions

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 Kingston, 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, or Acronis Secure Zone.
- Nonstop backups.

To clean up backup versions locally in Acronis True Image for Kingston

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 chain¹. 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 version² - 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.

¹Sequence 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).

²A 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.

However, if the chain is made up of only full versions, any of them can be deleted independently.

- When you select a differential version - it can be deleted independently.
- When you select an incremental version - the program also selects all dependent incremental versions within the backup version chain¹.

See also

[Full, incremental and differential backups](#)

"Deleting backups" (p. 45)

¹Sequence 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).

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. Refer to [Recovering your system](#) for details.

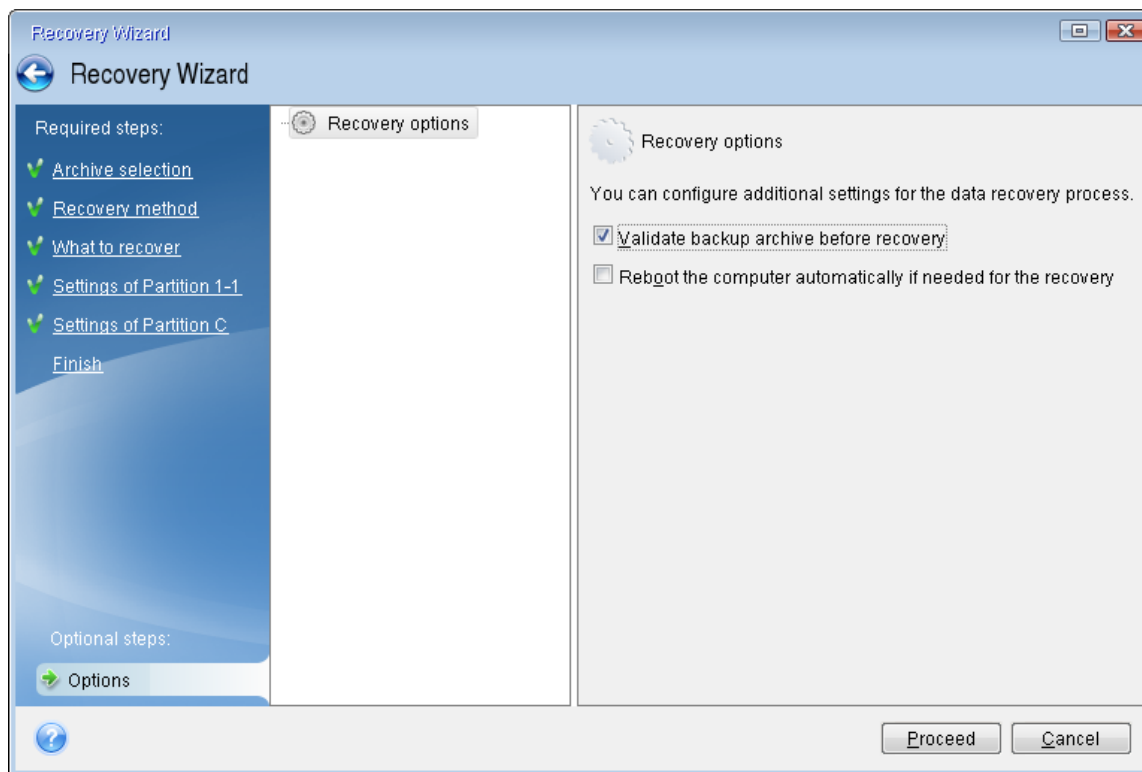
Preparing for recovery

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](#).

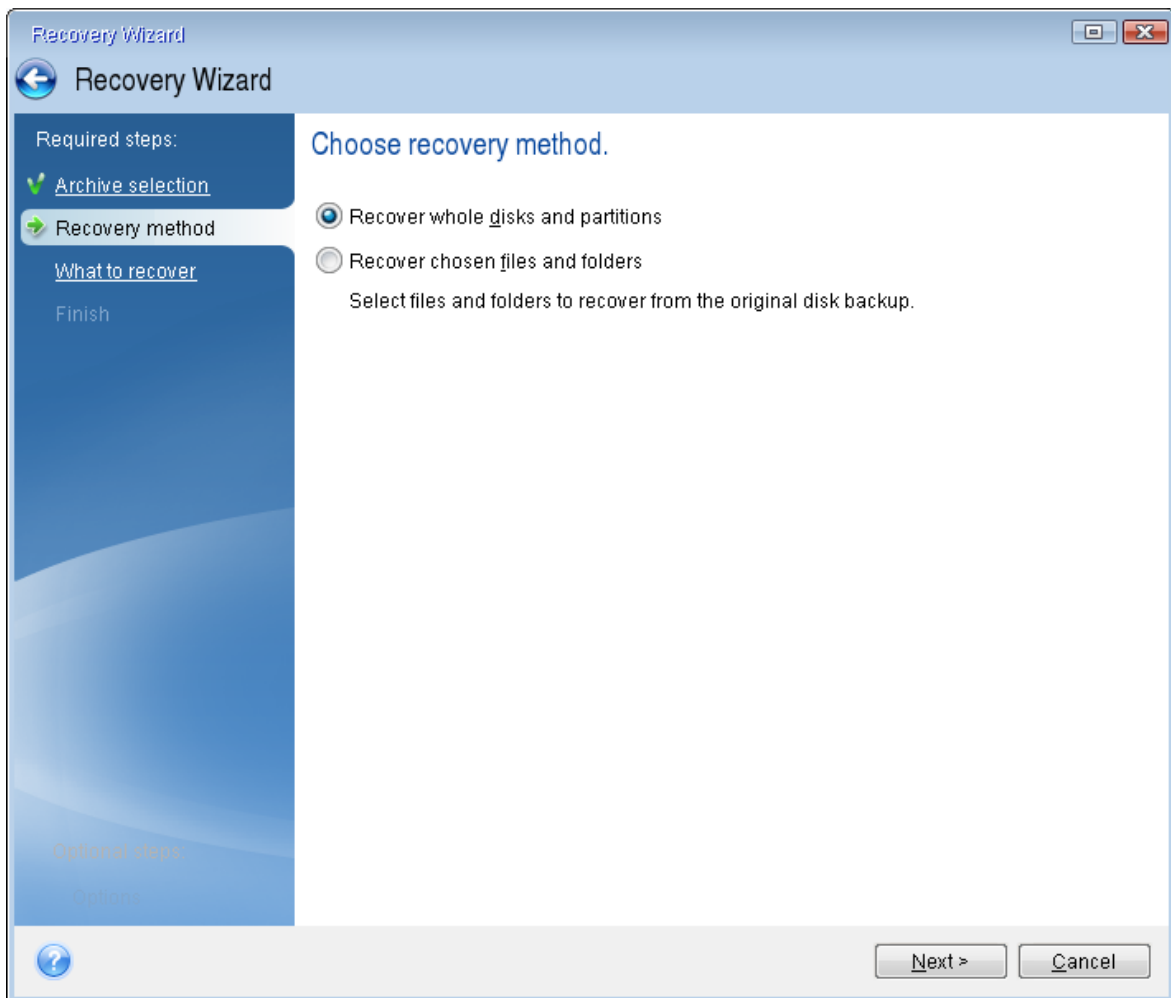
If you use a UEFI computer, pay attention to the boot mode of the bootable media in UEFI BIOS. It is recommended that the boot mode matches the type of the system in the backup. If the backup contains a BIOS system, then boot the bootable media in BIOS mode; if the system is UEFI, then ensure that UEFI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

3. Boot from Acronis bootable media and select **Acronis True Image for Kingston**.
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.

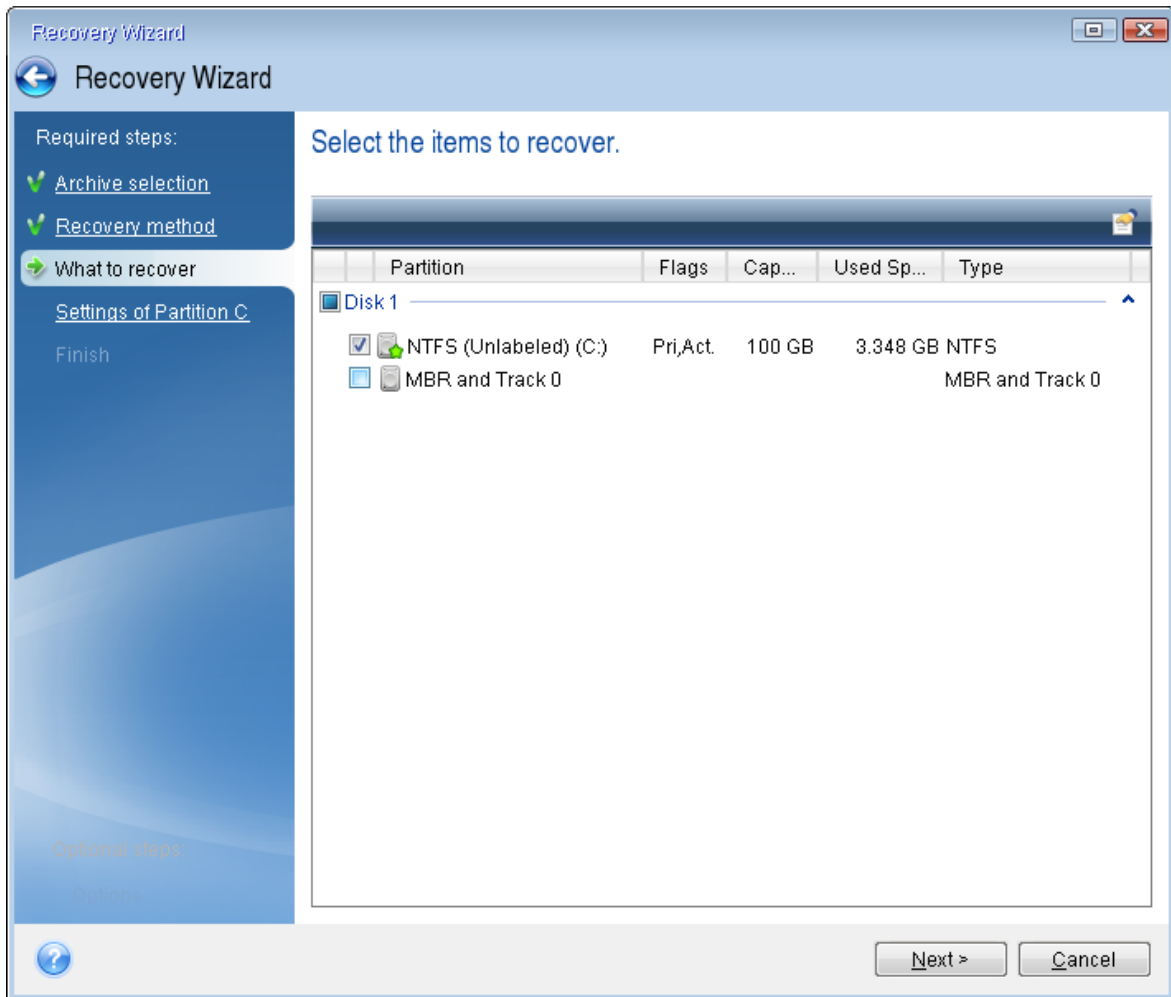
Note

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.

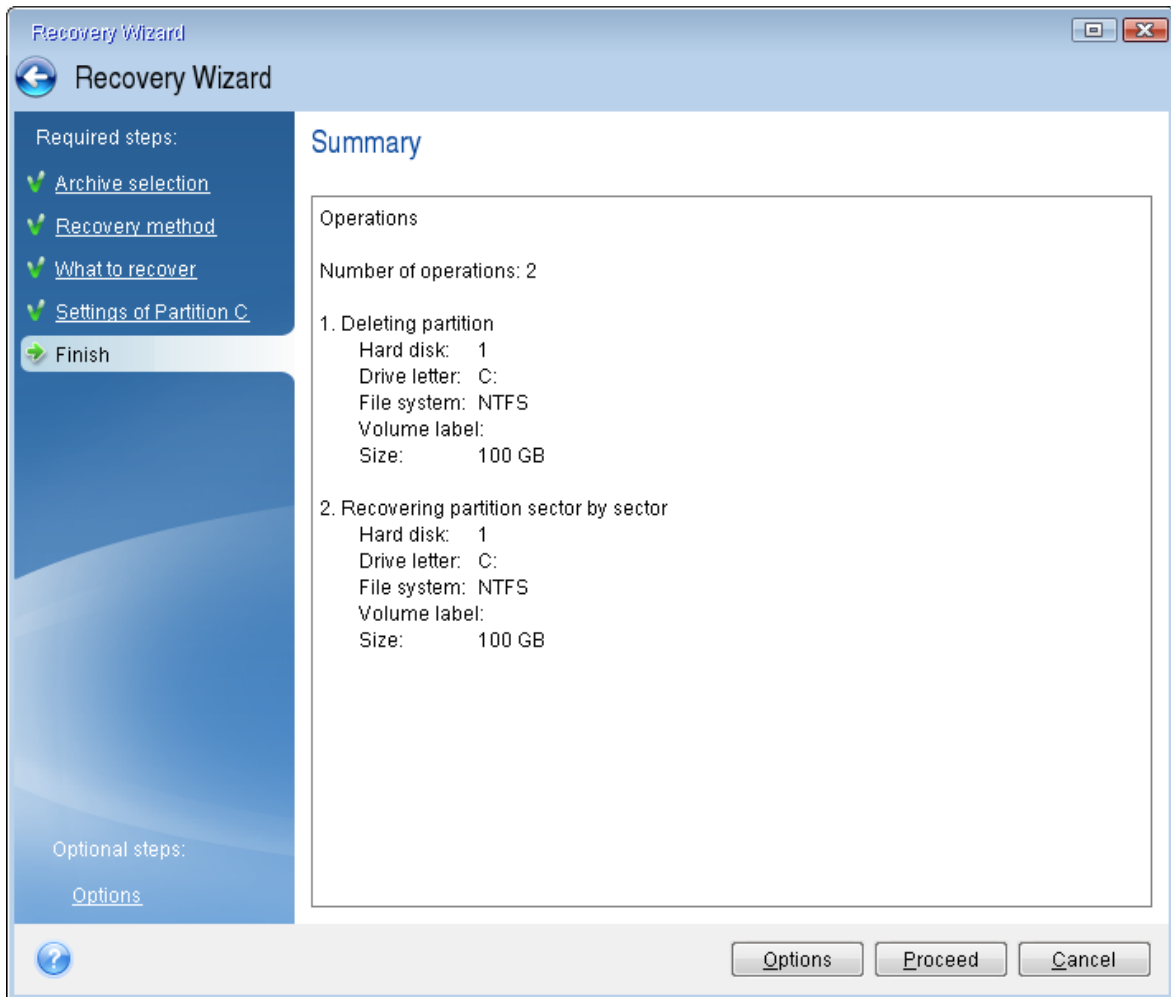
6. Select **Recover whole disks and partitions** at the **Recovery method** step.



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 Kingston, 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

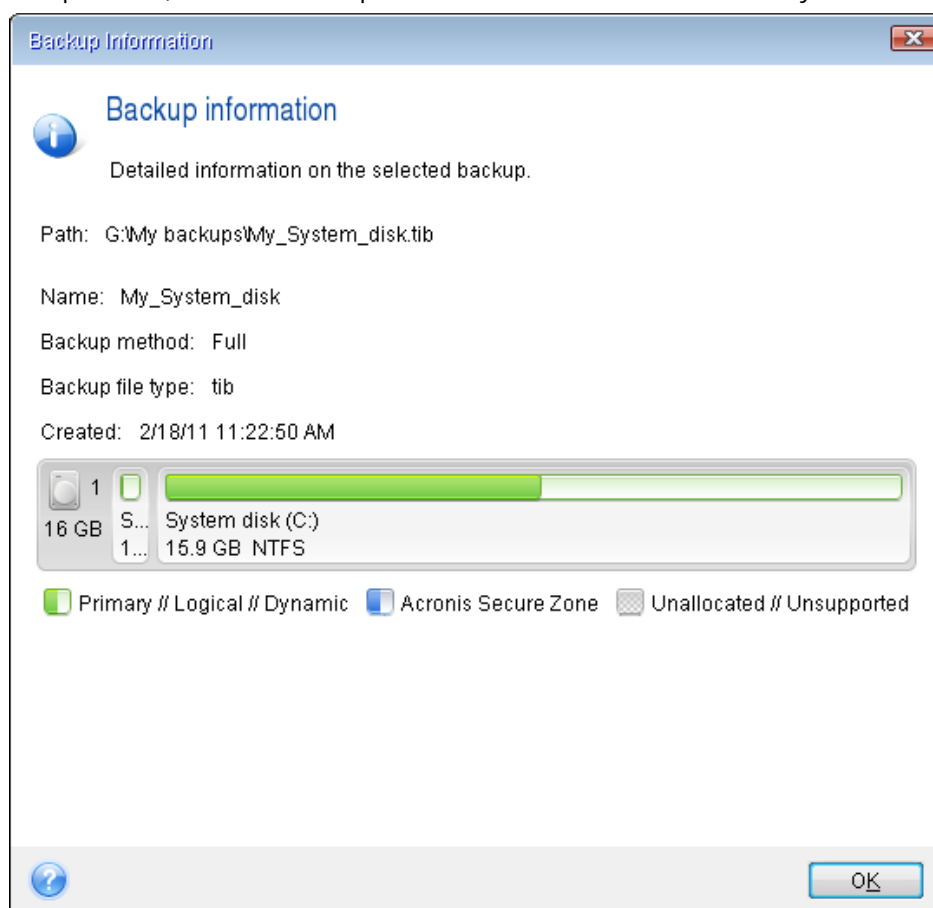
1. Install the new hard drive to the same position in the computer and use the same cable and connector that was used for the original drive. If this is not possible, install the new drive to where it will be used.
2. Attach the external drive if it contains the backup to be used for recovery and make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

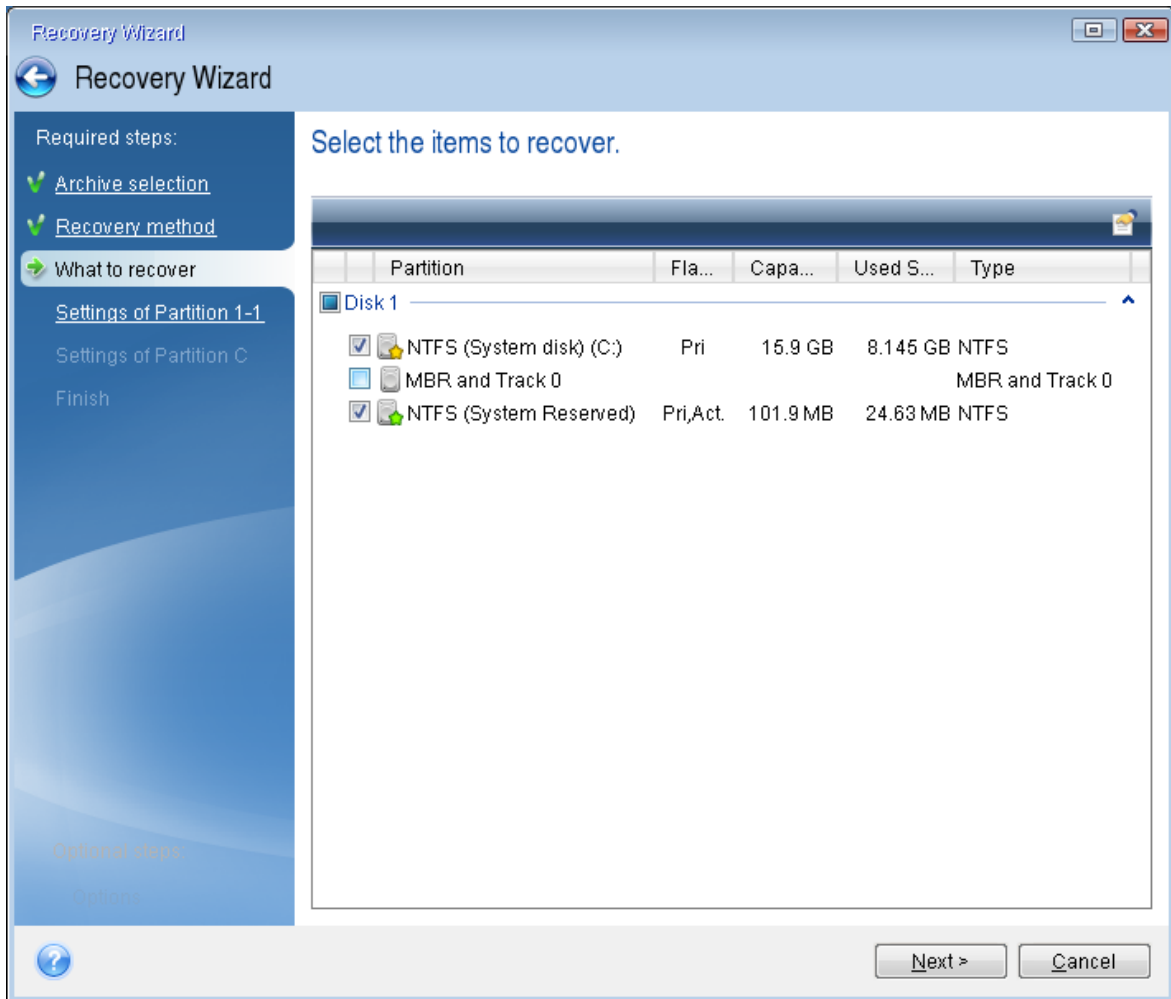
Note

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.

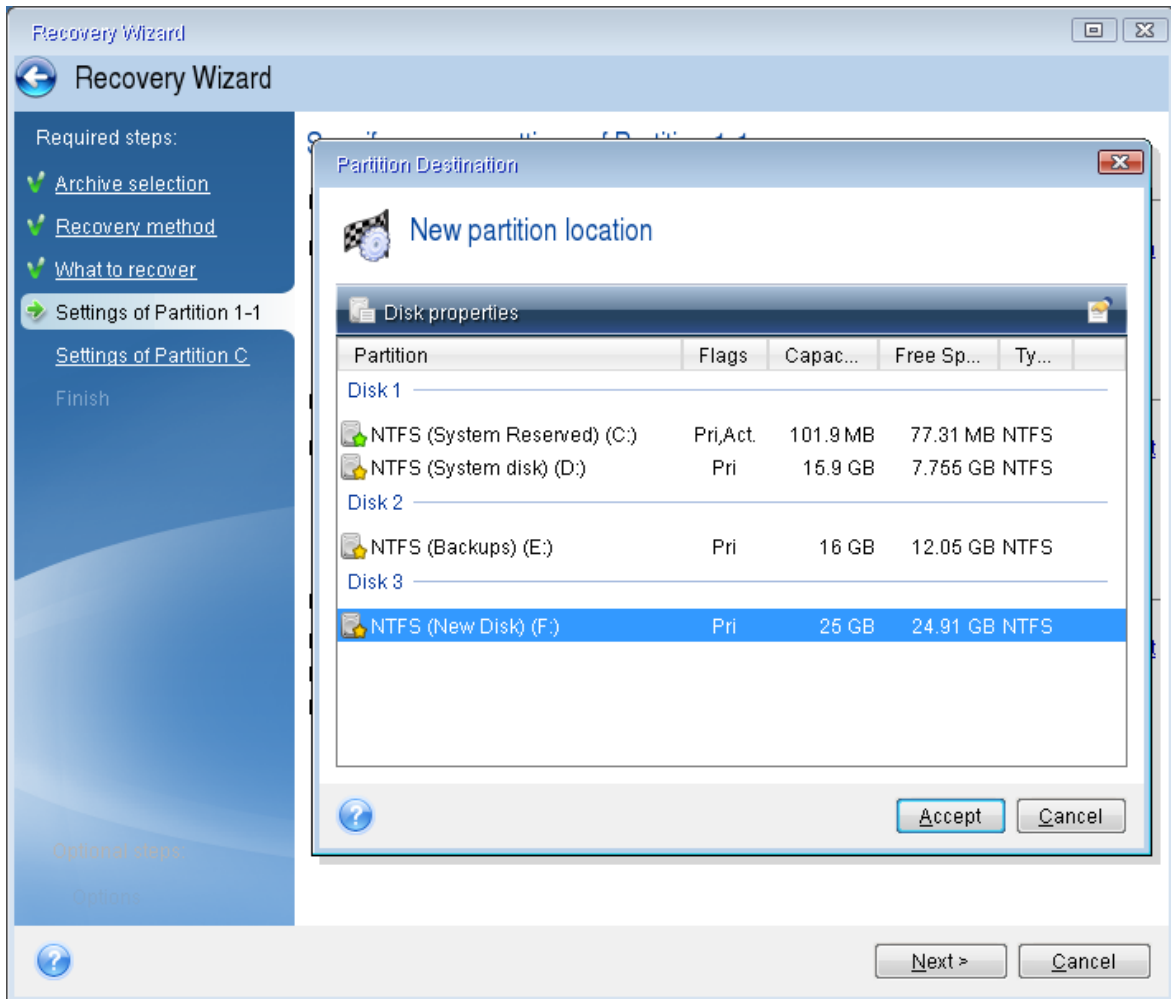


8. Select **Recover whole disks and partitions** at the **Recovery method** step.
9. On the **What to recover** step, select the boxes of the partitions to be recovered.
If you select an entire disk, MBR and Track 0 of the disk will also be recovered.

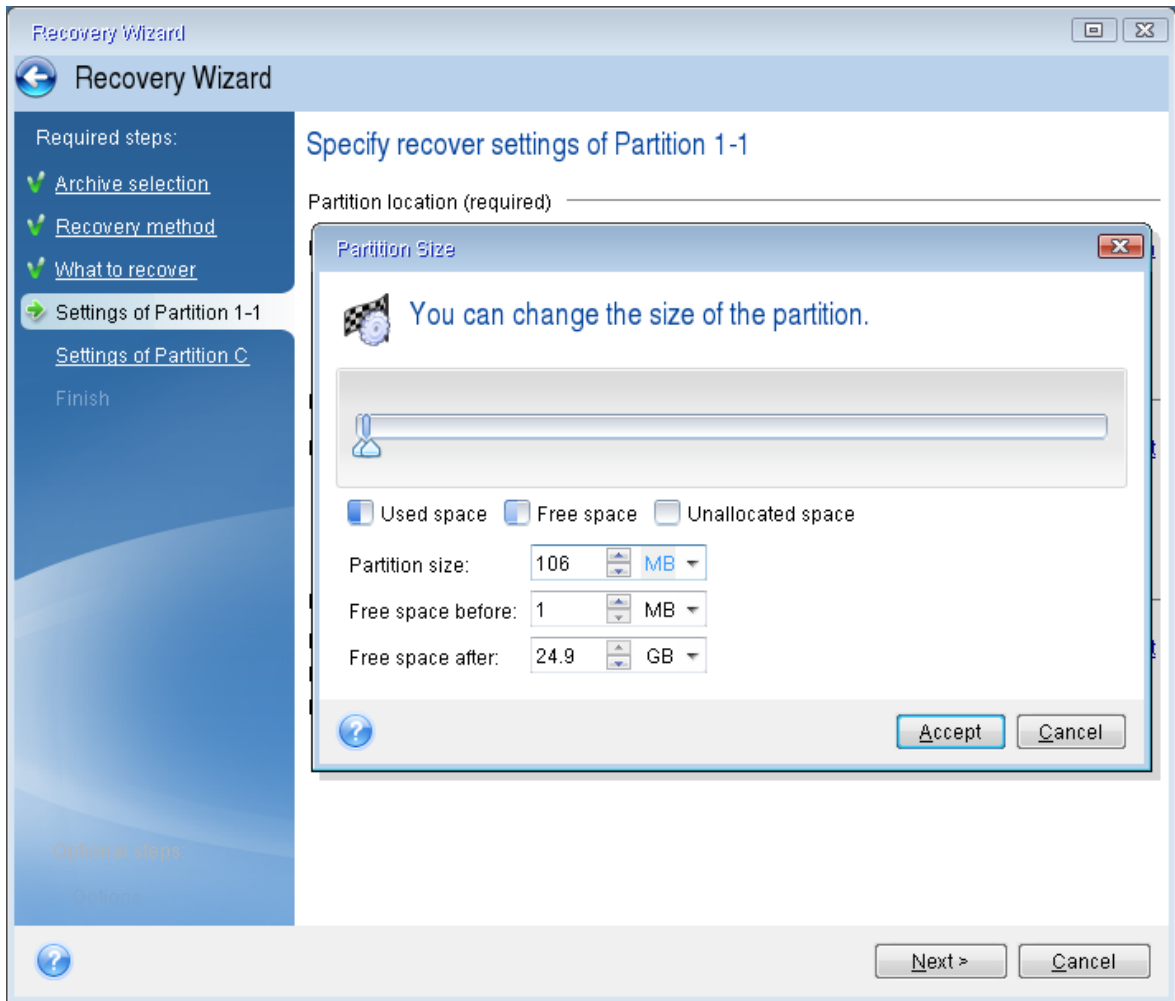


Selecting partitions leads to appearance of the relevant steps **Settings of partition**. Note that these steps start with partitions which do not have an assigned disk letter (as usually is the case with hidden partitions). The partitions then take an ascending order of partition disk letters. This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

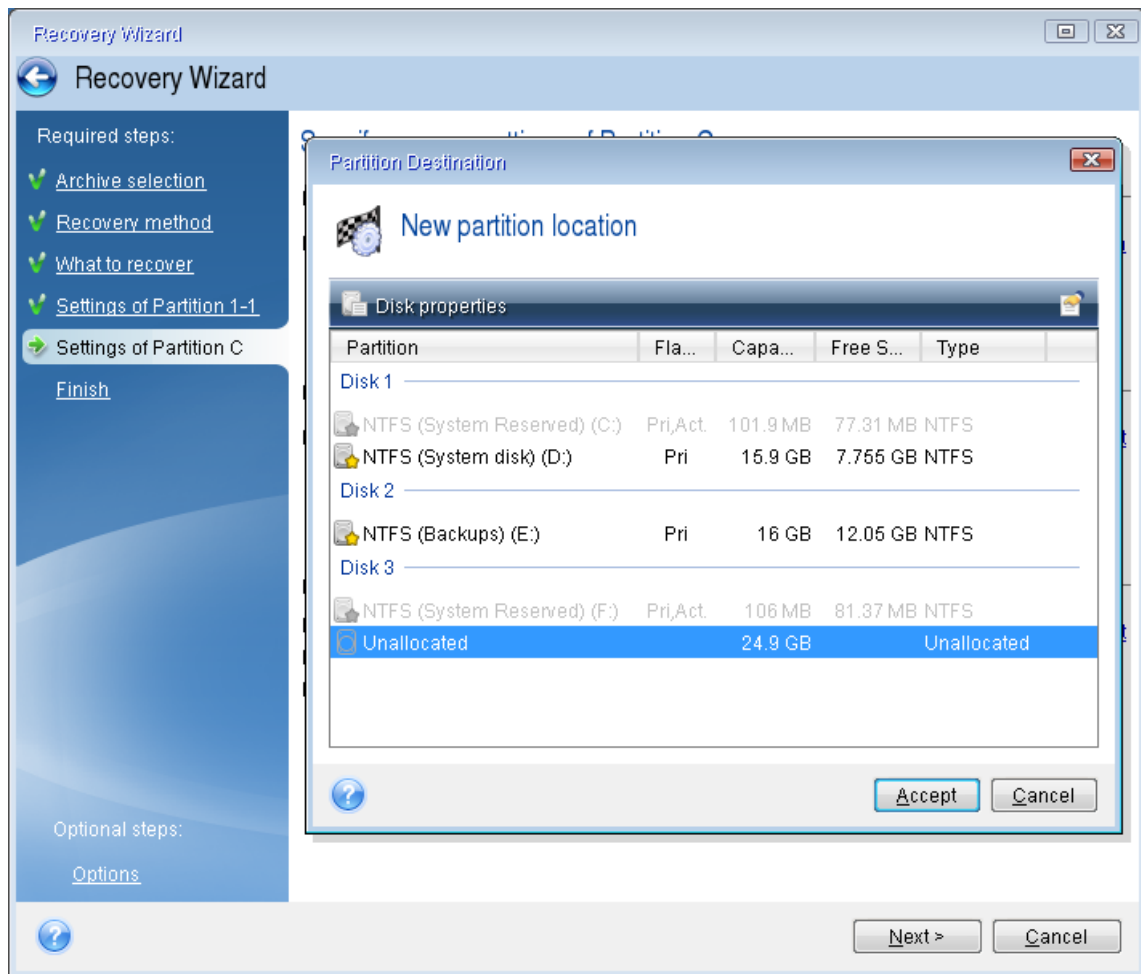
10. On the Settings of the hidden partition step (usually named Settings of Partition 1-1), specify the following settings:
 - **Location**—Click **New location**, select your new disk by either its assigned name or capacity, and then click **Accept**.



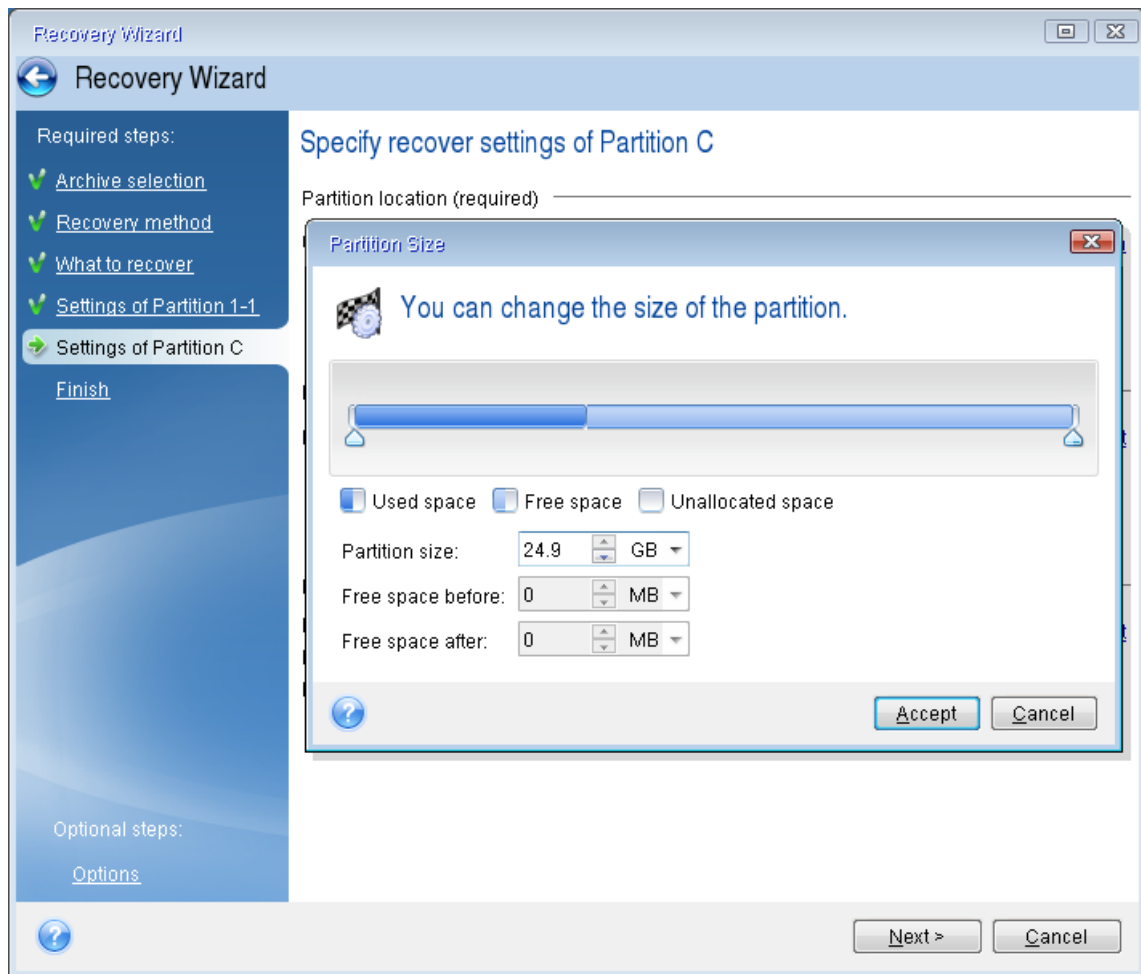
- **Type**—Check the partition type and change it, if necessary. Ensure that the System Reserved partition (if any) is primary and marked as active.
- **Size**—Click **Change default** in the Partition size area. By default the partition occupies the entire new disk. Enter the correct size in the Partition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



- 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

To recover partitions or disks

- Start Acronis True Image for Kingston.
- 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**.
- 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.

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.

Manage Partition ✕

Letter: Label: Type:

Used: **1.2 GB** Partition size:

Unallocated space

i You can create partitions on the unallocated space, by using Acronis Disk Director.
[Learn more about Acronis Disk Director](#)

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 and my OS supports UEFI | The operation will not affect neither partition layout nor bootability of the disk: partition style will remain MBR, the destination disk will be bootable in BIOS. | The destination partition will be converted to GPT style that will make the destination disk bootable in UEFI. See Example of recovery to UEFI system . |
| 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.

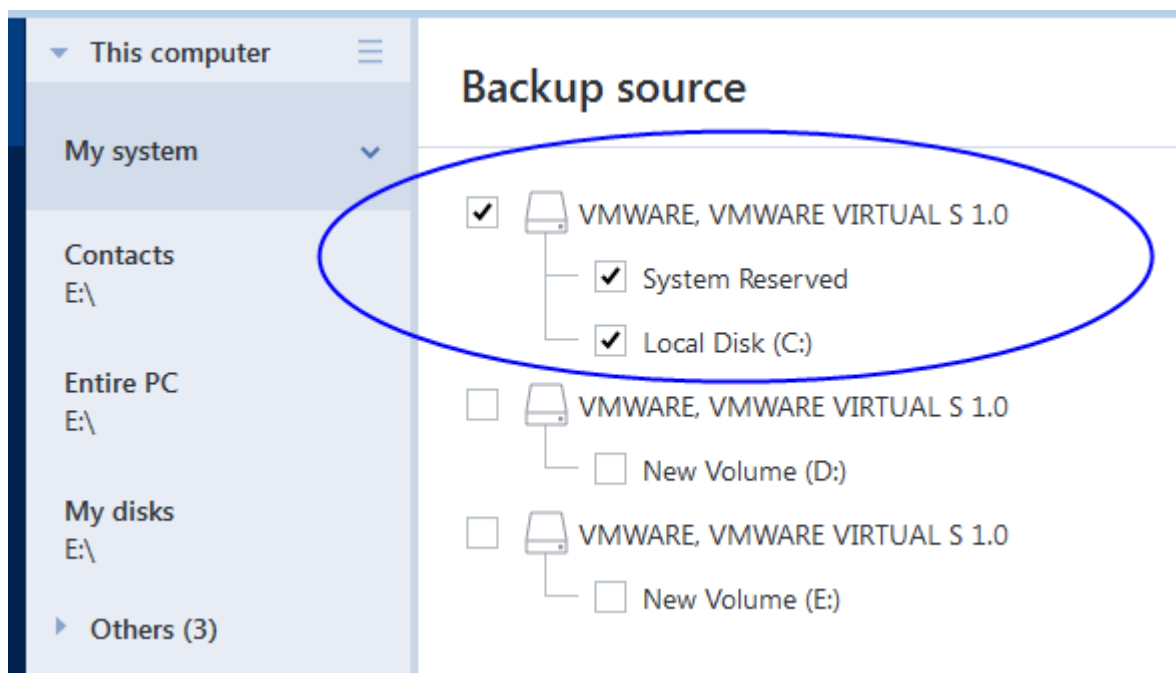
Before you start the procedure, ensure that you have:

- **Acronis bootable media.**

Refer to [Creating Acronis bootable media](#) for details.

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

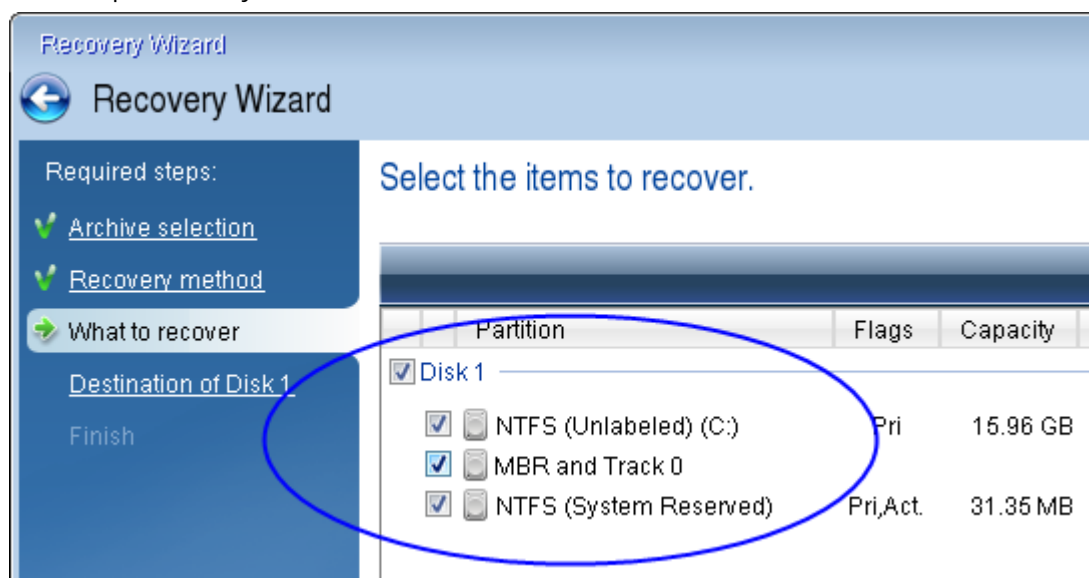
To create this backup, switch to disk mode, and then select the hard drive that contains your system partition. Refer to [Backing up disks and partitions](#) for details.



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

1. Boot from the Acronis bootable media in UEFI mode and select Acronis True Image for Kingston.
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

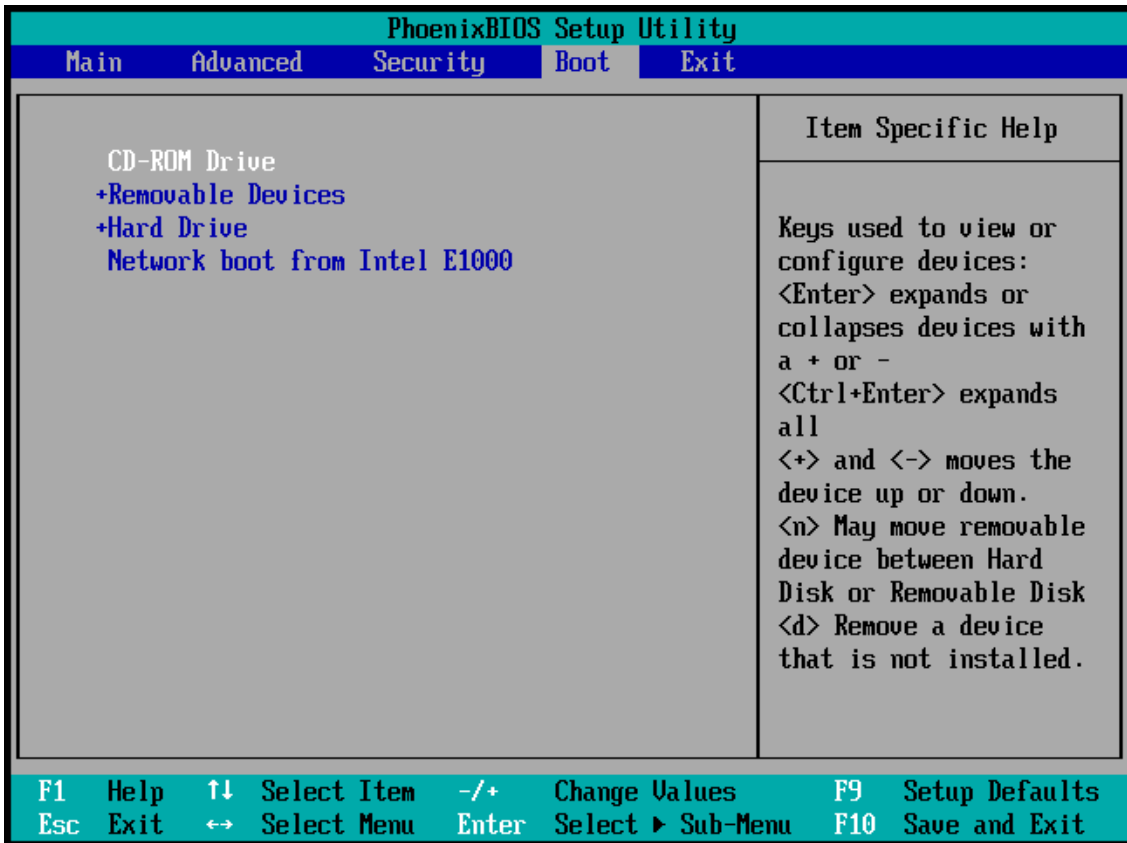
1. If you use a USB flash drive or external drive as a bootable media, plug it into the USB port.
2. Turn your computer on. During the Power-On Self Test (POST), you will see the key combination that you need to press in order to enter BIOS or UEFI BIOS.
3. Press the key combination (such as, **Del**,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

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.

- [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.
- 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.

To recover data in File Explorer

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

Note

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

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

- Start recovering data as described in [Recovering partitions and disks](#) or [Recovering files and folders](#).
- 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**.
- By default, Acronis True Image for Kingston 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.
- 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 the equal priority with other processes.
- **High**—The backup or recovery process will run faster, but the performance of other programs will be reduced. Be aware that selecting this option may result in 100% CPU usage by Acronis True Image for Kingston.

Notifications for recovery operation

Location: **Recovery options > Notifications**

Sometimes a backup or recovery procedure can last an hour or longer. Acronis True Image for Kingston 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 Kingston 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 Kingston 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 Kingston UI only. You cannot stop the process manually through Task Manager or any other external tool.

The Protection dashboard

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

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

- View statistics about the active protection status.
- View the number of detected issues, 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 Kingston 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 Kingston 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 Kingston 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 Kingston finds a good temporary copy, the file is restored from that copy.

Note

Acronis True Image for Kingston does not support file recovery from password-protected backups.

To configure Acronis True Image for Kingston 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 Kingston recovers the files as follows.

Acronis True Image for Kingston 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 Kingston 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 Kingston 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 Kingston does not support file recovery from password-protected backups.

- **Protect backup files from ransomware** – Acronis True Image for Kingston will protect its own processes and your backups from ransomware.
 - **Protect network shares and NAS** – Acronis True Image for Kingston 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

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

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

To restore or delete files from quarantine:

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

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

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

Configuring Protection exclusions

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

To add a file or folder to the Protection exclusions list

1. On the **Protection** dashboard, click **Protection exclusions**.
2. From the **Add exclusion** menu, select what you want to exclude.
 - **Add file**—to exclude executable or other files from scanning 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.

Tools

Note

Certain features and functionalities may be unavailable in the edition that you use.

Protection tools

- "Acronis Media Builder" (p. 75)

Disk cloning

- "Disk cloning utility" (p. 95)

Image mounting

- "Mounting a backup image" (p. 92)
- "Unmounting an image" (p. 94)

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 Kingston and recover your computer.

You can create several types of bootable media:

- **Acronis bootable media**

This type is recommended for most users.

Notes

- We recommend that you create a new bootable media after each Acronis True Image for Kingston update.
- If you use non-optical media, the media must have a FAT16 or FAT32 file system.
- If Acronis Media Builder does not recognize your USB flash drive, you can try using the procedure described in the Acronis Knowledge Base article at <https://kb.acronis.com/content/1526>.
- 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 Kingston, you cannot recover files and folders encrypted with the encryption available in Windows XP and later operating systems. However, backups encrypted using the Acronis True Image for Kingston 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 Kingston.
3. In the **Tools** section, click **Bootable Rescue Media Builder**.

4. Choose a creation method.
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 Kingston will suggest formatting it to FAT file system.

Warning!

Formatting permanently erases all data on a disk.

- **ISO image file**

You will need to specify the .iso file name and the destination folder.

When the .iso file is created, you can burn it onto a CD or DVD. For example, in Windows 7 and later, you can do this by using a built-in burning tool. In File Explorer, double-click the created ISO image file, and then click **Burn**.

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 media, it may be best to contact the 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 Kingston 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.

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.

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. Refer to [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 Kingston**.

Note

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

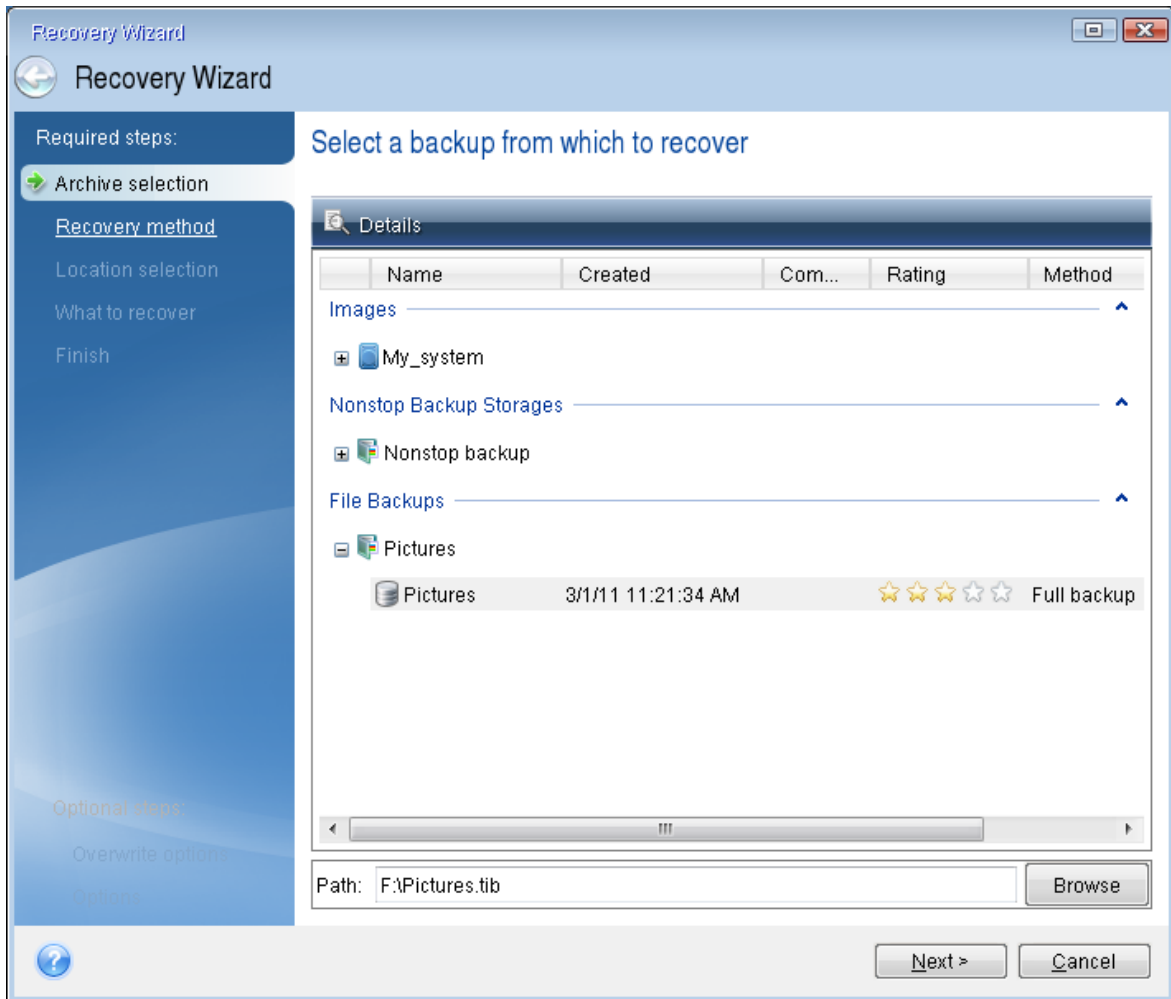
4. When the program starts, we recommend that you try recovering some files from your backup. A test recovery allows you to make sure that your bootable CD can be used for recovery. In addition, you can make sure that the program detects all of the hard drives you have in your system.

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. Start Recovery Wizard by clicking **Recovery** -> **Disk Recovery** on the toolbar.
2. Select a backup at the **Archive location** step, and then click **Next**.



- 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.
- After the **Destination** window opens, check that all of your drives are shown under **My Computer**.

Note

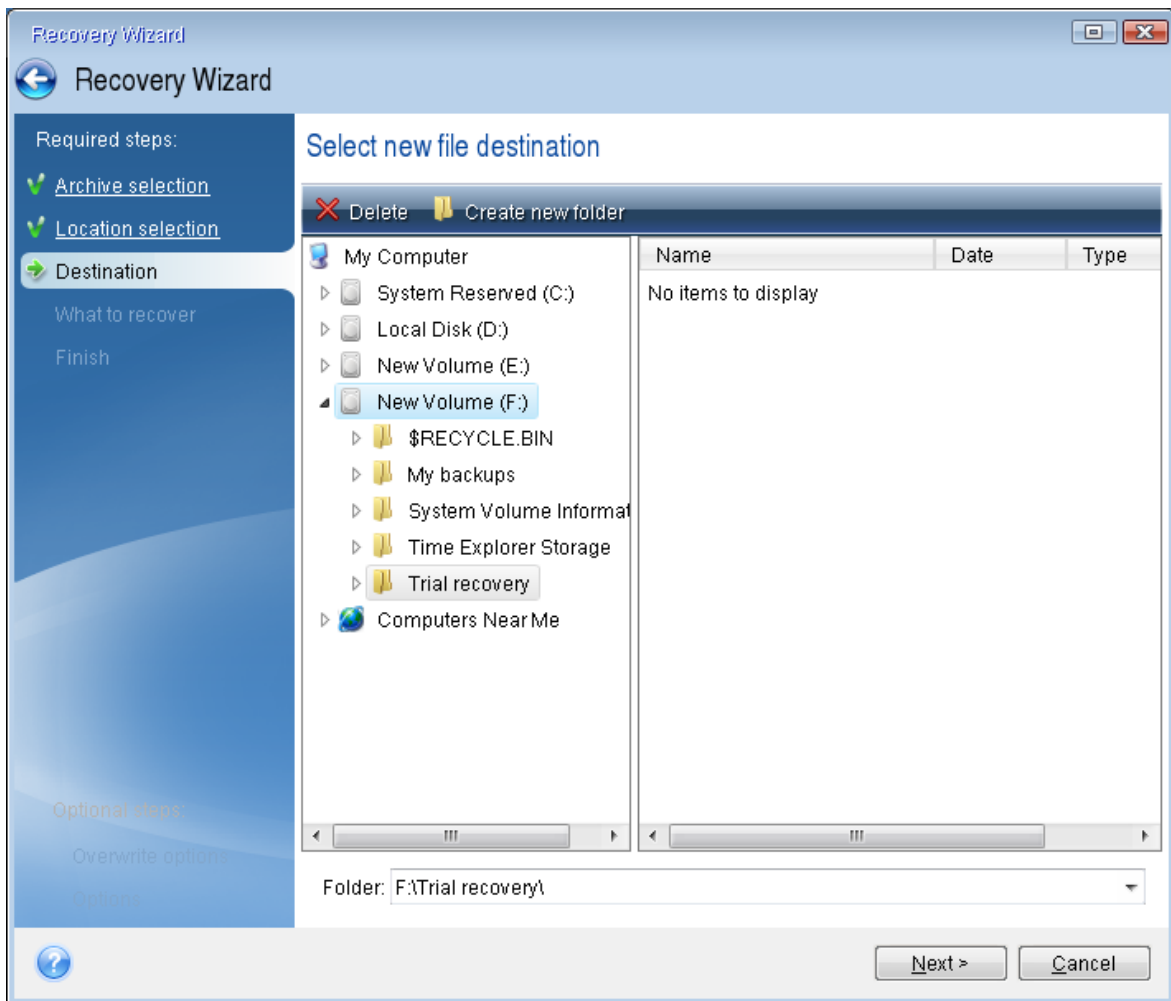
If you store your backups on the network, verify that you can access the network.

Note

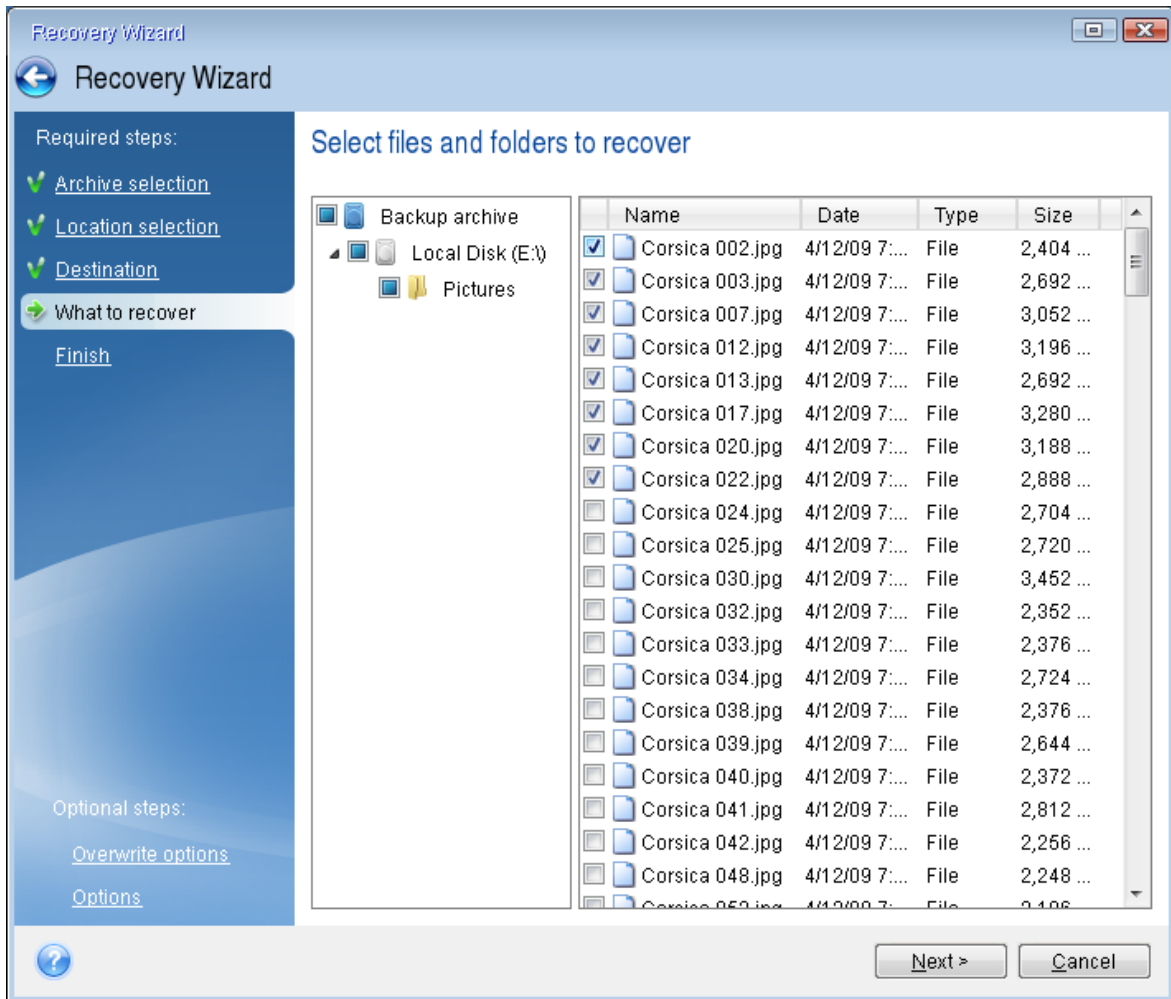
If no computers are visible on the network, but the **Computers Near Me** icon is found under **My Computer**, specify the network settings manually. To do this, open the window available at **Tools & Utilities > Options > Network adapters**.

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 Kingston.



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 Kingston.

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 Kingston** item and press the F11 key.
2. When the command line appears, type **vga=ask** and click **OK**.
3. Select **Acronis True Image for Kingston** 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).

```

333 1024x768x16 VESA      334 1152x864x16 VESA      335 1280x960x16 VESA
336 1280x1024x16 VESA     337 1400x1050x16 VESA     338 1600x1200x16 VESA
339 1792x1344x16 VESA     33A 1856x1392x16 VESA     33B 1920x1440x16 VESA
33C  320x200x32 VESA      33D  320x400x32 VESA      33E  640x400x32 VESA
33F  640x480x32 VESA      340  800x600x32 VESA      341 1024x768x32 VESA
342 1152x864x32 VESA      343 1280x960x32 VESA      344 1280x1024x32 VESA
345 1400x1050x32 VESA     346 1600x1200x32 VESA     347 1792x1344x32 VESA
348 1856x1392x32 VESA     349 1920x1440x32 VESA     34A 1366x768x8 VESA
34B 1366x768x16 VESA      34C 1366x768x32 VESA      34D 1680x1050x8 VESA
34E 1680x1050x16 VESA     34F 1680x1050x32 VESA     350 1920x1200x8 VESA
351 1920x1200x16 VESA     352 1920x1200x32 VESA     353 2048x1536x8 VESA
354 2048x1536x16 VESA     355 2048x1536x32 VESA     356  320x240x8 VESA
357  320x240x16 VESA      358  320x240x32 VESA      359  400x300x8 VESA
35A  400x300x16 VESA      35B  400x300x32 VESA      35C  512x384x8 VESA
35D  512x384x16 VESA      35E  512x384x32 VESA      35F  854x480x8 VESA
360  854x480x16 VESA      361  854x480x32 VESA      362 1280x720x8 VESA
363 1280x720x16 VESA      364 1280x720x32 VESA      365 1920x1080x8 VESA
366 1920x1080x16 VESA     367 1920x1080x32 VESA     368 1280x800x8 VESA
369 1280x800x16 VESA      36A 1280x800x32 VESA      36B 1440x900x8 VESA
36C 1440x900x16 VESA      36D 1440x900x32 VESA      36E  720x480x8 VESA
36F  720x480x16 VESA      370  720x480x32 VESA      371  720x576x8 VESA
372  720x576x16 VESA      373  720x576x32 VESA      374  800x480x8 VESA
375  800x480x16 VESA      376  800x480x32 VESA      377 1280x768x8 VESA
378 1280x768x16 VESA      379 1280x768x32 VESA
Enter a video mode or "scan" to scan for additional modes: _

```

5. Wait until Acronis True Image for Kingston 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 Kingston 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

Note

Certain features and functionalities may be unavailable in the edition that you use.

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.

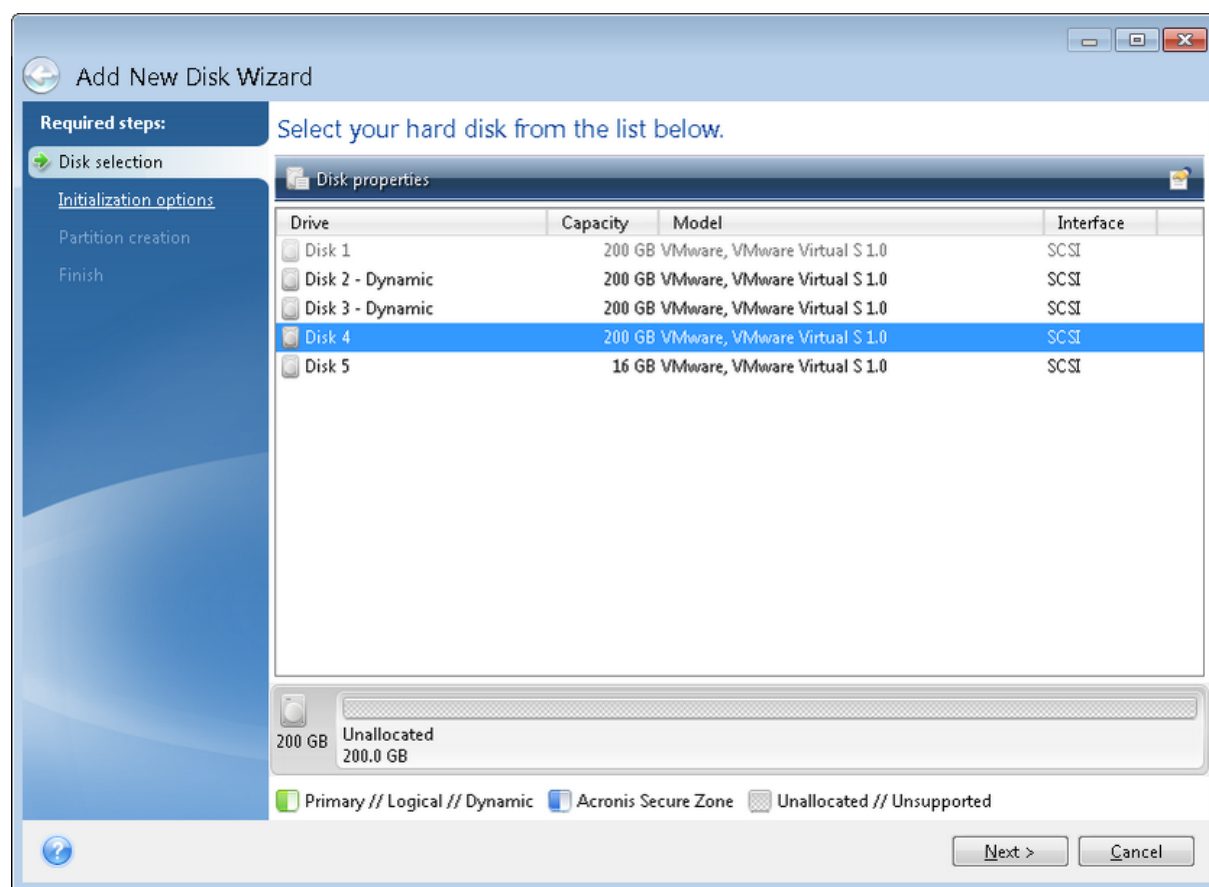
5. On the **Finish** step, ensure that the configured disk layout suits your needs, and then click **Proceed**.

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.

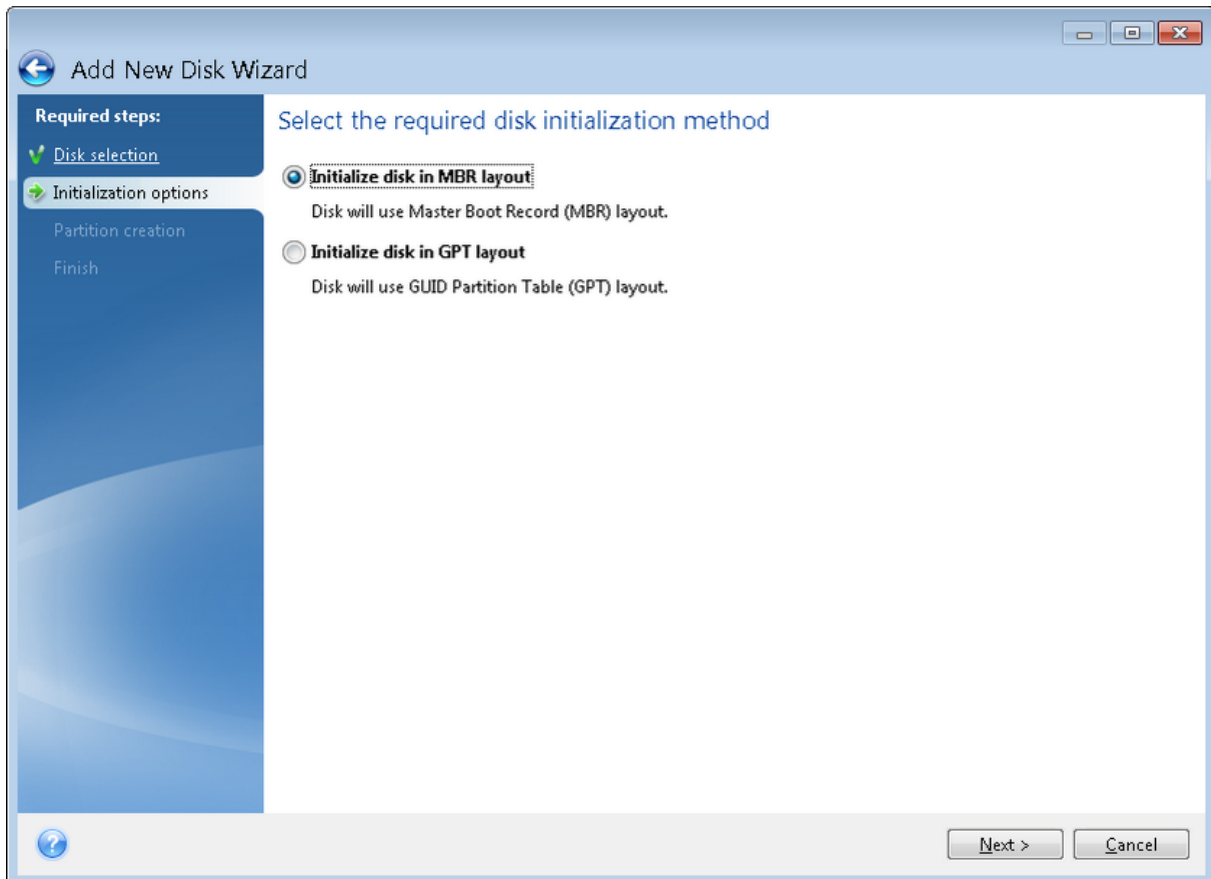
Note

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



Selecting initialization method

Acronis True Image for Kingston 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**.

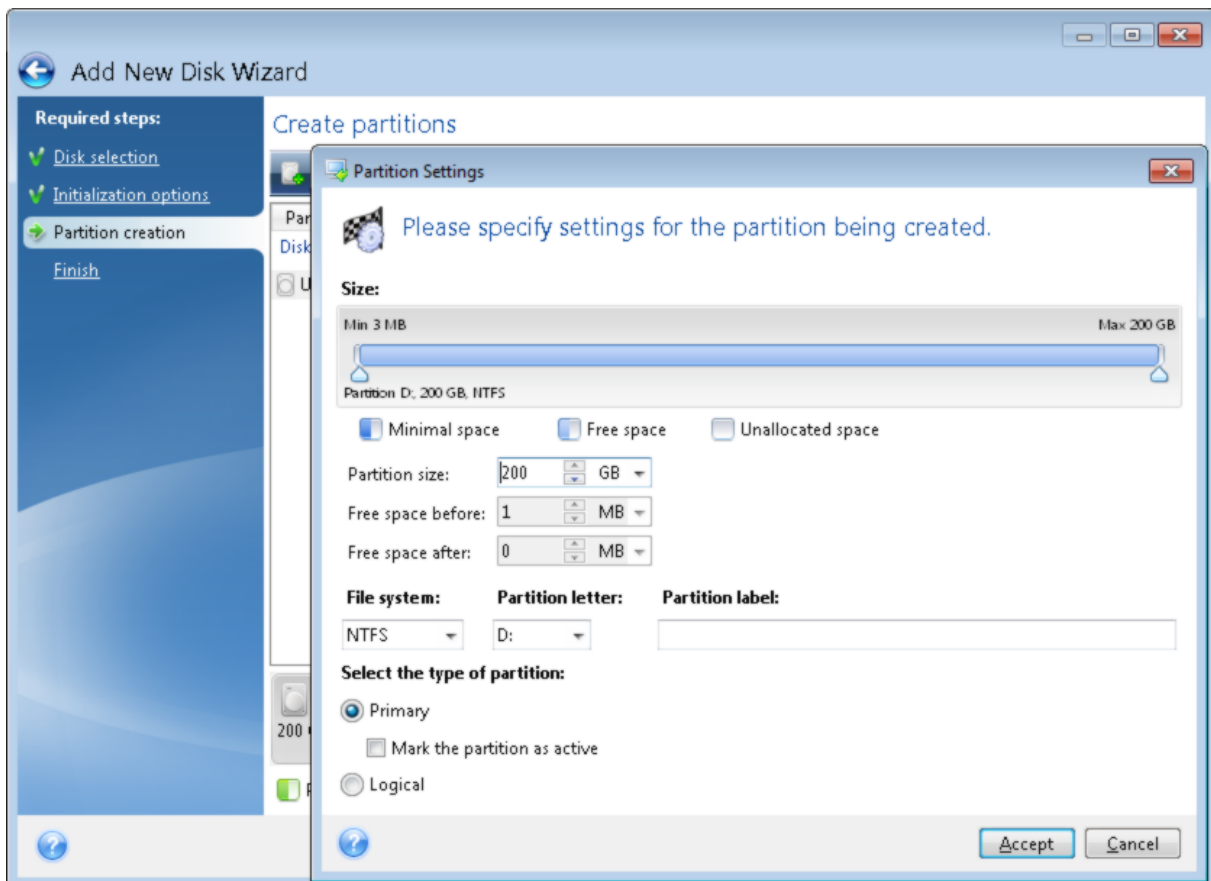
After selecting the required initialization method click **Next**.

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 labelRefer to [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

Note

Certain features and functionalities may be unavailable in the edition that you use.

Acronis DriveCleanser allows you to permanently destroy all data on selected hard disks and partitions. For the destruction, you can use one of the preset algorithms or create your own. Refer to [Algorithm selection](#) 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. Refer to [Source selection](#) for details.
3. On the **Algorithm selection** step, select an algorithm that you want to use for the data destruction. Refer to [Algorithm selection](#) for details.
4. [optional step] You can create your own algorithm. Refer to [Creating custom algorithm](#) for details.
5. [optional step] On the **Post-wiping actions** step, choose what to do with the partitions and disk when the data destruction is complete. Refer to [Post-wiping actions](#) 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**.

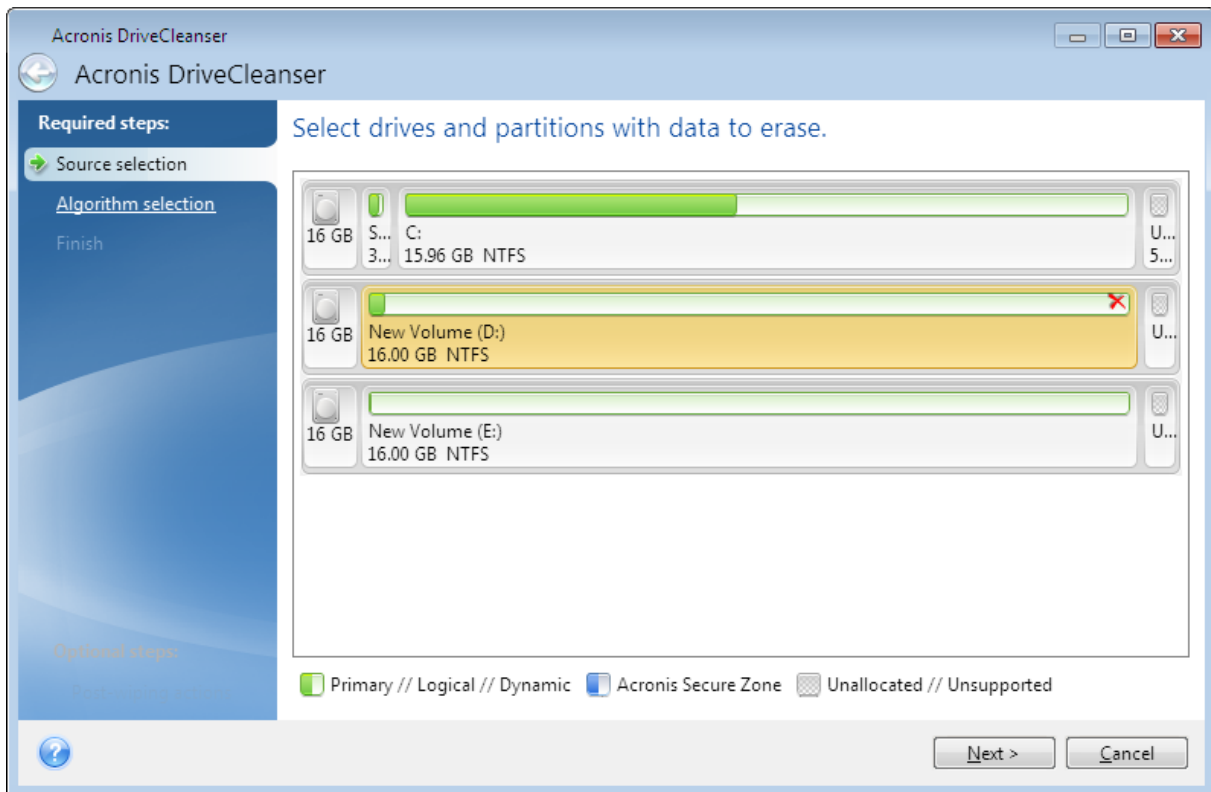
Warning!

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 (📀).



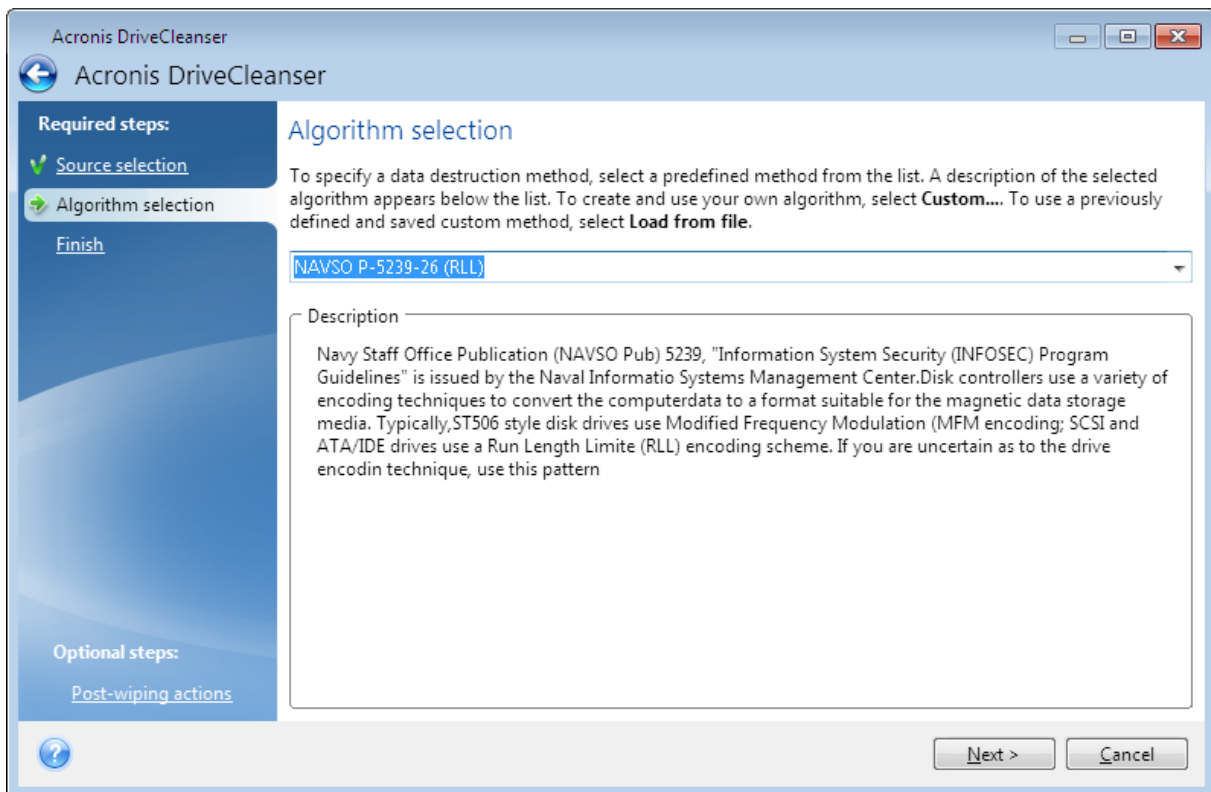
Note

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. Refer to [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. 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.

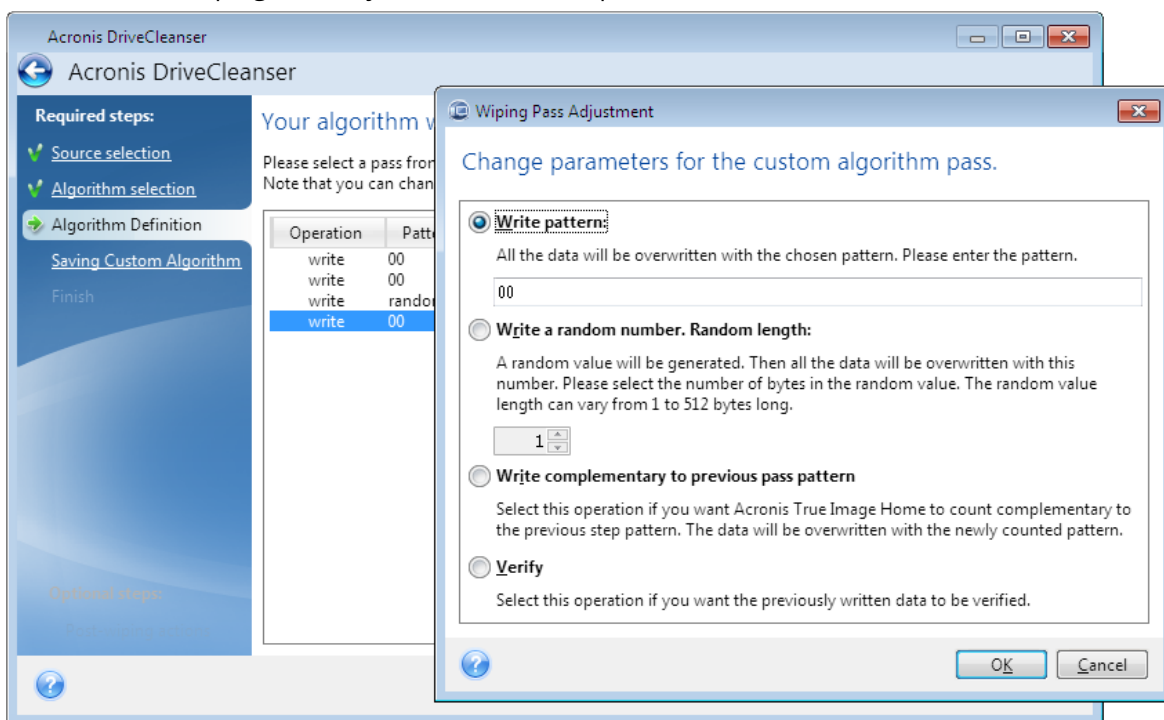
The table has the following legend:

- 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 Kingston adds a complementary value to the one written to disk during the previous pass.

- **Verify**

Acronis True Image for Kingston 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**.

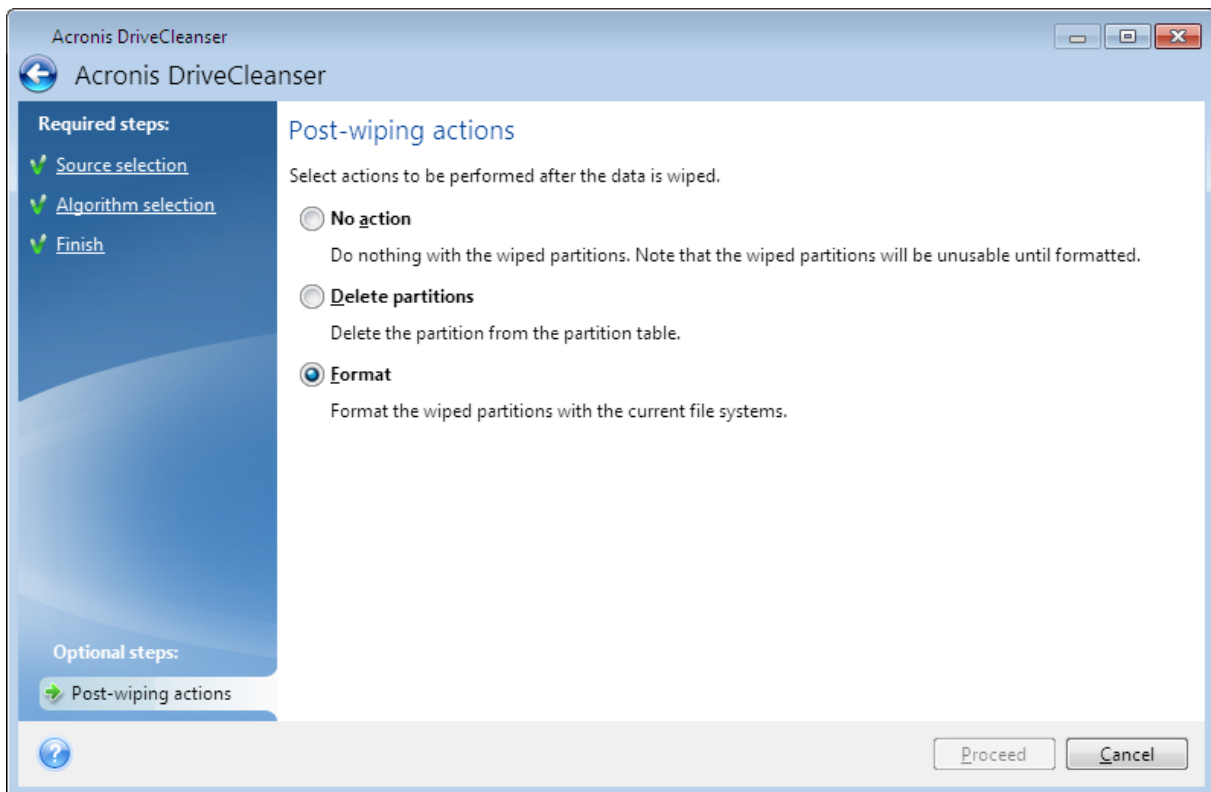
Saving algorithm to a file

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

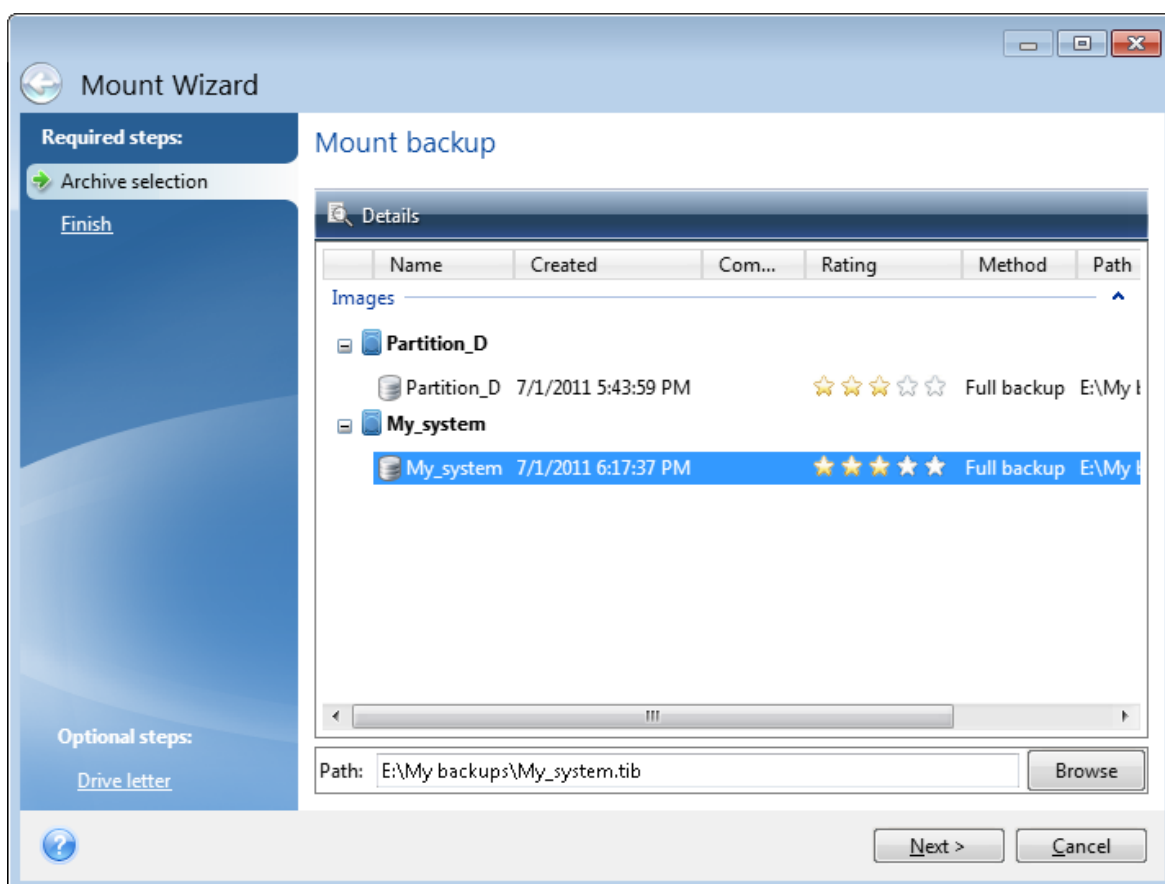
The operations described in this section are supported only for the FAT and NTFS file systems.

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.

Disk cloning and migration

Note

Certain features and functionalities may be unavailable in the edition that you use.

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.

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.

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 Kingston.
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 Kingston does not support cloning of dynamic disks.

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.

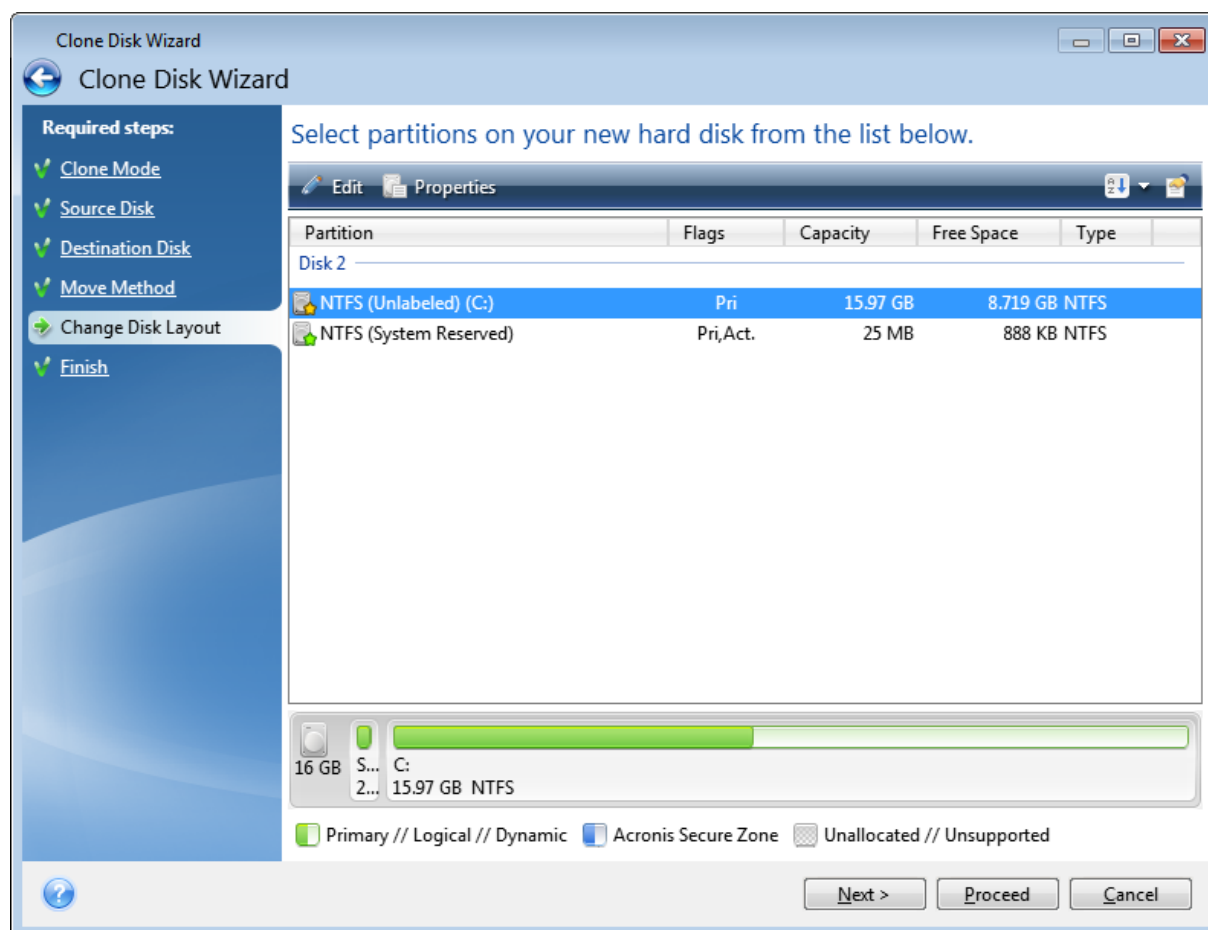
6. [This step is only available if the source disk has an OS installed]. On the **Disk Usage** step, select how you are going to use the clone.
 - **To replace a disk on this machine**—the system disk data will be copied, and the clone will be bootable. Use this clone for replacing the system disk with 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.
 - **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.
- [This step is only available in the manual cloning mode]. On the **Change disk layout** step, you can edit settings of the partitions that will be created on the destination disk. Refer to [Manual partitioning](#) for details.
 - [Optional step] On the **What to exclude** step, you can specify files and folders that you do not want to clone. Refer to [Excluding items from cloning](#) for details.
 - 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 Kingston does not alter the original disk and data stored on it during cloning.

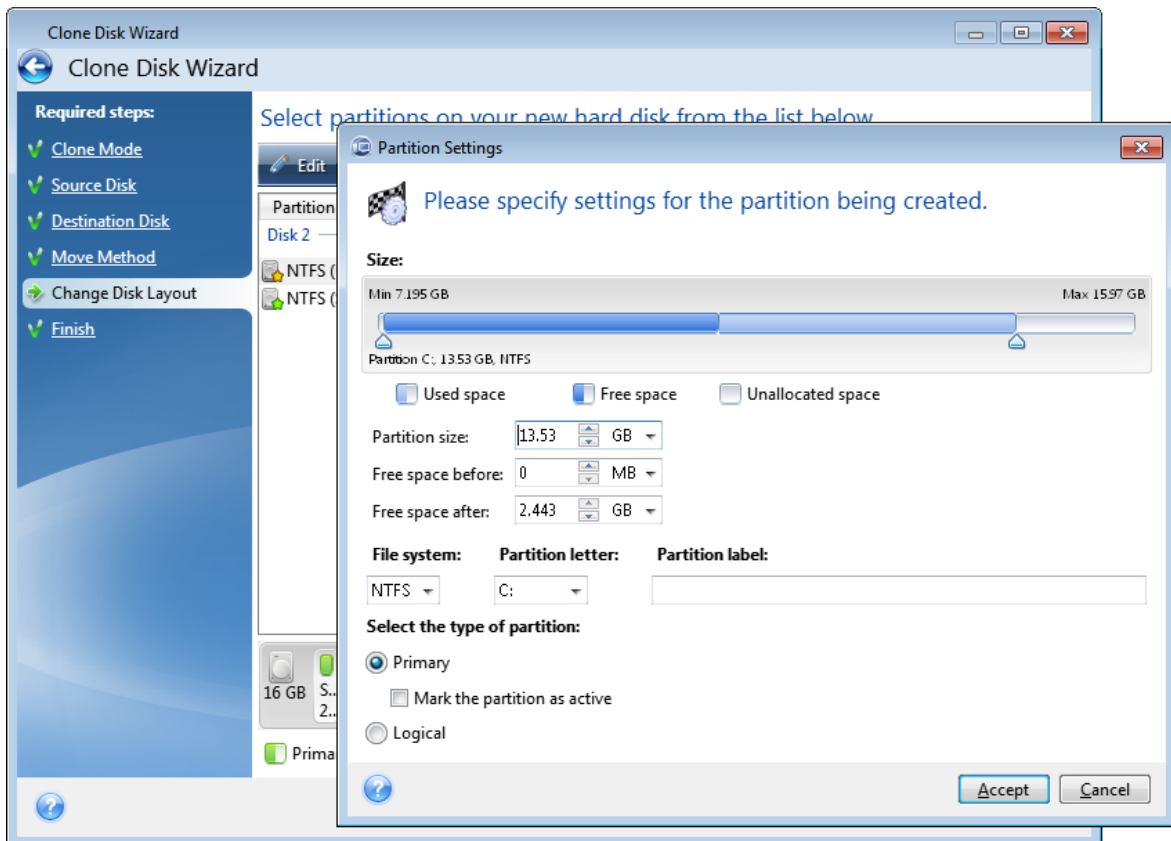
Manual partitioning

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

Refer to [Partition settings](#) for details.

3. Click **Accept**.

Warning!

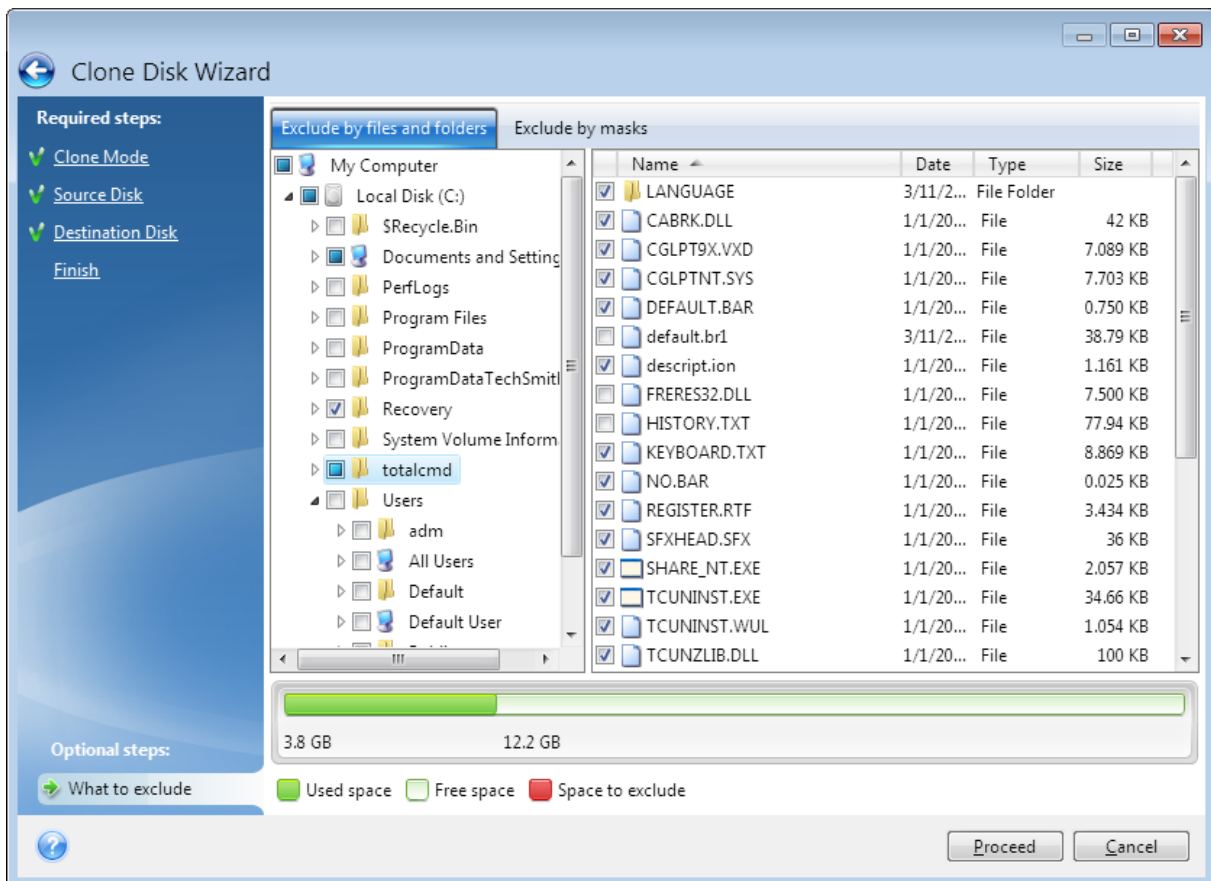
Clicking any previous wizard step on the sidebar in this window will reset all size and location changes that you've selected, so you will have to specify them again.

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 Kingston 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 Kingston 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 Kingston does not recognize your SSD

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

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

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

If the BIOS of your computer does show the 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
```

Start Acronis True Image for Kingston 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 7 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 Kingston.
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 Kingston.
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](#).

Troubleshooting

If Acronis True Image for Kingston 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 Kingston installer again. It will detect Acronis True Image for Kingston 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 Kingston. You can read the corresponding solutions in the [Acronis Knowledge Base](#).

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://kb.acronis.com/true-image-known-solutions>.

See also troubleshooting information about recovery fails at <https://kb.acronis.com/content/46340>.

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 Kingston 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**.
- If you use Windows 7 or 8, click **Start > All Programs > 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 Kingston. 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 Kingston 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. Refer to [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. Refer to [Arranging boot order in BIOS](#) for details.
3. Boot from the Acronis bootable media and select **Acronis True Image for Kingston**.

Note

Instead of clicking **Acronis True Image for Kingston**, 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.

How to collect crash dumps

Because a crash of Acronis True Image for Kingston 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 Kingston crashes, please provide the following information

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

If Acronis True Image for Kingston causes a Windows crash

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

If Acronis True Image for Kingston hangs

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

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

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

Glossary

A

Acronis Active Protection

A technology that protects data from ransomware, malicious software that blocks access to some files or an entire system and demands a ransom for unblocking. Based on a heuristic approach, this technology monitors processes on a computer in real-time mode and informs the user about attempts to encrypt data on the computer. In case files are encrypted, they can be recovered from the temporary copies or backups.

Acronis Cloud

A secure remote storage which you can use to store backups of your files, folders, partitions, disks, as well as versions of your synchronized files and folders.

B

Backup

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

Backup operation

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

Backup settings

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

Backup version

The result of a single backup operation. 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 Kingston have a .tibx extension. The TIBX files resulting from consolidation of backup versions are also called backup versions.

Backup version chain

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).

Bootable media

A physical media (CD, DVD, USB drive, or other media supported by a machine BIOS as a boot device) that contains standalone version of Acronis True Image for Kingston. Bootable media is most often used to recover an operating system that cannot start, to access and back up the data that has survived in a corrupted system, to deploy an operating system on bare metal, to create basic or dynamic volumes on bare metal, or to back up sector- by- sector a disk that has an unsupported file system.

D

Disk backup (Image)

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

F

Full backup

A backup method that is used to save all the data selected to back up. A backup process that creates a full backup version.

Full backup version

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.

O

Online backup

A backup whose destination is Acronis Cloud. Online backups are stored remotely and accessible over the Internet.

Online Dashboard

A unified cross-platform solution that allows you to track and control the protection status of all computers, smartphones, and tablets sharing the same account. To track and control the protection status of the devices in your account, use Online Dashboard

R

Recovery

Recovery is a process of returning of a corrupted data to a previous normal state from a backup.

S

Suspicious process

Acronis Active Protection uses behavioral heuristics and analyzes chains of actions done by a program (a process), which is then compared with the chain of events in a database of malicious behavior patterns. If the program acts similar to ransomware behavior and tries to modify a user's files, it is considered as suspicious.

V

Validation

An operation that checks whether you will be able to recover data from a particular backup version. For a full backup version, the program validates the full backup version only. For a differential backup version, the program validates the initial full backup version and the selected differential backup version. For an incremental backup version, the program validates the initial full backup version, the selected incremental backup version, and the whole chain (if any) of backup versions to the selected incremental backup version. If the chain contains one or more differential backup versions, the program validates (in addition to the initial full backup version and the selected incremental backup version) only the most recent differential backup version in the chain and all subsequent incremental backup versions (if any) between the differential

backup version and the selected incremental backup version.

Index

A

About recovery of dynamic/GPT disks and volumes 60

Acronis bootable media startup parameters 76

Acronis DriveCleanser 87

Acronis Media Builder 75

Acronis patented technologies 6

Acronis System Report 103

Acronis True Image advanced features 10

Active protection 71

Adding a new hard disk 82

Adding an existing backup to the list 45

Algorithm definition 90

Algorithm selection 88

Anti-ransomware protection 71

Arranging boot order in BIOS or UEFI BIOS 63

Authentication settings 25

B

Backing up all data on your PC 15

Backing up data 29

Backing up disks and partitions 29

Backing up your computer 13

Backup activity and statistics 41

Backup file naming 25

Backup operations menu 41

Backup options 30

Backup reserve copy 36

Backup schemes 30

Backup splitting 35

Backup to various places 44

Backup validation option 36

Basic concepts 21

Before you start 16

Built-in store 10

C

Cleaning up backups and backup versions 46

Cleaning up backups manually 46

Clone Disk wizard 95

Cloning a disk 16

Cloning your hard drive 15

Compression level 38

Computer restart 67

Computer shutdown 38

Configuring Active Protection 72

Configuring Protection exclusions 73

Copyright statement 6

Creating Acronis bootable media 14, 75

Creating custom algorithms 90

Creating new partitions 84

Custom schemes 31

D

Deciding where to store your backups 23

Deleting backups 45

Disk cloning and migration 95

Disk cloning utility 95

Disk recovery mode 66

E

- Edit user command for backup 35
- Edit user command for recovery 66
- Email notification 33, 70
- Error handling 37
- Example of recovery to a UEFI system 61
- Excluding items from cloning 98

F

- FAQ about backup, recovery and cloning 27
- File recovery options 67
- File System 85
- Free disk space threshold 32, 69
- FTP connection 24
- Full backup 23

G

- Getting started 13

H

- Hard Disk Wiping methods 89
- How to collect crash dumps 105
- How to mount an image 93
- How to use Acronis DriveCleanser 87

I

- Image creation mode 34
- Installing and uninstalling Acronis True Image for Kingston 9
- Introduction 7

L

- Laptop power settings 40
- Limitations on operations with dynamic disks 9

M

- Making sure that your bootable media can be used when needed 78
- Managing custom backup schemes 32
- Managing files in Quarantine 73
- Manual partitioning 97
- Migrating to SSD using the backup and recovery method 101
- Migrating your system from an HDD to an SSD 100
- Minimum system requirements 7
- Mounting a backup image 92

N

- Network connection transfer rate 39
- Notifications for backup operation 32
- Notifications for recovery operation 69

O

- Operation priority 39, 68
- Operations with backups 41
- Other requirements 7
- Overwrite file options 68

P

- Partition label 86
- Partition letter 86
- Partition properties 59

Partition settings 85
Partition style after recovery 61
Partition type (these settings are available only for MBR disks) 86
Performance of backup operation 38
Performance of recovery operation 68
Post-wiping actions 92
Pre/Post commands for backup 34
Pre/Post commands for recovery 66
Preparing a new disk for backup 24
Preparing for recovery 48
Protecting your system 13
Protection 71

R

Recovering data 48
Recovering disks and partitions 48
Recovering files and folders 64
Recovering partitions and disks 58
Recovering your computer 17
Recovering your system after a crash 48
Recovering your system to a new disk under bootable media 52
Recovering your system to the same disk 49
Recovery of basic volumes and disks 60
Recovery of dynamic volumes 60
Recovery options 66
Resolving the most frequent issues 103

S

Saving algorithm to a file 92
Searching backup content 65

Security and Privacy Tools 87
Selecting a hard disk 83
Selecting initialization method 83
Selecting video mode when booting from the bootable media 81
Single version scheme 31
Size 85
Snapshot for backup 39
Sorting backups in the list 43
Source selection 88
Splitting backups on the fly 44
SSD size 100
Supported file systems 8
Supported operating systems 8
Supported storage media 9
System requirements and supported media 7

T

Technical Support 12
The Activity tab 42
The Backup tab 43
The difference between file backups and disk/partition images 22
The Protection dashboard 71
Tools 75
Troubleshooting 25, 103
Trying to determine the crash cause 48
Two-factor authentication (2FA) 18

U

Unmounting an image 94
Upgrading Acronis True Image for Kingston 10

User interface language 13

V

Validating backups 44

Validation option 67

W

What is Acronis True Image for Kingston? 7

What to do if Acronis True Image for Kingston
does not recognize your SSD 100

When the recovery is complete 58

Which migration method to choose 100

Why do I need it? 15, 87

Wizards 26