

Acronis

acronis.com

Acronis True Image



User Guide for Windows

REVISION: 4/1/2026

Table of contents

Introduction	10
What is Acronis True Image?	10
Backups created before Acronis True Image 2020	10
System requirements and supported media	11
Minimum system requirements	11
Supported operating systems	11
Supported file systems	12
Supported internet connection types	12
Supported storage media	13
Installing Acronis True Image	14
Application settings	15
Activating Acronis True Image	15
Too many activations issue	16
Managing your subscription licenses manually	16
Upgrading Acronis True Image	16
Built-in store	18
Uninstalling Acronis True Image	18
Technical Support	19
Getting started	20
User interface language	20
Protecting your system	20
Backing up your computer	20
Creating Acronis bootable media	22
Using WinPE- or WinRE-based bootable media	23
Backing up all data on your PC	23
Creating an Acronis Survival Kit	24
Backing up your files	27
Cloning your hard drive	28
Why do I need it?	28
Before you start	29
Cloning a disk	29
Recovering your computer	30
Acronis account	32
Two-factor authentication (2FA)	33
Getting started with Acronis Cloud	35

How we ensure security of your data	36
Subscription information	36
Licensing	38
Available licenses	38
Reliable data protection: backup, cloning, and recovery features	38
Integrated anti-malware and privacy features	39
Management features	40
Trial version features and limitations	40
General limitations	40
Acronis Cloud during trial	40
Purchasing a subscription to the full version	41
Purchasing and activating a subscription	41
Purchasing a subscription	41
Activating a subscription	42
Deactivating a subscription	42
Transferring your subscription to another account	43
Transferring your subscription to a new computer	43
Troubleshooting activation issues	43
Too many activations	43
Other common activation problems	44
Auto-renewal of subscription	44
Updating the product to the latest version	45
Upgrading your license	45
Changing billing information	46
Basic concepts	47
The difference between file backups and disk/partition images	48
Full, incremental and differential backups	50
Full method	50
Incremental method	50
Differential method	51
Changed Block Tracker (CBT)	52
Deciding where to store your backups	53
Preparing a new disk for backup	54
FTP connection	54
Authentication settings	55
Acronis Nonstop Backup	56
Nonstop Backup limitations	56

How it works	56
Retention rules	57
Acronis Nonstop Backup data storage	57
Nonstop Backup - Frequently asked questions	58
Backup file naming	59
Naming convention for backup files created in Acronis True Image	59
Naming convention for backup files created before Acronis True Image 2020 (.tib)	59
Integration with Windows	60
Compatibility with Microsoft BitLocker encryption feature	61
Wizards	62
FAQ about backup, recovery and cloning	63
Backing up data	65
Backing up disks and partitions	65
Backing up disks and partitions using bootable media	68
Backing up files and folders	68
Backing up mobile devices	70
Acronis Mobile	71
Local destination of mobile backups	72
Backing up Microsoft 365 data	72
Why back up Microsoft 365 data?	72
Backing up Microsoft 365 data	73
Backup options	74
Scheduling	74
Backup schemes	77
Notifications for backup operation	83
Excluding items from backup	85
Image creation mode	87
Backup protection	87
Online backup protection	88
Pre/Post commands for backup	89
Backup splitting	90
Backup validation option	90
Removable media settings	91
Error handling	92
File-level security settings for backup	93
Computer shutdown	94
Performance of backup operation	94

Selecting a data center for backup	96
Laptop power settings	96
Wi-Fi networks for backup to Acronis Cloud	97
Operations with backups	97
Backup operations	97
Backup activity and statistics	100
Sorting backups in the list	103
Validating backups	103
Backup to various places	104
Adding an existing backup to the list	105
Notarized backup	105
Deleting backups and replicas	110
Cleaning up backups, backup versions, and replicas	111
Recovering data	114
Recovering disks and partitions	114
Recovering your system after a crash	114
Recovering partitions and disks	126
About recovery of dynamic/GPT disks and volumes	139
Arranging boot order in BIOS or UEFI BIOS	142
Disk recovery from Cloud	143
Recovering files and folders	148
Searching backup content	150
Recovering Microsoft 365 data	151
What items can be recovered?	151
Recovering Microsoft 365 data	151
Recovery options	152
Disk recovery mode	152
Pre/Post commands for recovery	152
Validation option	153
Computer restart	154
File recovery options	154
Overwrite file options	155
Performance of recovery operation	155
Notifications for recovery operation	156
Online Dashboard and Acronis Cloud	159
What is Online Dashboard?	159
Adding a new device to Online Dashboard	159

Backing up data remotely	160
Recovering data with Online Dashboard	161
Email notifications	161
Replicating backups to Acronis Cloud	162
Why replicate?	162
Replication activation	162
Cleaning up space on Acronis Cloud	163
Removing data from Acronis Cloud	163
Deleting an entire backup	163
Deleting the versions of a backup to cloud	164
Deleting the versions of a backup replica to cloud	164
One-time cleanup	165
Protection	166
The Protection dashboard	166
Active protection	167
Anti-ransomware protection	167
Real-time Protection	168
Web filtering	169
Configuring Active Protection	169
Identity protection	171
Antivirus scans	172
Configuring Antivirus scans	173
Vulnerability assessment	174
Patch management	175
Automatic patch installation	176
Manual patch installation	176
Viewing patch installation results	177
Troubleshooting patch installation	177
Managing detected issues	177
Managing files in Quarantine	178
Configuring Protection exclusions	178
Videoconference app protection	179
Downloading Protection updates	179
Archiving data	181
What is data archiving?	181
What is excluded from archives?	182
Cloud archiving vs. Online backup	182

Archiving your data	183
Data archiving options	184
Accessing your archived files	185
Sharing data	186
Disk cloning and migration	187
Disk cloning utility	187
Clone Disk wizard	188
Manual partitioning	189
Excluding items from cloning	191
Migration method	193
Migrating your system from an HDD to an SSD or NVMe drive	199
Target drive size	199
Which migration method to choose	199
What to do if Acronis True Image does not recognize your SSD or NVMe drive	199
Migrating to an SSD or NVMe drive using the backup and recovery method	200
Tools	202
Acronis Cloud Backup Download	202
Acronis Media Builder	203
Creating Acronis bootable media	204
Acronis bootable media startup parameters	206
Adding drivers to an existing .wim image	207
Creating an .iso file from a .wim file	208
Making sure that your bootable media can be used when needed	209
Selecting video mode when booting from the bootable media	213
Acronis Startup Recovery Manager	215
Additional information	216
Try&Decide	217
When Try&Decide can help	217
How Try&Decide works after a computer restart	217
Limitations in using Try&Decide	218
Using Try&Decide	219
Try&Decide options and notifications	220
Try&Decide: typical use cases	221
Acronis Secure Zone	222
Acronis Secure Zone cleanup	223
Creating and managing Acronis Secure Zone	223
Acronis Secure Zone location	224

Size of Acronis Secure Zone	225
Acronis Secure Zone protection	226
Removing Acronis Secure Zone	227
Adding a new hard disk	227
Selecting a hard disk	227
Selecting initialization method	228
Creating new partitions	229
Security and Privacy Tools	232
Acronis DriveCleanser	232
System Clean-up	237
Mounting a backup image	244
How to mount an image	245
Unmounting an image	246
Working with .vhd(x) files	246
How to use .vhd(x) files	246
Limitations and additional information	246
Converting Acronis backup	247
Importing and exporting backup settings	247
Acronis Universal Restore	248
What problem does it solve?	248
How do I use it?	249
Creating Acronis Universal Boot media	249
Using Acronis Universal Restore	251
Troubleshooting	253
Resolving the most frequent issues	253
Acronis System Report	253
Acronis Smart Error Reporting	255
When you have an internet connection	255
When you do not have an internet connection	255
Sending feedback to Acronis	255
How to collect crash dumps	257
Log files	257
Log retention rules	258
Firewall settings	258
Glossary	260
Index	264

Copyright statement

© Acronis International GmbH, 2003-2026. 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?

Acronis True Image 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.

For an overview of basic system protection steps, see [Protecting your system](#).

Online backup¹ 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.

Key features:

- [Disk backup to a local storage and to Acronis Cloud](#)
- [File backup to a local storage and to Acronis Cloud](#)
- [Antivirus and Anti-malware Protection](#)
- [Acronis bootable media](#)
- [Hard disk cloning](#)
- [Data archiving](#)
- [Online dashboard](#)
- [Security and privacy tools](#)

Note

You cannot create backups to Acronis Cloud with Acronis Startup Recovery Manager and Acronis bootable media.

Backups created before Acronis True Image 2020

Acronis True Image uses the .tibx backup format for new backups. The previously used .tib format is applicable to older backups.

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

To compare naming of current .tibx archives with older .tib archives, see [Backup file naming](#).

¹A backup whose destination is Acronis Cloud. Online backups are stored remotely and accessible over the Internet.

See [Cleaning up backups, backup versions, and replicas](#) for more details about the cleanup.

System requirements and supported media

Minimum system requirements

Acronis True Image requires the following hardware.

- Intel CORE 2 Duo (2 GHz) or equivalent processor that supports SSE instructions.

Note

Acronis True Image supports only 64-bit (x64) editions of Windows. Devices running Windows on ARM processors (such as some lightweight laptops and tablets) are not supported.

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

Warning!

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

Other requirements

- An internet connection is required for the product activation, for downloading protection updates, and for all features that use Acronis Cloud.
- You need to have administrator privileges to run Acronis True Image.

Supported operating systems

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

- Windows 11 (including 25H2)
- Windows 10 (64-bit only)

Note

Acronis True Image 2026 and later cannot be installed on 32-bit Windows operating systems. If you use an earlier version of Acronis True Image on 32-bit Windows, you can continue using the installed version.

Note

- Beta builds are not supported. See [Windows Insider Preview builds support](#).
 - Windows Embedded, IoT editions, Windows 10 LTSC, Windows 10 LTSC, and Windows 10 in S mode are not supported.
-

Acronis True Image 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

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

Supported internet connection types

The table below shows which internet connection types are supported by the product functions.

Note

If there is no internet connection, cloud-related actions (for example, replication and searching/recovering from Acronis Cloud) may be unavailable or fail with a **No Internet connection** error until connectivity is restored.

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.

	internet connection type				
	Acronis Console in Windows		Acronis bootable media		
	Any connection established in Windows	Proxy server	Ethernet cable	Wi-Fi	Proxy server
Disk-level and file-level backup to Acronis Cloud	+	-	-	-	-
Disk-level recovery from Acronis Cloud	+	-	+	+	-
File-level recovery from Acronis Cloud	+	-	-	-	-
Data synchronization	+	-	-	-	-
Product activation	+	-	-	-	-
Product update	+	- *	-	-	-

* - To update the product, download the newer product version from the Acronis website and install it over your current one.

Supported storage media

- Hard disk drives (HDD)
- Solid-state drives (SSD, including NVMe)
- FTP servers

Note

The FTP server must allow passive mode file transfers. Acronis True Image splits a backup into files with a size of 2GB when backing up directly to an FTP server. Working with .tibx backups over FTP is not supported.

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

Limitations on operations with dynamic disks

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

To install Acronis True Image

1. Download the Acronis True Image setup file from the Acronis website at <https://go.acronis.com/true-image>.
2. Run the setup file.
Before starting the setup process, Acronis True Image will check for a newer build on the website. If there is one, the newer version will be offered for installation.
3. Select the installation mode:
 - Click **Install** for the default installation.
 - Click **Custom installation** to choose the required components.
 - **Backup and core protection.** This component is essential for:
 - "Backing up data" (p. 65)
 - "Recovering data" (p. 114)
 - "Vulnerability assessment" (p. 174)
 - "Archiving data" (p. 181)
 - "Sharing data" (p. 186)
 - "Disk cloning and migration" (p. 187)
 - "Tools" (p. 202)
 - **Anti-ransomware protection, Cryptomining detection, and Videoconference protection.** For more information, see "Active protection" (p. 167).
 - **Real-time protection, Antivirus scan, and Web filtering.** For more information, see "Active protection" (p. 167) and "Antivirus scans" (p. 172).
 - **Try&Decide tool.** If you're using the Memory integrity feature of Windows, do not install this component to avoid compatibility issues. For more information, see "Try&Decide" (p. 217).

Note

If you install only **Backup and core protection** (without Active Protection / Real-time protection), the **Protection** area may show that Active Protection is turned off and may display prompts to install the missing protection components.

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

4. When the installation is complete, click **Start application**.
5. Read and accept the terms of the license agreement.
6. [Optional] **Allow Acronis to collect de-identified service usage information for analyzing and improving the service**

If you agree to participate, Acronis will anonymously collect technical information to improve Acronis True Image. Personal data, such as name, address, phone number, email address, and keyboard input, will not be collected.

7. In the **Activation** window, you can do one of the following:
 - To activate Acronis True Image, enter your serial number, and then click **Activate**. The product will be activated.
 - To sign in to your Acronis account, click **Sign in**. See [Acronis account](#) for details.
 - To use the trial version, click **Start trial**.

Application settings

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

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

The following settings are available:

- **Interface language**
Select a preferred language from the list.
- **Application startup**
 - **Automatically check for updates at startup**
See [Installing and uninstalling Acronis True Image](#) for details.
- **Customer insights**
 - **Allow Acronis to collect de-identified service usage information for analyzing and improving the service**
If you agree to participate, Acronis will anonymously collect technical information to improve Acronis True Image. Personal data, such as name, address, phone number, email address, and keyboard input, will not be collected.
- **Show personalized offers**
Select this check box to receive personalized offers about products and features.
- **Backup settings transfer**
 - To import the backup settings**
 - Select **Import settings from file**, and then show the path to the script files with the settings.
 - To export the backup settings**
 - Select **Save settings to file**, and then browse for the destination to save the script files with the settings.

Activating Acronis True Image

To use Acronis True Image, you need to activate it via the internet. Without activation the fully functional product works for 30 days. If you do not activate it during that period, all the program functions become unavailable except the recovery.

If your computer is connected to the internet, the product will be activated automatically.

Offline activation is not available in this version of Acronis True Image.

If your computer is not connected to the internet, or if Acronis True Image cannot connect to Acronis Activation Server, wait until internet connection is available, return to activation, and then click **Try again** on the **Account** tab.

Too many activations issue

Possible reasons for the "Too many activations" issue:

- **You exceed the maximum number of computers with installed Acronis True Image.**

For example, you have one license or a serial number for one computer and you install Acronis True Image on a second computer.

Solutions:

- Enter a new serial number. If you do not have one, you can buy it in the Acronis built-in store or at the Acronis website.
- Move the license to your new computer from another one on which the product is already activated. To do this, select the computer from which you want to move the license. Note that Acronis True Image will be deactivated on that computer.

- **You reinstall Windows or change hardware of your computer.**

For example, you might upgrade motherboard or processor in your computer. Activation is lost, because Acronis True Image sees your computer as a new one.

Solution:

To reactivate Acronis True Image on your computer, choose from the list the same computer by its old name.

Managing your subscription licenses manually

If you use the subscription-based version of Acronis True Image, you can manage the licenses manually at the Acronis website. You can do the following:

- Move licenses between your computers
- Transfer licenses between your accounts
- Remove a license from a computer
- Resolve product activation conflicts, including the "Too many activations" issue
- Buy new licenses

To manage licenses

1. Go to <https://account.acronis.com/>, and then sign in with your Acronis account.
2. In the **Products** section, find Acronis True Image, and then click **Manage**.

Upgrading Acronis True Image

When an update for Acronis True Image is available at the Acronis website, you can download it. If you currently have Acronis True Image 2017 or later, the new version will simply update it; there is

no need to remove the old version and reinstall the software.

If your current version is older than 2017, we recommend that you remove the current version first.

Note

Please note that uninstalling the previous version will remove all product settings and configuration.

Before uninstalling, we recommend that you review your backup settings, such as backup destinations, schedules, and encryption options. Saving screenshots or writing down important settings can help you quickly reconfigure the product after installing the new version.

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

The backups created by a more recent program version may be incompatible with previous program versions. If you roll back Acronis True Image to a previous version, you likely will have to re-create the backups using the older version. We strongly recommend that you create new bootable media after each Acronis True Image upgrade.

Acronis True Image is available only as a subscription. Purchasing a subscription gives you access to all features, updates, and technical support for the duration of your subscription period.

To purchase a subscription or to upgrade to a more advanced type of subscription to Acronis True Image

1. Start Acronis True Image.
2. On the sidebar, click **Account**, and then click **Buy full version**. The built-in store opens.
3. Select the license that you want to buy, the number of devices you want to protect, and then click **Buy now**.
4. Review your order, select additional services, if needed, provide your payment information, and then click **Buy now**.

To update Acronis True Image

1. Start Acronis True Image.
2. On the sidebar, click **Account**.
If there is a new version available, you will see the appropriate message next to the current build number.
3. Click **Download and install**.

Note

Before you start downloading, make sure that your firewall won't block the download process.

4. When the new version is downloaded, click **Install now**.

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

To purchase the full version

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

To update Acronis True Image

1. Start Acronis True Image.
2. On the sidebar, click **Account**.
If there is a new version available, you will see the appropriate message next to the current build number.
3. Click **Download and install**.

Note

Before you start downloading, make sure that your firewall won't block the download process.

4. When the new version is downloaded, click **Install now**.

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

Built-in store

Acronis True Image provides an in-app store. Using this store, you can:

- Buy the full version of Acronis True Image.
- Buy Acronis True Image subscription.
- Buy more storage space on Acronis Cloud.

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

Uninstalling Acronis True Image

To add or remove components of Acronis True Image

1. Click **Start > Settings > Apps > Acronis True Image > Modify**.
2. In the installer, click **Modify**. Then, select or clear the check boxes for the required components.
You may have to restart your computer to complete the task.

To uninstall Acronis True Image

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

Note

If you used the "Acronis Secure Zone" (p. 222) or "Acronis Nonstop Backup" (p. 56), select in the window that appears what to do with the zone and Nonstop Backup storages.

Technical Support

If you need assistance with Acronis True Image, see <https://www.acronis.com/support/>.

Note

Before contacting support, prepare your product version, a description of the issue, and (if possible) a System Report and log files. A System Report can be generated and saved to a local disk or a network share for later upload. See [Log files](#) for details.

You can also use **Send Feedback** to submit a report with attachments (for example, a screenshot) and an attached System Report.

If Windows does not boot, you may be able to collect a System Report from the recovery environment and save it to a USB drive.

Getting started

User interface language

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

Note

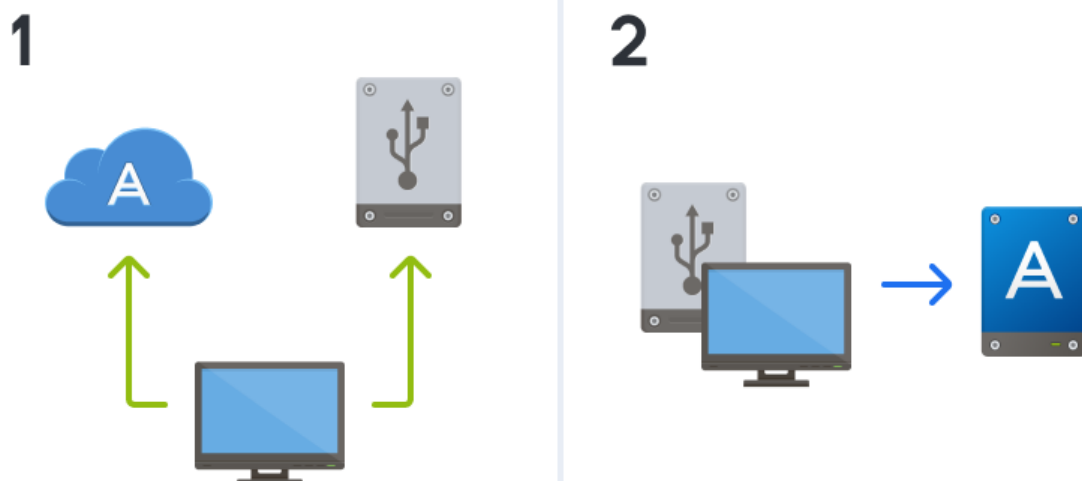
After you change the interface language, Acronis True Image may restart (or prompt you to restart) to apply the change. After that, Help can open in the selected language. Also, bootable media you create may use the language that was selected in Acronis True Image at the time you created the media.

To change the user interface language

1. Start Acronis True Image.
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 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. See [Backing up all data on your PC](#) for details.

- **System disk backup**

You can choose to back up your system partition or the entire system drive. See [Backing up disks and partitions](#) for details.

We do not recommend using nonstop backup as a primary way to protect your system, because the main purpose of this technology is protection of frequently changed files. For the safety of your system, use any other schedule. See examples in "Examples of custom schemes" (p. 82). See "Acronis Nonstop Backup" (p. 56) for more details about the Nonstop Backup feature.

To back up your computer

1. Start Acronis True Image.

2. On the sidebar, click **Backup**.

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

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

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

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

5. Click **Back up now**.

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

Where do I store my disk backups?

- **Good** – Your ordinary internal hard disk.
- **Better** – [Acronis Secure Zone](#). This is a special secure partition on your local hard drive for storing backups.
- **The best** – [Acronis Cloud](#) or an external hard disk.

See [Deciding where to store your backups](#) for details.

How many backup versions do I need?

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

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

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

Note

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

Creating Acronis bootable media

Acronis bootable media is a CD, DVD, USB flash drive, or other removable media from which you can run Acronis True Image 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/NVMe external drive).
2. Start Acronis True Image.
3. On the sidebar, click **Tools**, and then click **Rescue Media Builder**.
4. On the first step, select **Simple**.
5. Select the device to use to create the bootable media.
6. Click **Proceed**.

To use Acronis bootable media

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

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

See [Arranging boot order in BIOS](#) for details.

3. Boot your computer from the bootable media and select **Acronis True Image**.

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

See [Acronis Media Builder](#) for details.

Using WinPE- or WinRE-based bootable media

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

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

When you boot your computer from this media, the recovery procedure is the same as described in [Recovering your computer](#).

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

Backing up all data on your PC

What is an Entire PC backup?

In Acronis True Image, an **Entire PC backup** is similar to an **Entire machine backup** in enterprise products such as Acronis Cyber Protect. It creates a full image of your computer, including the operating system, system files, applications, and all user data across all internal drives.

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

To enhance backup speed, a local cache technique is used to accelerate network access to data files. This technique involves caching data on the client side rather than on servers whenever possible. The effect of local caching is that it eliminates unnecessary multiple read operations across the network and increases the backup speed by up to 20%, based on internal tests.

The local cache technique is implemented for cloud backups and is not used for other backups.

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

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

You can also recover specific files and folders from an Entire PC backup. See [Backing up files and folders](#) for details.

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

To create an Entire PC backup

1. Start Acronis True Image.
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.
We recommend that you back up your computer to Acronis Cloud or to local or network storage. See [Deciding where to store your backups](#) for details.
6. [optional step] Click **Options** to set the options for the backup. For more information see [Backup options](#).
7. Click **Back up now**.

Note

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

Additionally, watch the English-language video instructions at <https://goo.gl/KjW5sM>.

See also [Difference between Backup and Disk Clone](#)

Creating an 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. Most often these components are separated, for example, the system backup is stored on an external drive or Acronis Cloud and the bootable media is a small USB flash drive. An Acronis Survival Kit combines both components so that you could have a single device that has everything that you need to recover your computer in case of a failure. It is an external hard disk drive that contains both the Acronis bootable media files and a backup of your system partition, entire computer, or any disk backup. Moreover, the backup of your data can be used as a normal backup: it can contain any data that you need to secure, you can set up [Scheduling](#) to update it as a normal backup. And even more, the external hard drive is not exclusively booked

by the Acronis Survival Kit, its bootable media takes 4 GB of the disk space, and the remaining space can be shared by the system partition or entire computer backup which is the part of the Acronis Survival Kit, and by any other data including other backups, your personal data, photos, whatever. But keep only one Acronis Survival Kit on one external hard disk.

No matter how many backups are stored in this external hard disk, only one Acronis Survival Kit is required to recover a computer. Its bootable media component works with any system partition or entire computer backup if they both are created for the same computer or computers with the same configuration.

As a device for an Acronis Survival Kit you can use:

- **an external hard disk drive**

It should be larger than 32 GB and have an NTFS, FAT32, or exFAT file system. If the drive has another file system, Acronis True Image suggests formatting the drive.

Note

exFAT formatted partitions are supported only for disk or partition recovery operations without resizing. Individual file browsing or selective recovery from backups on exFAT partitions is not supported, and such partitions may appear empty when attempting to recover individual files.

- **a USB flash drive**

It should be an MBR flash drive with minimum size of 32 GB. If you use a GPT flash drive, Acronis True Image suggests formatting the drive to MBR. Note, flash drives are supported only for Windows 10 (build 1703 and later) and for Windows 11.

The device you choose for an Acronis Survival Kit must be large enough to store both the bootable media and the backup. For example, if your system partition contains 200 GB of data, a 256 GB drive or larger is required.

The following limitations apply to supported file systems for Acronis Survival Kit:

- NTFS and FAT32 are fully supported for all recovery operations.
- exFAT is supported only for disk or partition recovery operations without resizing.
- Selective recovery of individual files and folders from exFAT partitions is not supported; these partitions may appear empty during browsing.

For optimal performance and compatibility, we recommend using NTFS formatted drives for creating the Survival Kit and storing backups.

The following limitations apply to the use of exFAT formatted drives with Acronis Survival Kit:

- WinRE/WinPE-based bootable media is required to recover system backups stored on an exFAT-formatted disk.
- exFAT is supported only for disk or partition recovery operations without resizing.
- It is not possible to browse and restore individual files and folders selectively from a backup of an exFAT disk volume. exFAT partitions are shown as empty when attempting to browse and recover

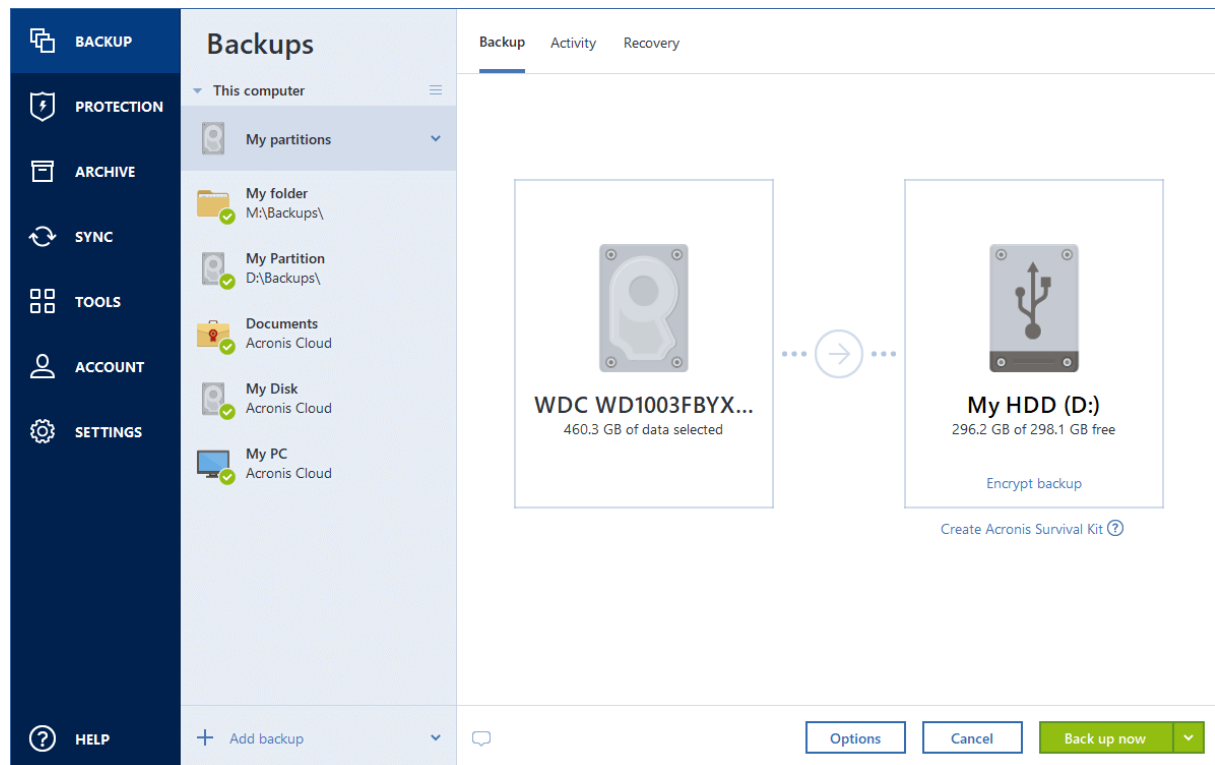
individual files.

- It is possible to restore all files at once in disk/partition recovery mode.

Note

To create an Acronis Survival Kit

When you configure a backup of your system partition, entire computer, or any disk backup and select an external hard disk drive as a destination, Acronis True Image will suggest creating an Acronis Survival Kit.



1. Click **Back up now** or **Create Acronis Survival Kit**.
2. In the opened window, click **Create**.

Acronis True Image creates a small partition on the selected drive and writes the boot files there. To create it, one of the existing volumes will be resized. If the disk is not a GPT one and has a file system different from NTFS, FAT32, or exFAT, Acronis True Image suggests formatting the disk. Pay attention, that disk formatting deletes all the data stored on the disk.

Note

exFAT formatted partitions are supported only for disk or partition recovery operations without resizing. For best results and full recovery capabilities, use NTFS formatted drives when creating the Survival Kit or storing backups.

3. When the boot files are successfully written to the drive, it becomes Acronis bootable media that you can use to recover your computer. To complete creating an Acronis Survival Kit, you need to save a backup of your system partition, entire computer, or any disk backup to this drive. To do

this, click **Back up now**. If you skip this step, do not forget to create a backup on this drive later. See [Backing up disks and partitions](#) for details.

When your Acronis Survival Kit is ready, you can use it to recover your computer. See [Recovering your system to the same disk](#) for details.

Every time you configure a backup to an external device with a Survival Kit on it, Acronis True Image will check its version. If an up-to-date version of the Survival Kit is available, Acronis True Image will suggest updating the Survival Kit on your external device.

Backing up your files

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

- **Local or network storage**

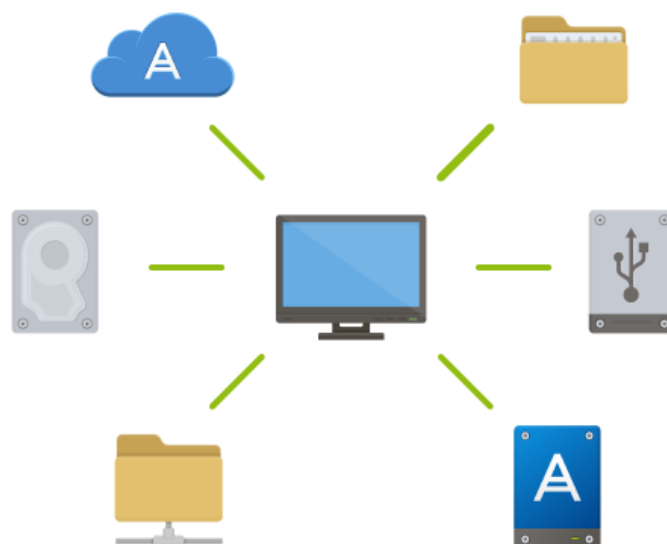
This option is fast and easy. Use it to protect rarely changed files.

- **Acronis Cloud**

This option is reliable. Use it to protect critical files and files that you want to share between devices or people.

To use Acronis Cloud, you must have an Acronis account and a subscription to the Acronis Cloud service.

See "Subscription information" (p. 36) for details.



To back up files and folders

1. Start Acronis True Image.
2. On the sidebar, click **Backup**.
3. Click the **Backup source** icon, and then select **Files and folders**.

4. In the opened window, select the check boxes next to the files and folders that you want to back up, and then click **OK**.
5. Click the **Backup destination** icon, and then select a destination for backup:
 - **Acronis Cloud** – Sign in to your account, and then click **OK**.
 - **Your external drive** – When an external drive is plugged into your computer, you can select it from the list.
 - **NAS** – Select an NAS from the list of found NAS devices. If you have only one NAS, Acronis True Image will suggest using it as a backup destination by default.
 - **Browse** – Select a destination from the folder tree.
6. Click **Back up now**.

See [Backing up files and folders](#) for details.

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

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.

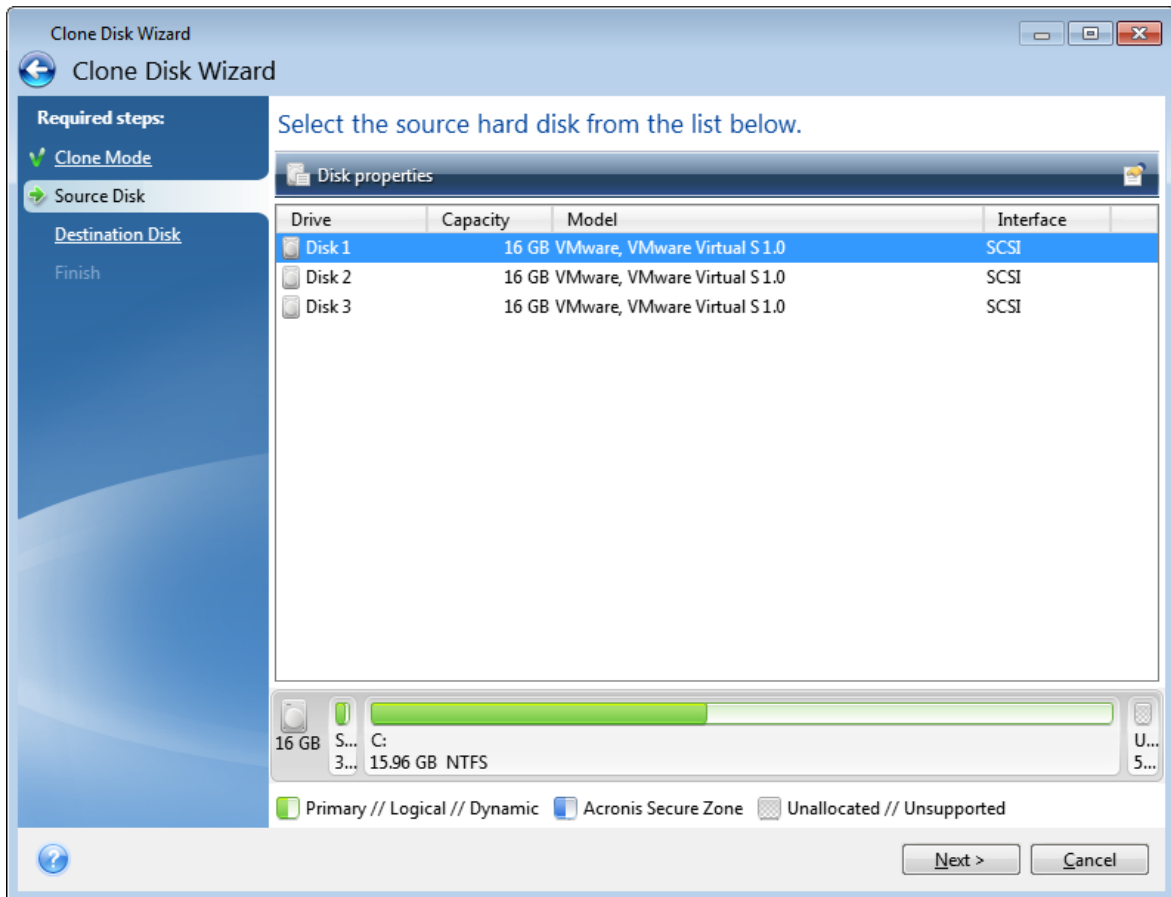
Cloning a disk

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. See [Clone Disk wizard](#) for more details about the manual mode.

Note

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

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



- 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.

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

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

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

Recovering your computer

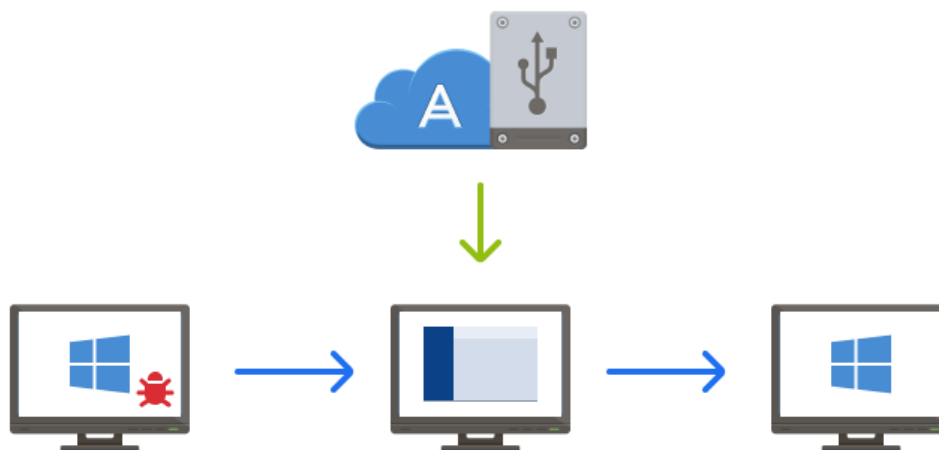
Recovery of a system disk is an important operation. Before you start, we recommend that you read the detailed descriptions in the following Help topics:

- [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.
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?

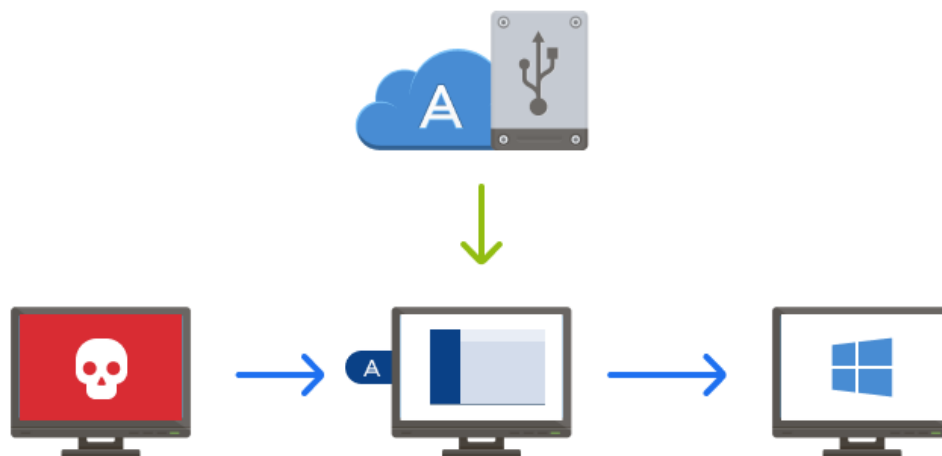


1. Start Acronis True Image.
2. On the sidebar, click **Backup**.
3. From the backup list, select the backup that contains your system disk. The backup can be located on local, network storage, or Acronis Cloud.
4. On the right panel, click **Recovery**.
5. Depending on the backup type, click **Recover 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 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.
See [Step 2 Creating Acronis bootable media](#) and [Arranging boot order in BIOS](#) for details.
Alternatively, you can use [WinPE- or WinRE-based bootable media](#) to recover backups created in Acronis True Image.
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. In the same window, you can connect to Acronis Cloud and select an online backup. See [Recovering your system from Acronis Cloud](#) for details.
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, 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.

Acronis account

An Acronis account is required when you:

- Register an Acronis product.
- Back up to Acronis Cloud.

- Synchronize your data.
- Archive your data.

To create an Acronis account

1. On the sidebar, click **Account**, and then click **Sign in or create an account**.
2. Click **Create an account**.
3. Fill in the registration form. Provide the required data, accept the Terms of Use, and, optionally, subscribe to receive news and promotional offers occasionally.

Note

To keep your personal data secure, choose a strong password for your online backups, guard it from getting into the wrong hands, and change it from time to time.

4. Click **Create account**.
5. An email message will be sent to the address you specified. Open this message and confirm your wish to create an account.

To sign in with your Acronis account

1. On the sidebar, click **Account**, and then click **Sign in** or **Create an account**.
2. Enter your registration email address and password, and then click **Sign in**.

To sign out of your Acronis account

1. On the sidebar, click **Account**.
2. Click your email address, and then choose **Sign out**.

To delete your Acronis account

1. Go to <https://account.acronis.com>
2. Click **Profile**.
The **Profile** window opens.
3. In the **Delete account** section, click the **Delete account** button.
The **Delete profile** window opens.

Important

Once the account is deleted, your personal profile, license keys of all the registered products, as well as all the data stored in Acronis Cloud, will be permanently lost.

4. Click **Proceed to deletion** to confirm that you want to permanently and irreversibly delete your account.

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 build 40713 and later.

To see the build number:

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

- Acronis Mobile for iOS app version 6.2 and later.
- Acronis Mobile for Android app version 6.2 and later.

To set up two-factor authentication for your account

1. Open Online Dashboard at: <https://cloud.acronis.com>.
2. Click 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 sign in using 2FA

1. Sign in using your Acronis credentials.
The **Two-factor authentication** window opens.
2. Enter the 6-digit code displayed on your authenticator app.

Important

Authenticator apps use time-based codes. If the device clock is inaccurate, the codes may not work. Make sure the device with the authenticator app is set to automatic date and time using the network or world clock.

3. Click **Sign in**.

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.
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:

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

Variant 2: Some authenticator apps, like Authy, can back up the 2FA configuration. You can later restore 2FA on a new device from this backup. To do so, install the same authenticator application, log in under the same authenticator app account, and restore the 2FA configuration from this authenticator app backup.

Variant 3: Some authenticator apps, like Microsoft, have the ability to add a recovery account. You can later restore 2FA on a new device by simply signing in using the recovery account. For more information, see support.microsoft.com.

Getting started with Acronis Cloud

Note

Acronis Cloud might be unavailable in your region. For more information, see the [Support Portal](#).

Acronis Cloud is a secure remote storage which you can use to store:

- Backups of your files and folders
- Backups of your partitions and disks
- Versions of your synchronized files and folders

Because files are stored on a remote storage, they are protected even if your computer is stolen or your house burns down. In the case of a disaster or data corruption, you can recover your files and even the entire contents of your computer.

With one account, you can save data from several computers and all your mobile devices running iOS and Android operating systems.

To start using Acronis Cloud, you need a subscription to the service. See [Subscription information](#) for details.

To open Acronis Cloud, go to <https://www.acronis.com/my/online-backup/webrestore/>, and then log in to your Acronis account.

How we ensure security of your data

When you use Acronis Cloud as storage, you want to be sure that your personal files won't get into the wrong hands. You may be especially concerned about your mobile device, because all of your data will be transferred through the internet.

Let us assure you that your data will be safe. First of all, we use encrypted protocols (SSL, TLS) to transfer all data through both the internet and LAN. To access the data, sign in to your account by providing the email address and password for that account. Second, you can choose to use only protected Wi-Fi networks for backing up of your data. In this case, your data will be completely safe while it is transferred to Acronis Cloud. Select the secure [Wi-Fi networks for backup](#) in the **Settings**.

Subscription information

To use Acronis True Image cloud features such as online backup, cloud archiving, and cloud synchronization, you need a subscription to Acronis Cloud Storage.

To subscribe, start Acronis True Image, open the **Account** tab, and select either a trial or full subscription.

Note

Acronis Cloud is subject to our Fair Usage Policy. For more details, see the [Support Portal article](#).

Trial version

When you activate the trial version of the product, your account is automatically assigned 1000 GB of cloud storage and a free Acronis Cloud subscription for the duration of the Acronis True Image trial period. For details, see [Trial version features and limitations](#).

Full version

You can purchase a subscription on the Acronis website or via the built-in store in the product interface.

For details, see [Purchasing and activating a subscription](#).

Licensing

When you start Acronis True Image for the first time, the product prompts you to either enter a license key or sign in to your Acronis account to activate it.

You can find your license key in the email confirmation that you receive after purchasing the product. Make sure to save that email for future reference.

Available licenses

Different license types provide access to different features, cloud storage options, and support levels.

Acronis True Image is available only as a subscription. Purchasing a subscription gives you access to all features, updates, and technical support for the duration of your subscription period.

When a trial or subscription expires, a 30-day grace period applies to data stored in Acronis Cloud. During the grace period, cloud storage is available in recovery-only mode. After the grace period ends, cloud access is disabled and the stored data is deleted.

The following table compares the available license types.

	Trial	Essentials	Advanced	Premium
License type	Trial (free for 30-days)	Subscription (annual commitment)	Subscription (annual commitment)	Subscription (annual commitment)
Number of devices	• Unlimited number of PC/Mac • Unlimited number of mobile devices	• Up to 5 PC/Mac • Unlimited number of mobile devices	• Up to 5 PC/Mac • Unlimited number of mobile devices	• Up to 5 PC/Mac • Unlimited number of mobile devices
Cloud storage	1 TB	0 GB	50GB up to 500GB	1TB to 5TB
Support	Limited support	Email, chat, and phone	Email, chat, and phone	Email, chat, and priority phone

Reliable data protection: backup, cloning, and recovery features

	Essentials	Advanced	Premium
Full image backup	Yes	Yes	Yes
Active disk cloning	Yes	Yes	Yes
File and folder backup	Yes	Yes	Yes

	Essentials	Advanced	Premium
Disk and partition backup	Yes	Yes	Yes
All-in-one recovery drive (Acronis Survival Kit)	Yes	Yes	Yes
Recover to similar or dissimilar hardware	Yes	Yes	Yes
Incremental and differential backups	Yes	Yes	Yes
Backup scheduling	Yes	Yes	Yes
Microsoft 365 backup, including Outlook.com and OneDrive	No	Yes	Yes
Local-to-cloud backups	No	Yes	Yes
Cloud restores	No	Yes	Yes
Automatic mobile backups	Yes	Yes	Yes

Integrated anti-malware and privacy features

	Essentials	Advanced	Premium
Anti-ransomware and cryptojacking * protection	Yes	Yes	Yes
Vulnerability assessments	Yes	Yes	Yes
Videoconference app protection	Yes	Yes	Yes
Real-time anti-malware protection	No	Yes	Yes
Antivirus scans	30-day free trial*	Yes	Yes
Web filtering	30-day free trial*	Yes	Yes
Quarantine and exclusions	30-day free trial*	Yes	Yes
User-defined passwords	Yes	Yes	Yes
Electronic signatures (Acronis ASign)	No	No	Yes
Blockchain notarization (Acronis Notary)	No	No	Yes
Identity protection	No	Yes (US only)	Yes (US only)

Note

*To continue using the feature after the 30-day free trial is over, you must upgrade your license to a higher tier.

Management features

	Essentials	Advanced	Premium
User-friendly cyber protection dashboard	Yes	Yes	Yes
Control backup-on-battery	Yes	Yes	Yes
Back up on preferred Wi-Fi	No	Yes	Yes
CPU load balancing	30-day free trial	Yes	Yes
Protection pause	Yes	Yes	Yes
Tray notification center	Yes	Yes	Yes
Remote data management	No	Yes	Yes

Trial version features and limitations

General limitations

The trial version of Acronis True Image is available for 30 days. During this period, the following limitations apply:

- [Disk cloning](#) is disabled.
- When booting from Acronis bootable media, only the recovery operation is available.
- Acronis Universal Restore is not available in the trial version.

Acronis Cloud during trial

You have 1000 GB of cloud storage space during the trial period. You can use this space to store your online backups¹ and archives.

After the trial expires, a 30-day grace period starts:

- During the grace period, Acronis Cloud switches to recovery-only mode.
- After the grace period ends, Acronis Cloud access is disabled, and all your data stored there is deleted.

¹A backup whose destination is Acronis Cloud. Online backups are stored remotely and accessible over the Internet.

Purchasing a subscription to the full version

You can purchase a subscription on the Acronis website or via the built-in store in the product interface.

For details, see [Purchasing a subscription](#).

Purchasing and activating a subscription

Purchasing a subscription

Acronis True Image is available only as a subscription. Purchasing a subscription gives you access to all features, updates, and technical support for the duration of your subscription period.

Acronis standard licensing policy is based on the number of computers on which Acronis True Image is installed. If multiple operating systems are installed on the computer, only one license is required.

You can purchase a subscription on the Acronis website or via the built-in store in the product interface.

To purchase a subscription via the built-in store

1. Start Acronis True Image.
2. On the sidebar, click **Account**, and then click **Buy full version**. The built-in store opens.
3. Select the license that you want to buy, the number of devices you want to protect, and then click **Buy now**.
4. Review your order, select additional services, if needed, provide your payment information, and then click **Buy now**.

To purchase a subscription on the website

1. Go to <https://acronis.com/#/products/>
2. Select Acronis True Image.
3. Click **Buy now** to see the available subscription options.
4. Select the subscription plan that fits your needs.
5. Select the number of computers you want to protect.
6. If you select an Advanced or Premium subscription, choose the amount of Acronis Cloud storage.
7. Click **Buy now**.
8. Provide your payment information and the email address where you want to receive the license details.
9. Click **Review and buy**.

Activating a subscription

To use Acronis True Image, you must activate your serial number on each computer that you want to protect. Without an activated subscription, the product remains fully functional for 30 days in trial mode. If you do not activate it during that period, all features except recovery become unavailable.

The first time your computer is connected to the internet and you log in to Acronis True Image with your login and password, the product will be activated automatically.

Note

An internet connection is required to activate Acronis True Image subscriptions (Essentials, Advanced, and Premium editions).

To activate your subscription

1. Open Acronis True Image.
2. Enter the license key received on your email address when you bought your subscription.
3. Click **Activate**.

Note

An Acronis account is automatically created using the email that you specified during the purchase. If you used an existing account, the subscription will be registered there automatically.

Note

If you encounter problems during activation, such as exceeding the number of allowed activations, see [Troubleshooting activation issues](#) for detailed instructions.

Deactivating a subscription

If you no longer use Acronis True Image on a specific computer, you can manually free up the subscription on that computer in your Acronis account.

Deactivating a computer does not cancel your subscription. When your subscription expires, a 30-day grace period applies to data stored in Acronis Cloud: during this period, cloud storage is available in recovery-only mode; after the grace period ends, cloud access is disabled and the stored data is deleted.

To deactivate a subscription on a computer

1. Go to <https://account.acronis.com/#/products/> and sign in to your Acronis account.
2. Under the subscription, locate the **WORKSTATION** section.
3. Click **Manage** to view the list of registered computers.
4. Click **Deactivate** next to the computer you want to remove.
5. Restart Acronis True Image so the updated license status is applied.

Note

The **Manage** button appears only if there is at least one computer registered under your subscription. If no computers are currently using the license, this option is hidden.

Transferring your subscription to another account

If you already have an Acronis True Image subscription registered under your account and purchase another subscription using the same email address, a conflict may occur. In this case, you need to transfer one of the subscriptions to a different account.

To transfer a subscription to another account

1. Go to <https://account.acronis.com/#/products/> and sign in to your Acronis account.
2. Locate the newly purchased subscription with a conflict.
3. Click **Transfer to another account** and confirm the transfer.

Transferring your subscription to a new computer

If your Acronis True Image subscription is activated on a computer that you no longer use (for example, it is broken or replaced), you can transfer the subscription to a new computer.

When activating the subscription on the new computer, you may see the error message **You've exceeded the maximum number of activations for this serial number**. This means the subscription is still assigned to the previous computer and must be deactivated.

To transfer your subscription to a new computer

1. If possible, uninstall Acronis True Image from the old computer.
2. Disconnect the old computer from the internet.
3. Download and install Acronis True Image on the new computer.
4. Open the product and sign in to your Acronis account.
5. Select the **Account** tab and check the activation status.
6. If the message **You've exceeded the maximum number of activations for this serial number** appears, click **Resolve problem** and follow the on-screen instructions.

For Acronis True Image 2016 and earlier versions, see the instructions in the corresponding product documentation.

Troubleshooting activation issues

Too many activations

This error appears when you've reached the maximum number of computers allowed under your subscription. This can occur after reinstalling the operating system, upgrading hardware, or moving Acronis True Image to a new computer.

To continue using the product, deactivate the subscription on a computer you no longer use.

To deactivate the subscription from an unused computer

1. Open Acronis True Image.
2. Select the **Account** tab.
3. Click **Resolve problem** next to the activation alert.
4. Click **Manage** in the **WORKSTATION** section of your subscription.
5. Click **Deactivate** next to the computer you no longer use.
6. Restart Acronis True Image to apply the changes.

Note

If no computers can be deactivated and you need to add another one, select the **Account** tab and click **Upgrade** to add more workloads to your subscription.

Other common activation problems

Ensure your computer is connected to the internet and that you're signed in with the correct Acronis account. If the issue persists, contact [Acronis Support](#).

Auto-renewal of subscription

Subscription-based products purchased on the Acronis website have the auto-renewal option enabled by default. This means you are automatically charged for the next subscription period, and your subscription is extended for another year.

To disable auto-renewal

1. In the purchase confirmation email, go to the **Manage your subscription** section. There is a separate link for each subscription in the order.
2. Select your subscription.
3. If auto-renewal is enabled, the **Cancel your subscription** option is available.
4. Click **Cancel your subscription** to turn off auto-renewal for the selected subscription.

Note

When you turn off auto-renewal, any future renewal charges are canceled. This action does not result in a refund of your existing order.

To enable auto-renewal

1. In the purchase confirmation email, go to the **Manage your subscription** section. There is a separate link for each subscription in the order.
2. Select your subscription.
3. If auto-renewal is disabled, the **Reactivate it yourself** option is available.
4. Click **Reactivate it yourself**.
5. Check your email for a renewal confirmation message.

6. Click the **Confirm renewal** button in the email.
A confirmation email will be sent to the address you used when purchasing the subscription.

Updating the product to the latest version

If you have an active Essentials, Advanced, or Premium subscription, all new product updates are available to you at no additional cost during your subscription period. To install an update, simply sign in to Acronis True Image installed on your computer. No additional serial number is required. Acronis True Image automatically detects available new versions and updates, notifies you, and offers to install them.

You can continue using the updated version until your current subscription expires. If more updates are released before that, you can install them as well.

You can also switch to a different subscription plan. For details, see [Upgrading your license](#). You can upgrade at any time, while downgrading is only available after your current subscription expires.

Upgrading your license

Acronis True Image is available only as a subscription. Purchasing a subscription gives you access to all features, updates, and technical support for the duration of your subscription period.

You can upgrade your subscription at any time to include more features or protect more computers. Any remaining days from your current subscription will be automatically transferred to the new one.

To upgrade your license using Acronis True Image

1. Open Acronis True Image.
2. Select the **Account** tab. The **Account** window opens.
3. Click **Upgrade**.
4. Select the number of computers to protect.
5. Select the subscription type.
6. If you upgrade to Acronis True Image Premium, select the amount of Acronis Cloud to include with your upgrade.
7. Click **Upgrade now**. The shopping cart opens.
8. Review the details and complete the purchase.
9. Go to your [Acronis account](#).

If you now have two active subscriptions, a conflict warning appears.

To resolve the subscription conflict

1. Click **Resolve conflict**.
2. Select the **Upgrade the current subscription to** checkbox.
3. Click **Resolve**.

Note

After your license expires, you can switch to a plan with fewer features. While your current subscription is active, downgrading is not available.

To learn how to get product updates while your subscription is active, see [Updating the product to the latest version](#).

Changing billing information

If you purchased the subscription in the Online store, and a scheduled auto-renewal payment was missed (for example, because the card was expired or there were not enough funds available in the account), you will receive an automatic notification containing a link to modify the payment method. Click the link and choose a different payment option or change credit card details to activate the auto-renewal.

For more information, see [How to change the payment option for my order?](#)

Basic concepts

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

Backup and recovery

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

Backups are useful primarily for two purposes:

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

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

Recovery methods:

- **Full recovery** can be performed to the original location or to a new one.
When the original location is selected, the data in the location is completely overwritten with the data from the backup. In case of a new location, the data is just copied to the new location from the backup.
- **Incremental recovery** is performed only to the original location and only from a cloud backup. Before the recovery starts, the files in the original location are compared with the files in the backup by file attributes, such as file size and date of last modification. Those files that do not match are marked for recovery, the remaining files will be skipped during recovery. In that way, as opposed to the full recovery, Acronis True Image recovers only changed files. This method significantly reduces the recovery time and saves internet traffic while recovering from Acronis Cloud.

Backup versions

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

Backup versions represent full, incremental and differential backups - see [Full, incremental and differential backups](#).

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

Disk cloning

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

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

Backup file format

Acronis True Image usually saves backup data in the proprietary .tibx format using compression. These backups are recovered in Acronis True Image (in Windows or in the recovery environment) and are not intended to be opened directly by standard Windows tools. Backups that were created earlier may be in a different format, and they remain recoverable in Acronis True Image.

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

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 opens the backup file, recalculates the checksum values and compares those values with the stored ones. If all compared values match, the backup file is not corrupted.

Scheduling

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

Deleting backups

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

See [Deleting backups and backup versions](#) for details.

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

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

Additionally, when you back up your system partition or disk to Acronis Cloud, Acronis True Image excludes the following data:

- The Temp folders, usually located in:
 - C:\Windows\Temp\
 - C:\Users\<username>\AppData\Local\Temp
- The System Volume Information folder (usually located in C:\System Volume Information\)
- The Recycle Bin
- Web browser temporary data:
 - Temporary internet files
 - Cookies
 - History
 - Cache
- .tib and .tibx files
- .tmp files
- .~ files

Full, incremental and differential backups

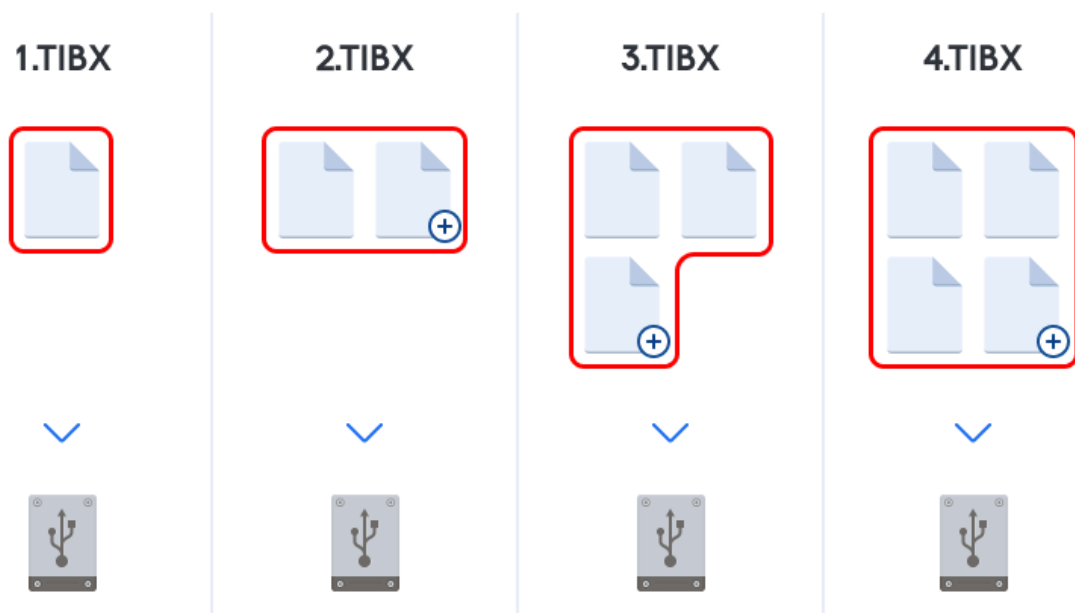
Acronis True Image offers three backup methods: full, incremental, and differential.

Full method

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

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

1.tibx, 2.tibx, 3.tibx, 4.tibx – files of full backup versions.



Additional information

A full backup version forms a base for further incremental or differential backups. It can also be used as a standalone backup. A standalone full backup might be an optimal solution if you often roll back the system to its initial state or if you do not like to manage multiple backup versions.

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

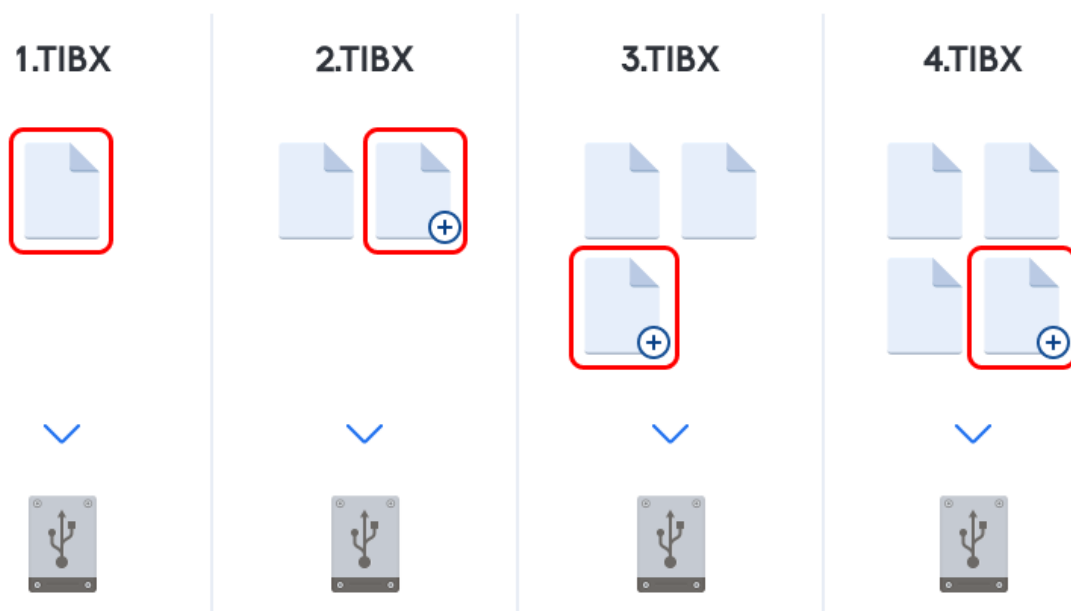
Incremental method

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

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

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

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



Additional information

Incremental method is the most useful when you need frequent backup versions and the ability to roll back to a specific point in time. As a rule, incremental backup versions are considerably smaller than full or differential versions. On the other hand, incremental versions require more work for the program to provide recovery.

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

This applies to lost, corrupted, or manually removed incremental versions. If versions are deleted by using the **Clean up versions** wizard, cleanup behavior depends on backup format and chain consistency.

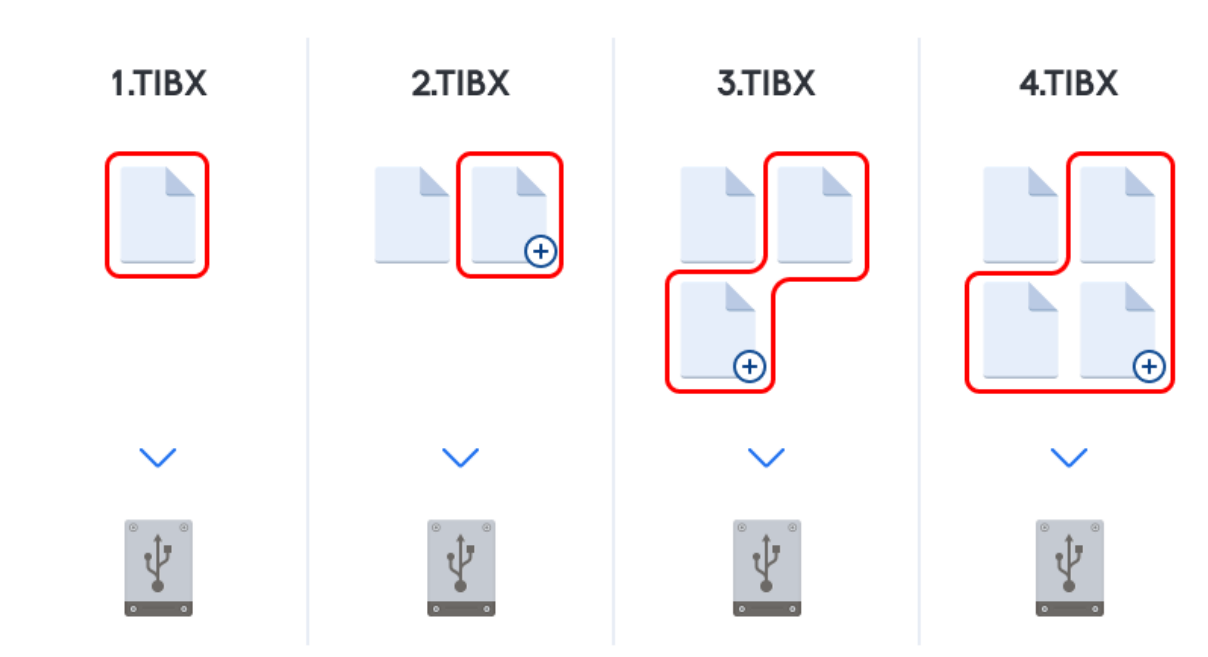
Differential method

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

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

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

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



Additional information

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

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

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

Note

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

Changed Block Tracker (CBT)

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

Deciding where to store your backups

Acronis True Image supports quite a few of storage devices. For more information, see "Supported storage media" (p. 13).

The table below shows possible backup destinations for your data.

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

*Internal or external.

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

Recommended storage media:

1. **Acronis Cloud**
2. **External drive**

If you plan to use an external USB hard drive with your desktop PC, we recommend that you connect the drive to a rear connector by using a short cable.

3. **Home file server, NAS, or NDAS**

Check whether Acronis True Image detects the selected backup storage, both in Windows and when booted from the bootable media.

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

4. **Network share**

See also: [Authentication settings](#).

5. **FTP server**

See also: [FTP connection](#).

6. **Optical discs (CD, DVD, BD)**

Blank optical discs such as DVD-R, DVD+R are very cheap, so they will be the lowest cost solution for backing up your data, though the slowest one.

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

Preparing a new disk for backup

A new internal or external hard drive may not be recognized by Acronis True Image. 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 Tools**, 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 Tools**, 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 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 as an FTP URL (for example: `ftp://my.server.com/backups`)
- 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 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

Working with .tibx backups over FTP is not supported.

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 TCP protocol 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 10, you can find this setting at **Control Panel > Network and Internet > Network and Sharing Center > Advanced sharing settings** > Turn off password protected sharing.

In Windows 11, you can access it at **Settings > Network & internet > Advanced sharing settings**.

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

Acronis Nonstop Backup

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

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

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

Nonstop Backup limitations

- You can create only one nonstop backup.
- Acronis Cloud cannot be used as a destination for a disk-level nonstop backup.
- Windows libraries (Documents, Music, etc.) can be protected with a disk-level nonstop backup only.
- You cannot protect data stored on external hard drives.
- Nonstop Backup and Try&Decide cannot work simultaneously.

How it works

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

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

You may think that at these backup rates the storage will fill in no time. Do not worry as Acronis True Image will back up only so called "deltas". This means that only differences between old and

new versions will be backed up and not whole changed files. For example, if you use Microsoft Outlook or Windows Mail, your pst file may be very large. Furthermore, it changes with each received or sent E-mail message. Backing up the entire pst file after each change would be an unacceptable waste of your storage space, so Acronis True Image backs up only its changed parts in addition to the initially backed up file.

Retention rules

Local backups

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

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

Cloud backups

Acronis True Image keeps only the following backup versions:

- All versions for the last hour
- The first versions of every hour for the last 24 hours
- The first version of every day for the last week
- The first version of every week for the last month
- The first version of every month

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

Acronis Nonstop Backup data storage

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

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

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

When an external hard disk or NAS is unavailable, the Nonstop Backup destination can be an internal disk, including a dynamic one. Keep in mind that you cannot use a partition to be protected as a Nonstop Backup storage. If your computer has a single hard disk drive with a single partition, but you want to use Acronis Nonstop Backup anyway, you can create Acronis Secure Zone and use it as the Nonstop Backup data storage.

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

Nonstop Backup - Frequently asked questions

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

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

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

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

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

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

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

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

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

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

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

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

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

Backup file naming

Depending on the version by which a backup was created, its name will differ.

Naming convention for backup files created in Acronis True Image

A backup file name has only the backup name and an incremental counter. It does not contain any additional information such as backup method, backup chain number, backup version number, or volume number.

A backup name may look like:

1. my_documents.tibx
2. my_documents_0001.tibx
3. my_documents_0002.tibx
4. my_documents_0003.tibx

Full and differential backups are stored in separate files and incremental backups are automatically merged into full backups.

Naming convention for backup files created before Acronis True Image 2020 (.tib)

Note

.tib is a legacy archive format. Backups created in current versions of Acronis True Image use the .tibx format described above.

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. See [Backup splitting](#) for details.

Thus a backup name may look the following way:

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

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

Integration with Windows

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

Acronis True Image integrates the following components:

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

Windows Start menu

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

Acronis True Image button on the taskbar

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

Tray Notification Center

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

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

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

Shortcut menu commands

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

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

File-level recovery in File Explorer

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

Compatibility with Microsoft BitLocker encryption feature

Overview

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

Backing up BitLocker-encrypted drives

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

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

Restoring BitLocker-encrypted drives

When restoring data from a BitLocker-encrypted backup:

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

Cloning BitLocker-encrypted drives

Cloning BitLocker-encrypted drives requires additional steps:

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

System recovery with BitLocker

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

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

Recommendations

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

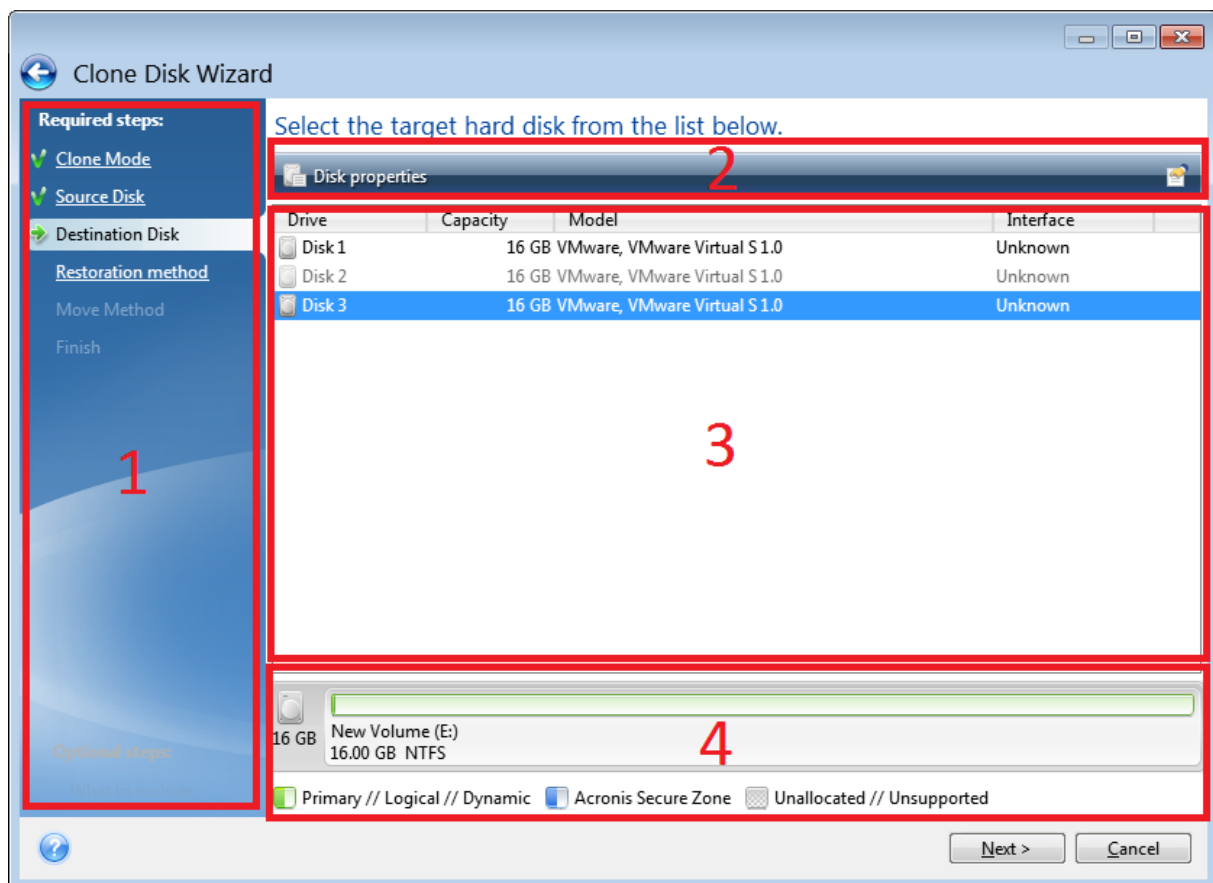
- Unlock and decrypt drives before performing backups or cloning.
- After restoring, allocate time to reapply encryption settings.
- For Windows 11 users, verify encryption settings since BitLocker is enabled by default.

For more details, see [BitLocker Compatibility with Acronis True Image](#).

Wizards

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

For example, see the screenshot below.



A wizard window usually consists of the following areas:

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

FAQ about backup, recovery and cloning

- **I have a 150 GB system partition, but the occupied space on that partition is only 80 GB. What will Acronis True Image include in a backup?** – By default, Acronis True Image 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 or NVMe drive. Can this be done with Acronis True Image?** – Yes, Acronis True Image provides such a function. For procedure details, see [Migrating your system from an HDD to an SSD or NVMe drive](#).
- **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 support RAID?** – Acronis True Image supports hardware RAID arrays of all popular types. Support of software RAID configurations on dynamic disks is also provided. Acronis bootable media supports most of the popular hardware RAID controllers. If the standard Acronis bootable media does not "see" the RAID as a single volume, the media does not have the appropriate drivers. In this case you can create WinPE-based media and add the required drivers there (in the advanced mode).

Backing up data

Backing up disks and partitions

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

Note

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

To back up partitions or disks

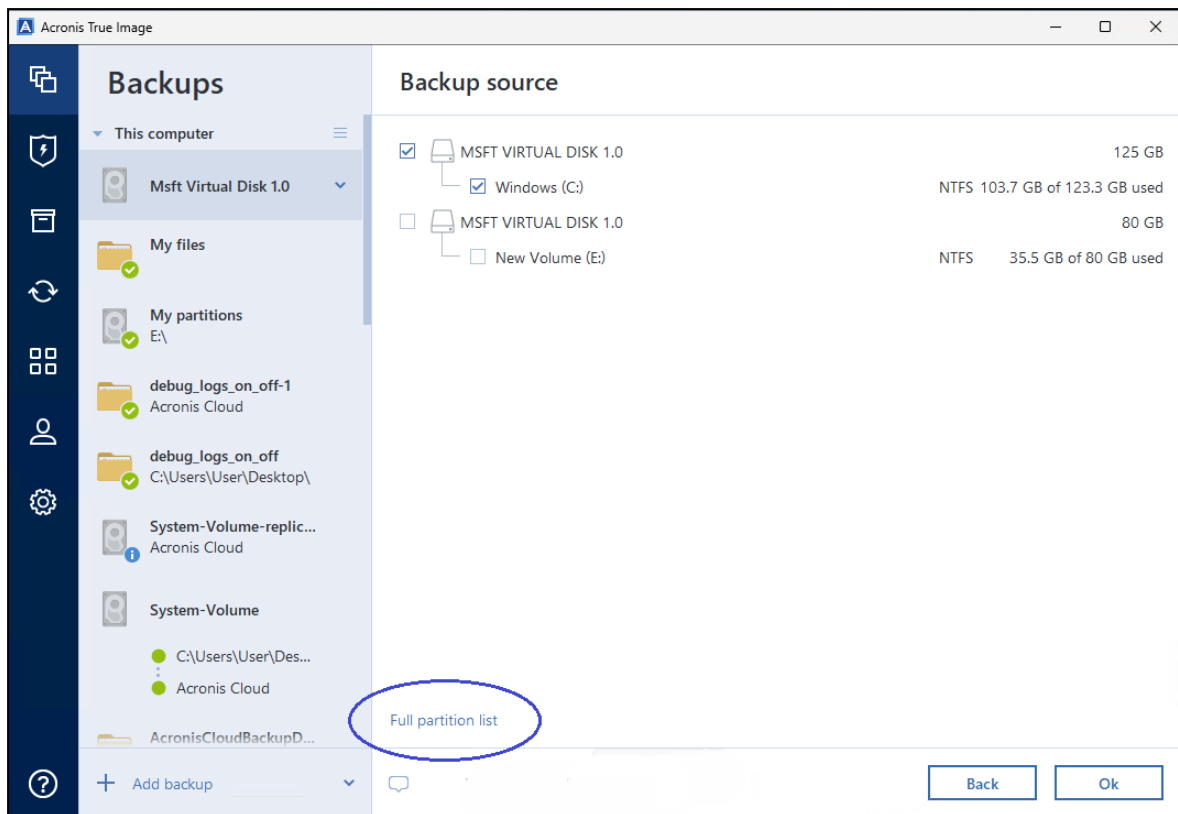
1. Start Acronis True Image.
2. On the sidebar, click **Backup**.
3. Click **Add backup**.
4. [Optional] To rename the backup, click the arrow next to the backup name, click **Rename**, and then enter a new name.
5. Click the **Backup source** area, and then select **Disks and partitions**.
6. In the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

Note

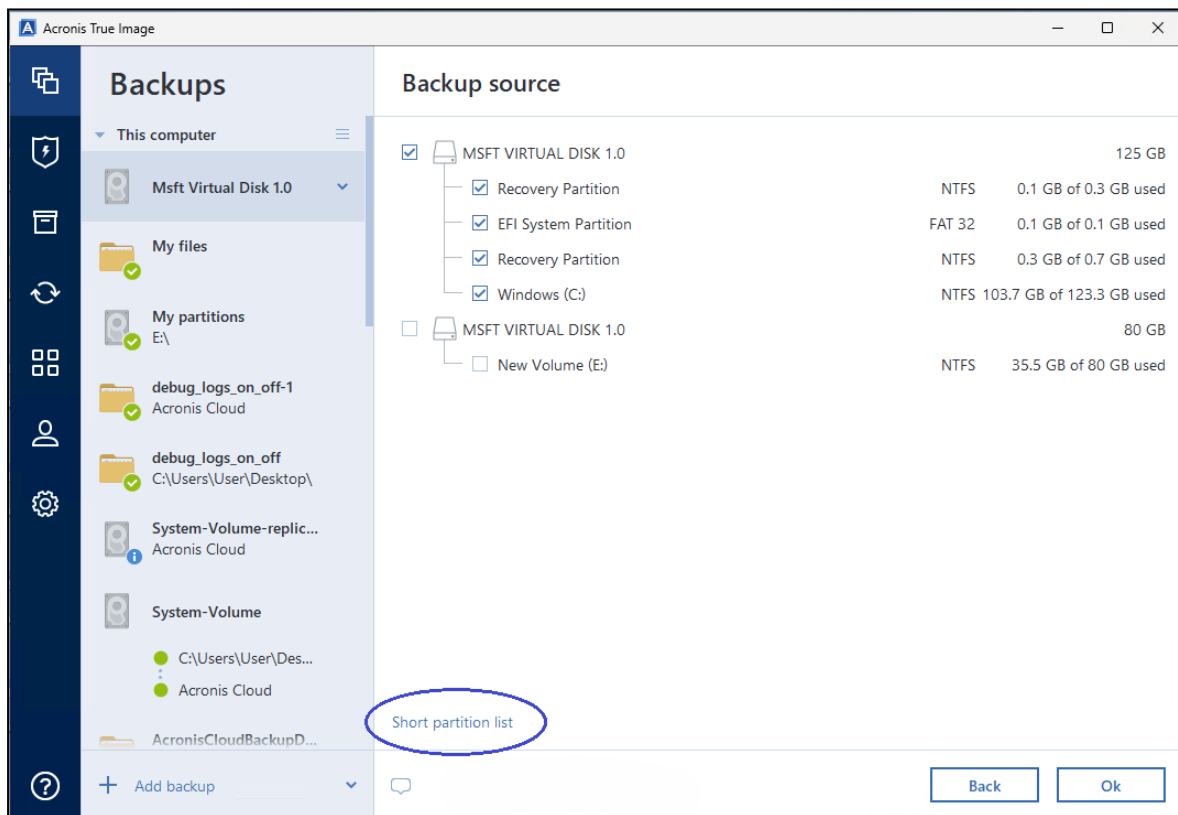
Virtual disks stored on the same volume as the backup source may cause snapshot creation issues and result in backup errors. Avoid this setup for a seamless backup process.

By default, the window opens in **Short partition list** mode, which shows the main disks and partitions for quick selection.

To view all partitions (including hidden/system partitions), click **Full partition list**.



To return to the compact view, click **Short partition list**.



Note

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

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

Note

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

Note

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

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

Example: Testing virtual disk backups

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

Note

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

Backing up disks and partitions using bootable media

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

To learn how to create such bootable media, see [Creating Acronis bootable media](#).

To back up disks or partitions from bootable media:

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

For more details, see the Knowledge Base article: [How to back up with Acronis bootable media](#).

Note

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

Note

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

Note

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

Backing up files and folders

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

To back up files and folders

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

5. Click the **Backup source** area, and then select **Files and folders**.

Important

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

6. In the opened window, select the check boxes next to the files and folders that you want to back up, and then click **OK**.
7. Click the **Backup destination** area, and then select a destination for backup:
 - **Acronis Cloud** – Sign in to your account, and then click **OK**.
If you do not have an Acronis account, click **Create account**, type your email address and password, and then click the **Create account** button. See [Acronis account](#) for details.
 - **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 will suggest using it as a backup destination by default.
 - **Browse** – Select a destination from the folder tree.New **Files and folders** backups to local destinations (for example, external drives) and NAS are created in the **.tibx** format.

These backup files are not intended to be opened directly by standard system tools. Use Acronis True Image to browse and recover data. Backups that were created earlier may be in a different format, and they remain recoverable in Acronis True Image.
8. [Optional] Click **Options** to set the options for the backup. For more information, see [Backup options](#).
9. [Optional] Click the **Add a comment** icon, and then type a comment to the backup version. Backup comments will help you to find the necessary version later, when recovering your data.
10. Perform one of the following:
 - To run the backup immediately, click **Back up now**.
 - To run the backup later or on a schedule, click the down arrow to the right of the **Back up now** button, and then click **Later**.

Note

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

Note

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

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

Backing up mobile devices

If you have an iOS or Android smartphone, you can use Acronis True Image to protect your mobile data such as photos, video files, contacts, and calendars.

See [Acronis Mobile documentation](#) for details.

Before you start a backup, choose where you want to store the backup: Acronis Cloud or local storage on your computer. You can change the destination later, but you cannot back up to both destinations simultaneously. To back up the data to Acronis Cloud, use the Acronis Mobile app. See [Backing up your mobile device to Acronis Cloud](#) for details.

To back up mobile data to local storage on your computer

1. Make sure that:
 - Acronis True Image (2017 or later) is installed on your computer.
 - The Acronis Mobile app is installed on your mobile device.
 - Your mobile device and your computer are connected to the same Wi-Fi network.
2. On your computer:
 - a. Start Acronis True Image (2017 or later).
 - b. On the sidebar, click **Backup**, and then click **Add backup**.
 - c. Click the **Backup source** area, and then select **Mobile device**.
A QR code will be displayed. Please do not close this window.
3. On your mobile device:
 - a. Start Acronis Mobile.
 - b. Tap a plus icon to create a backup. Note that this step does not occur the first time you back up your mobile device.
 - c. Select computer as a backup destination.
 - d. Tap **Scan QR code**, point your camera at the QR code on the computer screen, and then wait until the mobile device is connected to the computer.
 - e. Select the data categories that you want to back up, or tap **Confirm** if you want to back up all of them.
 - f. Allow Acronis Mobile to access to your personal data.
 - g. [optional step] Enter a password to encrypt the backup and protect it. Otherwise, tap **Skip Encryption**.
 - h. Tap **Start Backup**.

When the backup is started, you can track the progress in any application - on the computer or mobile device, but the errors and warning messages are displayed in the mobile app only.

You can close both Acronis True Image on your computer and the Acronis Mobile app. The backup will continue in the background mode.

If you want data changes (for example, new photographs) to be backed up automatically, make sure the **Continuous backup** setting is turned on. If this setting is turned off, the new data is backed up only when you tap **Back up**. See [Mobile app settings](#) for details.

When you change a mobile backup destination from local storage to Acronis Cloud, the connection between the mobile device and the computer is lost, and Acronis True Image stops associating the mobile backup in the list with the mobile device. Then, if you want to change the destination back to local storage, you will need to restore this connection. The connection may also be lost because of an error. To restore it, select the mobile backup in the backup list of Acronis True Image, click **Reconnect**, and then scan the QR code with your mobile device. After that, the backup will continue normally with the same settings.

Acronis Mobile

Note

Acronis Cloud might be unavailable in your region. For more information, see [Acronis Cloud List of supported countries](#).

Acronis Mobile allows you to back up your data to Acronis Cloud, to local storage on your computer, and then recover it in case of loss or corruption. Note that backup to the cloud storage requires an Acronis account and Acronis Cloud subscription.

Which devices does the mobile app support?

You can install Acronis Mobile on any mobile devices that runs one of the following operating systems:

- iOS 17 to iOS 26 (iPhone, iPod, iPad)
- Android 12 to Android 16

Key features

Acronis Mobile allows you to:

- Back up your personal data, including:
 - Photos
 - Videos
 - Contacts
 - Calendars

- Messages (Android only)
- Reminders (iOS only)
- Choose the following locations as a backup destination:
 - Acronis Cloud
 - Local storage on your PC or Mac
- Encrypt backups with the AES-256 cryptographic algorithm
- Automatically back up new and changed data
- Access cloud backups from all your mobile devices and recover data from these backups

Where can I find these apps?

You can view additional information and download Acronis Mobile from the Apple App Store or Google Play:

- Acronis Mobile for iOS devices: <https://go.acronis.com/atimobile/download/iOS>
- Acronis Mobile for Android devices: <https://go.acronis.com/atimobile/download/Android>

Local destination of mobile backups

When you back up your mobile data to a computer, Acronis Mobile stores the backups in the default folder `C:\ProgramData\Acronis Mobile Backup Data\acronis-local-data\`. When you change the default folder, the `acronis-local-data` folder is moved to the location that you selected. All new mobile data will be backed up to the new location.

Note

All mobile backups are always stored in the same folder and cannot be separated.

To change a local destination for mobile backups

1. On the sidebar, click **Settings**, find the **Mobile backup location** option.
2. In the **Mobile backup location** section, click **Change**. The **Change location** window is displayed.
3. Click **Select location**, and then select a new location for the backups. Note, you can select a location only on your internal hard drives.

To change the new location to the initial one, click **Reset to default**.

Backing up Microsoft 365 data

Why back up Microsoft 365 data?

Even though Microsoft 365 is a set of cloud services, regular backups provide an additional layer of protection from user errors and intentional malicious actions. With Acronis True Image, you can protect your Microsoft Outlook mailboxes and Microsoft OneDrive data by backing up them to secure Acronis Cloud. After uploading to Acronis Cloud, all of the content is available from any

device, any time. You can recover deleted items from a backup even after the Microsoft 365 retention period has expired.

Note

You cannot perform a backup operation using a Microsoft business account.

Backing up Microsoft 365 data

Data that you can back up in your Outlook mailbox:

- All folders
- E-mail messages
- Attachments

Note

You cannot back up shared or group mailboxes.

Data that you can back up in your OneDrive:

- All files and folders

To back up Microsoft 365 data:

1. Open Online Dashboard by doing one of the following:
 - Follow the link: <https://cloud.acronis.com>.
 - On the sidebar of Acronis True Image, click **Backup**, click **Add backup**, click the **Backup source** area, and then select **Cloud service**.
2. Sign in to your Acronis account.
3. On the sidebar, click **Resources**, click **Add**, and then choose **Microsoft 365**.
4. Log in to your Microsoft account, if prompted.

Note

You cannot perform a backup operation using a Microsoft business account.

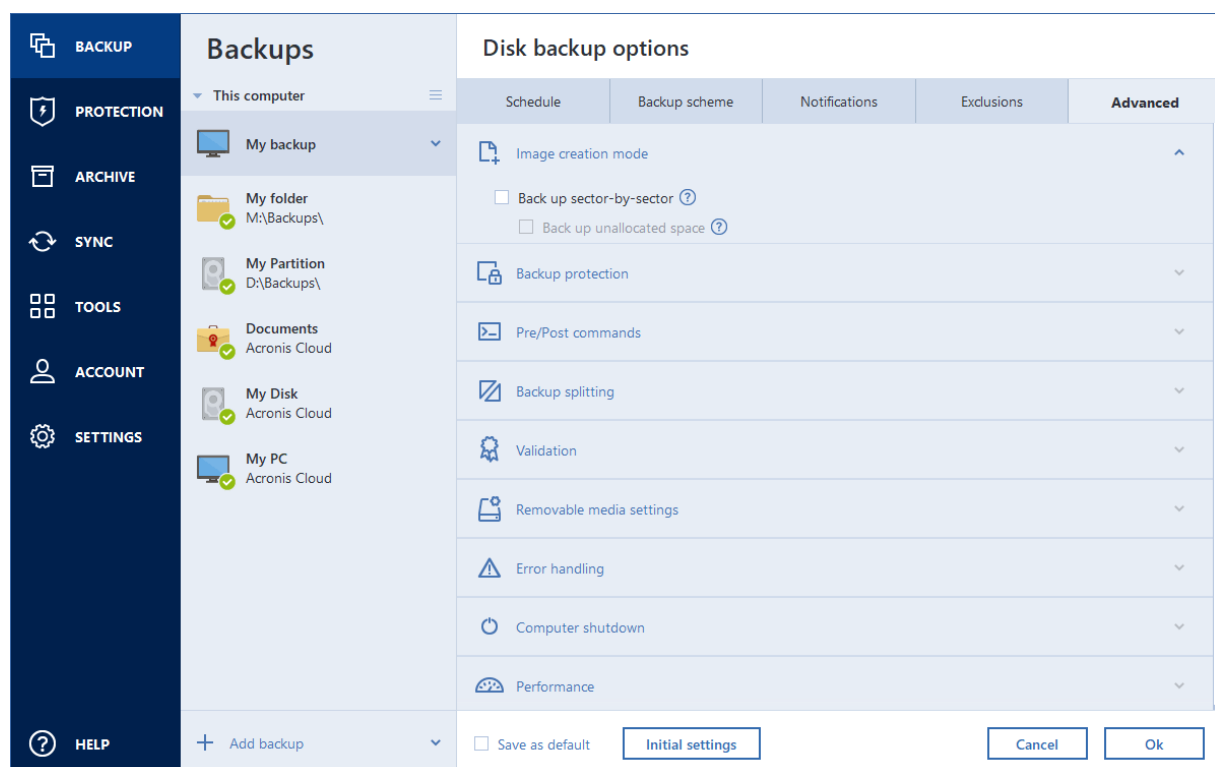
5. At the **Backup source** area, select items to backup:
 - Entire account
 - Outlook
 - OneDrive
6. Click **Done**.
7. You can configure cleanup rules for the backup via the **Cleanup** pane. You can also encrypt the backup and protect it with a password. When done, click **Apply**.
8. To start the backup, click **Run now**.

Backup options

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

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

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



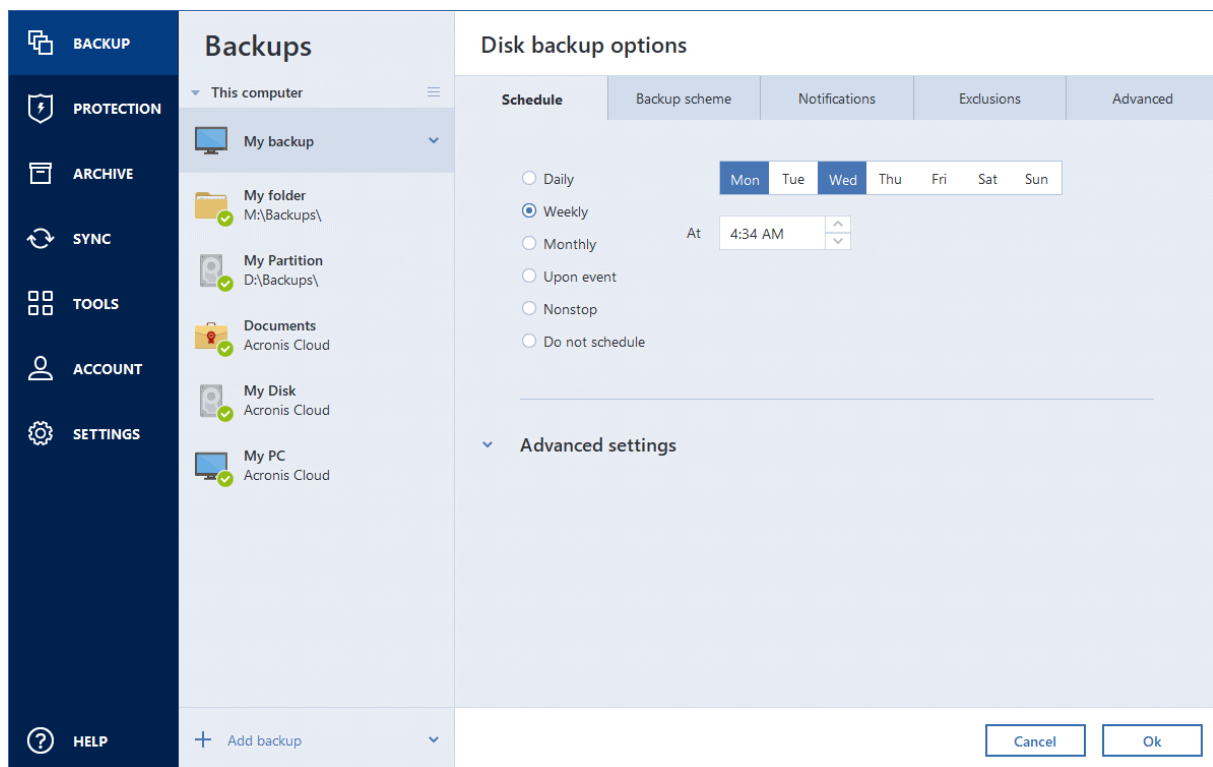
If you want to reset all the modified options to the values that were set after the product installation initially, click the **Reset to initial settings** button. Note that this will reset the settings for the current backup only. To reset the settings for all further backups, click **Reset to initial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

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

Scheduling

Location: **Options > Schedule**

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



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

- **Daily** – The operation will be executed once a day or more frequently.
- **Weekly** – The operation will be executed once a week or several times a week on the selected days.
- **Monthly** – The operation will be executed once a month or several times a month on the selected dates.
- **Upon event** – The operation will be executed upon an event.
- **Nonstop** – The operation will run every five minutes.
- **Do not schedule** – The scheduler will be turned off for the current operation. In this case the backup or validation will run only when you click **Back up now** or **Validate** respectively in the main window.

Advanced settings

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

- **Back up only when the computer is locked or screensaver is running** – Select this check box to postpone a scheduled operation until the next time the computer is not in use (a screen saver is displayed or computer is locked). For the validation schedule, the check box changes to **Run the validation only when the computer is idle**.
- **Wake up the sleeping/hibernating computer** – Select this check box to wake up the sleeping/hibernating computer to perform the scheduled operation.

- **Prevent the computer from going to sleep/hibernate** – Select this check box to eliminate a situation when a time-consuming backup is interrupted if the computer goes into sleep or hibernation mode.
- **Run missed operations at the system startup with delay (in minutes)** – Select this check box to force the missed operation to run at the next system startup, if the computer was switched off at the scheduled time, and the operation was not performed.
Additionally, you can set a time delay to start backup after the system startup. For example, to start backup 20 minutes after system startup, enter 20 in the appropriate box.
- **Run missed operations when an external device is connected** [optional, if you schedule a backup to a USB flash drive, or validation of a backup that is located on a USB flash drive] – Select this check box to run a missed operation when the USB flash drive is attached if it was disconnected at the scheduled time.

Daily backup parameters

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

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

Description of the **Advanced settings** see in [Scheduling](#).

Weekly backup parameters

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

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

Description of the **Advanced settings** see in [Scheduling](#).

Monthly backup parameters

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

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

Description of the **Advanced settings** see in [Scheduling](#).

Upon event execution parameters

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

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

Description of the **Advanced settings** see in [Scheduling](#).

Backup schemes

Location: **Options > Backup scheme**

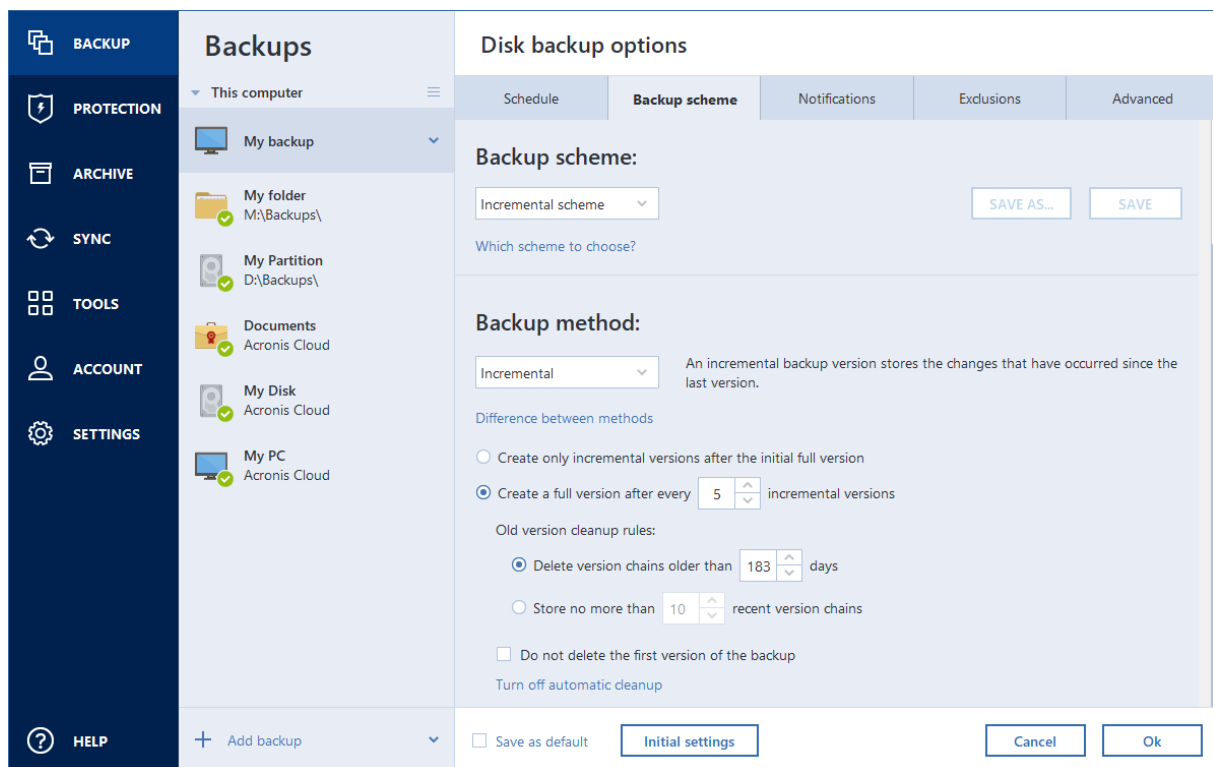
Backup schemes along with the scheduler help you set up your backup strategy. The schemes allow you to optimize backup storage space usage, improve data storage reliability, and automatically delete the obsolete backup versions.

Note

For online backups, the backup scheme is preset and cannot be changed. After the initial full backup, only incremental versions are created.

The backup scheme defines the following parameters:

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



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

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

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

Note

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

Single version scheme

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

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

Note

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

Backup scheduler setting for disk backup: monthly.

Backup scheduler setting for file backup: daily.

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

Required storage space: minimal.

Version chain scheme

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

Disk backup version chain

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

Backup scheduler setting: monthly.

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

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

File backup version chain

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

Backup scheduler setting: daily.

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

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

Custom schemes

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

Note

You cannot overwrite existing pre-defined backup schemes.

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

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

- **Full**

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

- **Incremental**

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

You can configure the scheme by using one of the following options:

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

- **Differential**

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

You can configure the scheme by using one of the following options:

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

Turn on automatic cleanup

- **Old version cleanup rules** – To delete obsolete backup versions automatically, you can set one of the following cleanup rules:
 - **Delete versions older than [n] days** [available for full method only] – Select this option to limit the age of backup versions. All versions that are older than the specified period will be automatically deleted.
 - **Delete version chains older than [n] days** [available for incremental and differential methods only] – Select this option to limit the age of backup version chains. The oldest version

chain will be deleted only when the most recent backup version of this chain is older than the specified period.

- **Store no more than [n] recent versions** [available for full method only – Select this option to limit the maximum number of backup versions. When the number of versions exceeds the specified value, the oldest backup version will be automatically deleted.
- **Store no more than [n] recent version chains** [available for incremental and differential methods only – Select this option to limit the maximum number of backup version chains. When the number of version chains exceeds the specified value, the oldest backup version chain will be automatically deleted.
- **Keep size of the backup no more than [defined size]** [not available for local backups – Select this option to limit the maximum size of the backup. After creating a new backup version, the program checks whether the total backup size exceeds the specified value. If it's true, the oldest backup version will be deleted.
- **Do not delete the first version of the backup** – Select this check box to keep the initial data state. The program will create two initial full backup versions. The first version will be excluded from the automatic cleanup, and will be stored until you delete it manually.
If you select incremental or differential method, the first backup chain will start from the second full backup version. And only the third version of the backup will be incremental or differential one.

Note that when the check box is selected for the full method, the **Store no more than [n] recent versions** check box changes to **Store no more than 1+[n] recent versions**.

Managing custom backup schemes

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

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

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

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

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

Note

The pre-defined backup schemes cannot be deleted.

Examples of custom schemes

1. Entire PC backup “Two full versions”

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

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

In this case, the program will create a new full version every month, on the 20-th day. After creating the third version, the oldest version will be automatically deleted.

7. Check that all settings are correct and click **Back up now**. If you want your first backup to be run only at the time you specified in the Scheduler, click the down arrow to the right of the **Back up now** button and select **Later** in the drop-down list.

2. File backup “Daily incremental version + weekly full version”

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

1. Start configuring a file backup. See [Backing up files and folders](#) for details.
2. Click **Options**, open the **Schedule** tab, click **Daily**, and then specify a start time for the backup operation. For example, if you finish your everyday work at 8 PM, specify this time or a little later (8.05 PM) as the start time.

3. Open the **Backup scheme** tab, and then choose **Custom scheme** instead of **Incremental scheme**.

4. In the **Backup method** box, select **Incremental** from the drop-down list.
5. Click **Create a full version after every [n] incremental versions**, and type or select **6**.

In that case, the program will first create the initial full backup version (no matter how you set up a backup process, the first backup version will always be the full one), and then six incremental versions day by day. Then, it will create one full version and six incremental versions again and so on. So every new full version will be created in exactly a week's time.

6. To limit the storage time for the versions, click **Turn on automatic cleanup**.
7. Click **Delete version chains older than [n] days**, type or select **21**, and click **OK**.

8. Check that all settings are correct and click **Back up now**. If you want your first backup to run only at the time you specified in the Scheduler, click the down arrow to the right of the **Back up now** button and select **Later** in the drop-down list.

3. Disk backup “Full version every 2 months + differential version twice a month”

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

1. Start configuring a disk backup. See [Backing up disks and partitions](#).
2. Select your system partition (usually C:) as the backup source.
3. Click **Options**, open the **Schedule** tab, click **Monthly**, and then specify, for example, the 1st and 15th days of the month. This will result in a backup version in about every two weeks. Then, specify a start time for the backup operation.
4. Open the **Backup scheme** tab, and then choose **Custom scheme** instead of **Incremental scheme**.
5. In the **Backup method** box, select **Differential** from the drop-down list.
6. Click **Create a full version after every [n] differential versions**, and type or select **3**.
In that case the program will first create the initial full backup version (no matter how you set up a backup process, the first backup version will always be the full one), and then three differential versions, each one in about two weeks. Then again a full version and three differential versions and so on. So every new full version will be created in two months.
7. To limit storage space for the versions, click **Turn on automatic cleanup**.
8. Click **Keep size of the backup no more than [defined size]**, type or select **100 GB**, and click **OK**.

Note

When the total backup size exceeds 100 GB, Acronis True Image will clean up the existing backup versions to make the remaining versions satisfy the size limit. The program will delete the oldest backup chain consisting of a full backup version and three differential backup versions.

9. Check that all settings are correct and click **Back up now**. If you want your first backup to be run only at the time you specified in the Scheduler, click the down arrow to the right of the **Back up now** button and select **Later** in the drop-down list.

Notifications for backup operation

Location: **Options > Notifications**

Sometimes a backup or recovery procedure can last an hour or longer. Acronis True Image 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 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 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. If you want to receive notifications about all of your backups, you can set up email notifications in the Online Dashboard. See [Email notifications](#) for details. Both methods work independently from each other and can be used simultaneously.

Excluding items from backup

Location: **Options > Exclusions**

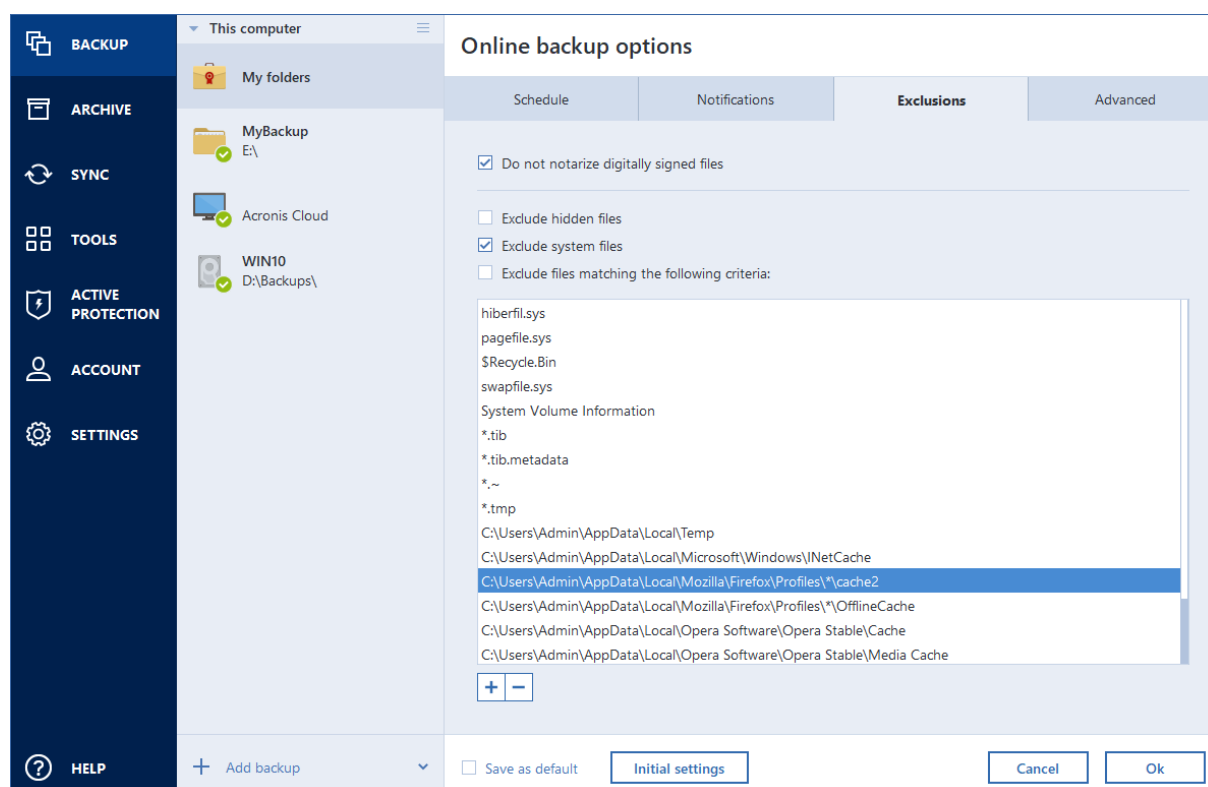
If you want to exclude unnecessary files from a backup, specify the appropriate file types on the **Exclusions** tab of the backup options. You can specify exclusions for disk backups, file backups or online backups.

When you select a specific file for backup, it cannot be excluded by the exclusion settings. The settings are applicable only to files located on a partition, disk, or inside a folder selected for backup.

How to use the default exclusion settings

After you have installed the application, all the exclusion settings 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 settings to the values that they were originally set to when the product was installed, click the **Reset to initial settings** button.



What you can exclude and how

You have the following options to exclude files from backups:

- **Do not notarize digitally signed files** (available for notarized backups only) – The main purpose of a notarized backup is protection of your personal files. Therefore, there is no need to back up system files, application files, and other files that have a digital signature. To exclude these files, select the corresponding check box.
- **Exclude hidden files** – Select this check box to exclude hidden files and folders from a file-level backup.
- **Exclude system files** – Select this check box to exclude system files and folders from a file-level backup.

You can exclude files meeting the criteria you specify. To do this, select the **Exclude files matching the following criteria** check box, click the plus sign, and then enter the exclusion criterion.

Note

We do not recommend excluding hidden and system files from the backups of your system partition.

To add an exclusion criterion

- You can enter explicit file names for exclusion from the backup:
 - *file.ext* - all such files will be excluded from the backup.
 - *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.
- To exclude a folder from a disk-level backup, click the plus sign, click the ellipsis button, go to the directory tree and select the folder you want to exclude, and then click **OK**.

To delete a criterion added by mistake, select the criterion, and then click the minus sign.

Image creation mode

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

This option is not available for the backups that use Acronis Cloud as a backup destination.

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. Keep in mind that this mode increases processing time and usually results in a larger image file.

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

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

Backup protection

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

Note

This topic is applicable to local and network backups. For information about protecting cloud backups, see [Online backup protection](#).

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

Note

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

To protect a backup

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

Note

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

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

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

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

- **AES 128** - to use 128-bit encryption key
- **AES 192** - to use 192-bit encryption key
- **AES 256** - to use 256-bit encryption key

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

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

How to get access to a password-protected backup

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

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

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

Online backup protection

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

To protect your data on Acronis Cloud from unauthorized access, you can use encryption. In this case, when you back up your data, it will be encrypted by using the AES-256 algorithm and then saved to Acronis Cloud. To encrypt and decrypt your data, the program needs the password, that you should specify when you configure the online backup¹. You can specify any set of characters you like. Note that the password is case-sensitive.

¹A backup whose destination is Acronis Cloud. Online backups are stored remotely and accessible over the Internet.

Warning!

A password of an online backup cannot be retrieved. Memorize the password that you specify for backup protection.

While attempting to access the encrypted data, the program asks you to enter the password.

Note

Note that you cannot set or change the password for a pre-existing online backup.

Pre/Post commands for backup

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

This option is not available for the backups that use Acronis Cloud as a backup destination.

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 cannot split already existing backups. Backups can be split only when being created.

This option is not available for the backups that use Acronis Cloud as a backup destination.

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 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 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**

This option is not available for the backups that use Acronis Cloud as a backup destination.

You can specify the following settings:

- **Validate backup each time after it is completed** – Select to check the integrity of the backup version immediately after backup. We recommend that you enable this option when you back up your critical data or system disk.

- **Validate the latest backup version only** – A quick validation of the last backup slice.
 - **Validate entire backup**
 - **Validate backup on schedule** – Select to schedule validation of your backups to ensure that they remain "healthy".
 - **The latest backup version when it is completed**
 - **Entire backup when it is completed**
- The default settings are as follows:
- **Frequency** – Once a month.
 - **Day** – The date when the backup was started.
 - **Time** – The moment of backup start plus 15 minutes.

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

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

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

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

You can change the default settings and specify your own schedule. For more information see [Scheduling](#).

Removable media settings

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

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

Warning!

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

The following settings are available:

- **Place Acronis True Image on media** – We strongly recommend selecting this option to support USB, PC Card (formerly PCMCIA), and SCSI interfaces along with the storage devices connected via them.
- **Place Acronis True Image (64-bit) on media** – The same option for 64-bit systems.
- **Place Acronis System Report on media** – Select this option to generate System Report that is used for collecting information about your system in case of any program problem. Report generation will be available before you start Acronis True Image from the bootable media. The

generated System Report can be saved to a USB flash drive.

- **Place Acronis System Report (64-bit) on media** – The same option for 64-bit systems.
- **Ask for first media while creating backups on removable media** – Select this option to display the **Insert First Media** prompt when backing up to removable media. With the default setting (option selected), backing up to removable media may not be possible if the user is away, because the program will wait for someone to click **OK** in the prompt box. Therefore, you should disable the prompt when scheduling a backup to removable media. Then, if the removable media is available (for example, CD-R/RW inserted) the backup can run unattended.

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

32-bit or 64-bit components

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

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

Error handling

When a backup fails

Note

This topic applies to local and network backups only. For cloud backup error options, see [Error handling for Cloud backups and replicas](#).

In backup settings, go to **Options > Advanced > Error handling**.

To set up error handling, configure one or more of the following options:

- **Do not show messages and dialogs while processing (silent mode)** - Ignores errors and continues the backup. Useful for unattended operations.
- **Ignore bad sectors** - For disk and partition backups only. Completes backup even if bad sectors are found on the source disk.
- **When not enough space in ASZ, delete the oldest backup** - Deletes the oldest backup in Acronis Secure Zone when free space is insufficient.
- **Repeat attempt if a backup fails** - Automatically retries a failed backup. Set the number of attempts and the interval between attempts.

If the error persists, the backup will fail after all retry attempts are used.

Note

Scheduled backups will not start until all retry attempts complete.

Error handling for Cloud backups and replicas

You can configure Acronis True Image to retry failed backups and replications to Cloud.

To configure the number of retry attempts and the interval between them:

1. On the **Backup** dashboard, click a backup to Cloud, click **Options**, and go to the **Advanced** tab.
2. Under **Error handling**, select the **Repeat attempt if a backup fails** check box, and then choose the number of attempts (from 1 to 99) and the interval between them.
3. Click **OK**.

The new setting will be applied for all following backup and replication operations to Cloud for the selected backup object.

Note

Scheduled backup operations will not start until all attempts to repeat the backup are completed.

File-level security settings for backup

Location: **Options > Advanced > File-level security settings**

Note

This option is only available for file-level backups.

This option is not available for the backups that use Acronis Cloud as a backup destination.

You can specify security settings for backed up files:

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

If you do not use the encryption feature available in Windows XP and later operating systems, simply ignore this option. (Files/folders encryption is set in **Properties -> General -> Advanced Attributes -> Encrypt contents to secure data**).

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

Location for backups to Acronis Cloud: **Options > Advanced > Performance and network**

Compression level

You can choose the compression level for a backup:

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

Note

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

Note

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

Operation priority

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

You can set up the operation priority:

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

When you back up data to Acronis Cloud, you can change the connection speed used by Acronis True Image. Set the connection speed that will allow you to use internet and network resources without annoying slowdowns.

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 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 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.
- **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.

Selecting a data center for backup

Location: **Options > Advanced > Data center**

Note

This option is only available for online backups¹.

When you create a backup to Acronis Cloud, your data is uploaded to one of the Acronis data centers, located in different countries. Initially, the data center is defined as the one closest to your location when you create your Acronis account. Afterwards, your online backups are stored in the same data center, by default.

We recommend that you set the data center for a backup manually, when you are in a different country, and your default data center is not the closest to your current location. This will significantly increase the data upload rate.

Note

You cannot change the data center for a pre-existing backup.

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

¹A backup whose destination is Acronis Cloud. Online backups are stored remotely and accessible over the Internet.

- 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.

Local mobile backups do not depend on this setting. Your mobile data is backed up to local storage on your computer as usual.

Wi-Fi networks for backup to Acronis Cloud

Location: **Settings > Wi-Fi networks for backup**

When you back up your data to Acronis Cloud, you can be concerned about the security of your personal data when it is transferred by unprotected Wi-Fi networks. To avoid the risk of theft of your personal data, we strongly recommend that you only use protected Wi-Fi networks.

To protect your data

1. On the sidebar, click **Settings > Wi-Fi networks for backup**, and then click **Set networks**.
2. In the **Wi-Fi networks for backup** window which contains all currently available and saved unavailable Wi-Fi networks, select the check boxes next to the networks that you want to use to back up your data.

When the networks are selected and your computer loses a connection to any of them, all current backups are paused and scheduled backups will not start. Once the computer connects to any of these networks, the suspended backups will be resumed. The scheduled backups that have been missed because of this setting will be started as well.

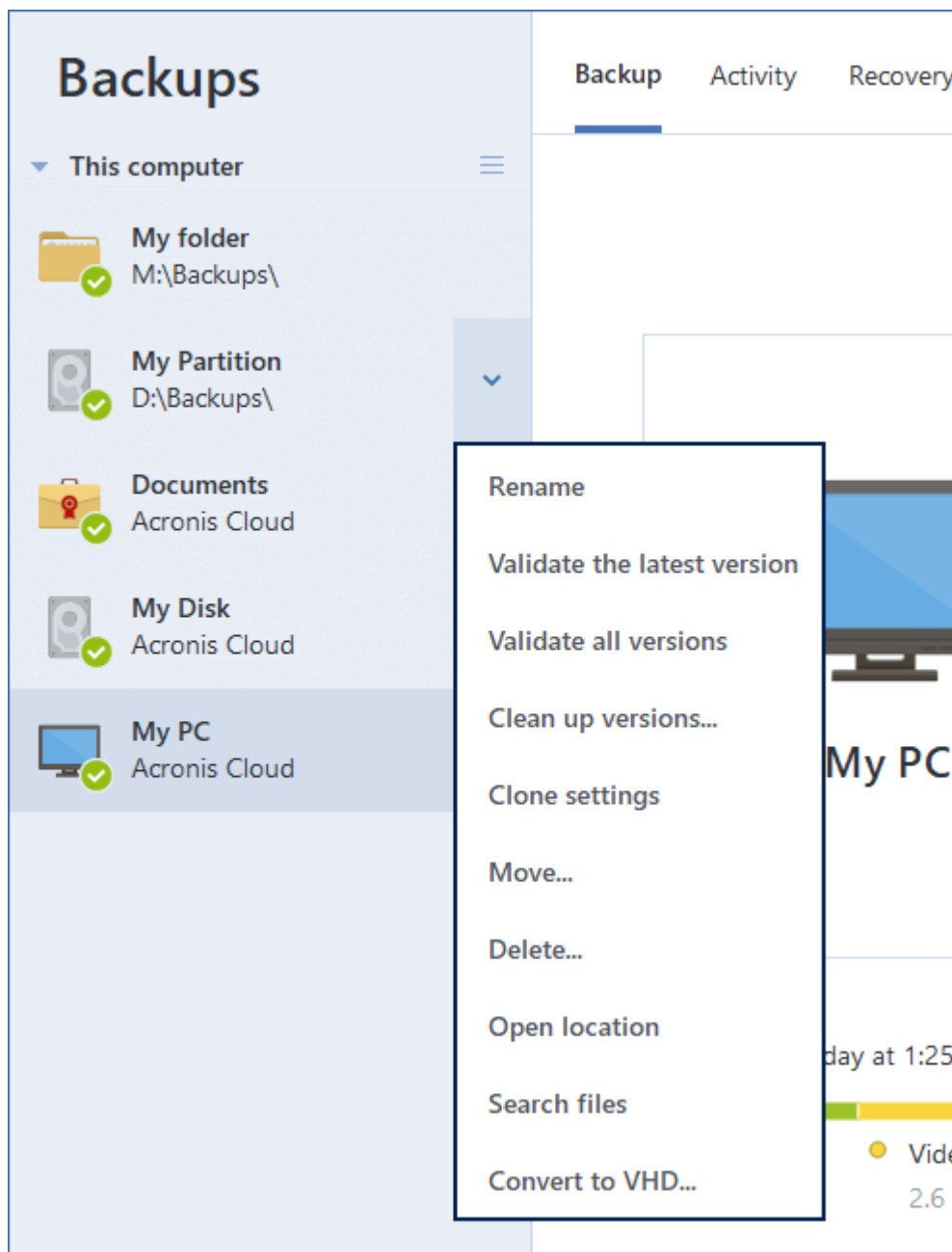
To back up your data by using a new Wi-Fi network, simply select it in the **Wi-Fi networks for backup** window. This can be done whenever you need to use new network.

Local mobile backups do not depend on this setting. Your mobile data is backed up to local storage on your computer, as usual.

Operations with backups

Backup operations

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



The backup operations menu can contain the following items:

- **Rename** (not available for backups to Acronis Cloud) – Set a new name for a backup in the list. The backup files will not be renamed.
- **Validate the latest version** – Start quick validation of the last backup slice.
- **Validate all versions** – Start validation of all backup slices.
- **Clean up versions** – Delete backup versions you no longer need.
- **Clone settings** – Create a new empty backup box with the settings of the initial backup and named **(1) [the initial backup name]**. Change the settings, save them, and then click **Back up now** on the cloned backup box.

- **Move** – Move all of the backup files to another location. The subsequent backup versions will be saved to the new location.

If you change the backup destination by editing the backup settings, only new backup versions will be saved to the new location. The earlier backup versions will remain in the old location.

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

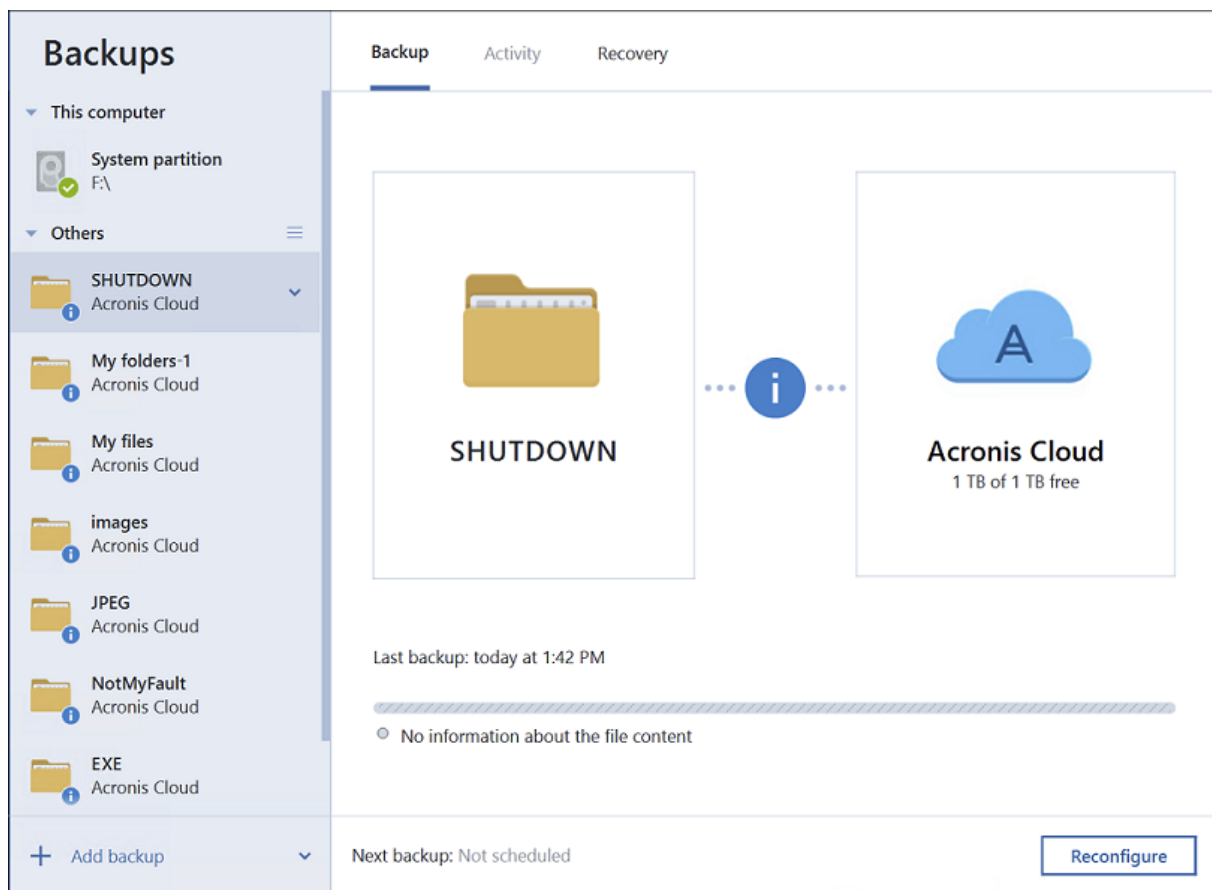
You can also reconfigure the backup settings to adjust parameters such as the source, destination, and schedule, ensuring they meet your current requirements.

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

- **Reconfigure** (for backups manually added to the backup list) – Configure the settings of a backup created by a previous version. This item may also appear for backups created on another computer and added to the backup list without importing their settings. Without backup settings, you cannot refresh the backup by clicking **Back up now**. Also, you cannot edit and clone the backup settings.
- **Reconfigure** (for online backups) – Bind a selected online backup to the current computer. To do this, click this item and reconfigure settings of the backup. Note that only one online backup can be active on one computer.

To reconfigure backups:

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



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

Backup activity and statistics

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

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

The Activity tab

Note

Nonstop backup and mobile backups do not have an activity feed.

To view backup activity

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

How to clear the backup log

The backup log is part of the selected backup history. Cleanup of backup versions does not clear log entries.

To clear the backup log in the **Activity** tab for a backup, remove the backup record (the item in the **Backup** list) in Acronis True Image:

1. In the **Backup** section, click the down arrow icon next to the backup, and then click **Delete**.
2. If available for this backup type, choose the option that removes only the backup record from the **Backup** list and keeps the backup files in the storage.
3. New log entries will appear when the next backup operations run.

For details about deleting backups and the available delete options, see "Deleting backups and replicas" (p. 110).

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

Backup size metrics (.tib archives, legacy)

- For file-level backups, Acronis True Image calculates the size of files to back up. The value of **Backed up** is equal to the value of **Data to recover** for full backup versions. For differential and incremental versions, **Backed up** is usually less than **Data to recover**, because the product additionally uses data from the previous versions for recovery.

- For disk-level backups, Acronis True Image calculates the size of the hard drive sectors that contain data to back up. Because sectors may contain hard links to files, even for full disk-level backup versions the value of **Backed up** can be less than the value of **Data to recover**.

Backup size metrics (.tibx archives, current format)

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

Causes of possible discrepancies in sizes

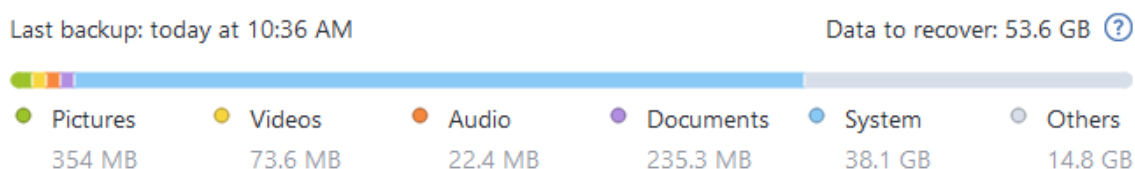
Acronis True Image uses different metrics to represent data at various stages. Because of this, the values of **Backed up** and **Data to recover** in the **Activity** tab can differ. Review the specifics above and validate the backup to ensure its consistency.

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

For more information, see the [Support Portal article](#).

The Backup tab

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



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

- Pictures
- Video files
- Audio files
- Documents
- System files
- Other file types, including hidden system files

When no information about the file content is shown

The Statistics bar may show the message "**No information about the file content**" in the following scenarios:

- After performing a system restore with Acronis True Image.
- After removing and re-adding a backup with the **Add existing backup** option.
- After successful backup of a hidden partition.
- After successful Sector-by-Sector backup.
- When using Non-stop Backup.

This message does not mean that the backup is corrupted. In these scenarios, Acronis True Image does not read or show detailed information about backup content in the Statistics bar.

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.

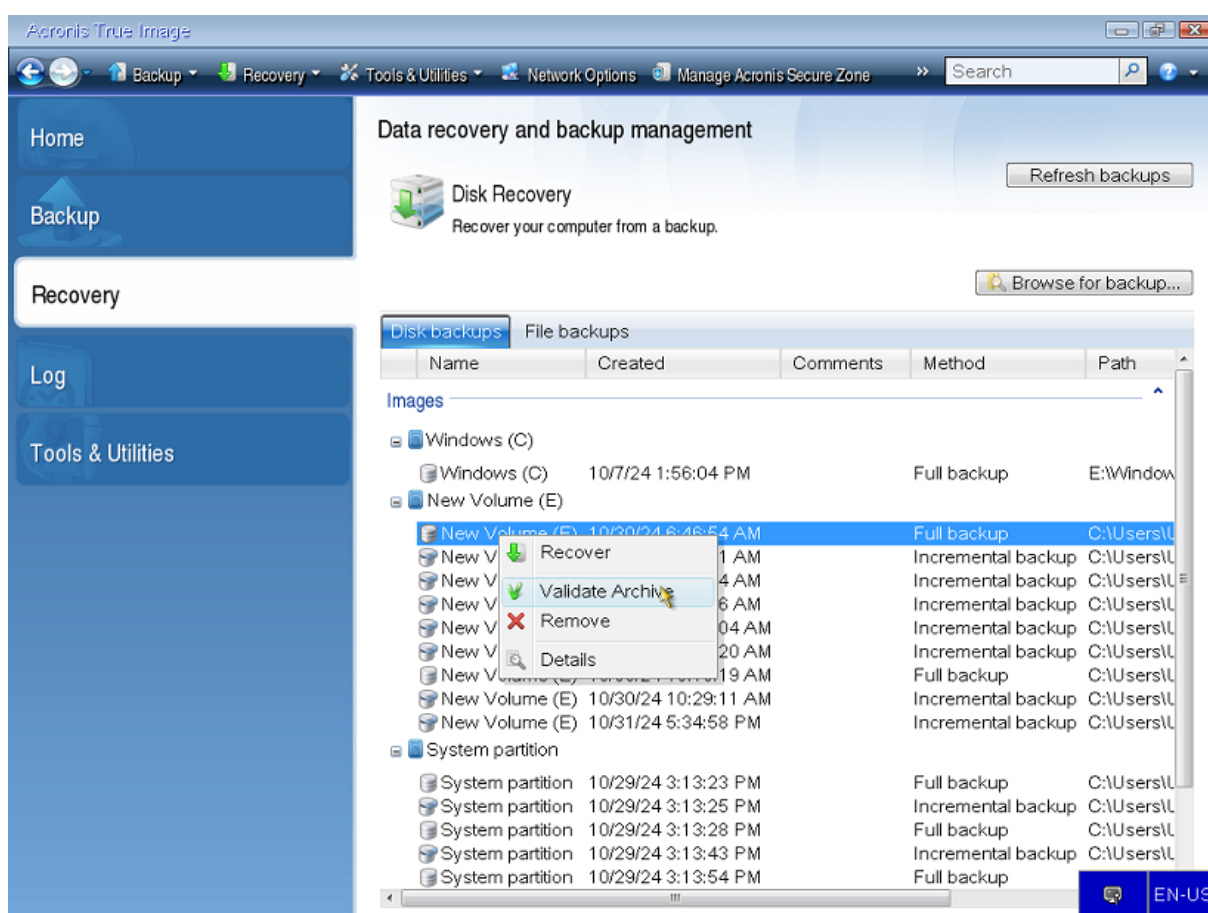
For example, backup validation is important before you recover your system. If you start recovery from a corrupted backup, the process will fail and your computer may become unbootable. We recommend that you validate system partition backups under bootable media. Other backups may be validated in Windows.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

To validate an entire backup in Windows

1. Start Acronis True Image, 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 (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 adds this backup to the list.
2. Right-click the backup or a specific version, and then click **Validate Archive**. This opens the **Validate Wizard**.
3. Click **Proceed**.



Backup to various places

You can save versions of a backup to different destinations by changing the backup destination when editing the backup settings. For example, after you save the initial full backup to an external USB hard drive, you can change the backup destination to a USB stick by editing the backup settings. The subsequent incremental or differential backups will be written to the USB stick.

Note

You cannot continue backing up to an optical disc.

Note

Acronis Secure Zone and FTP servers can contain an entire backup only.

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 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.

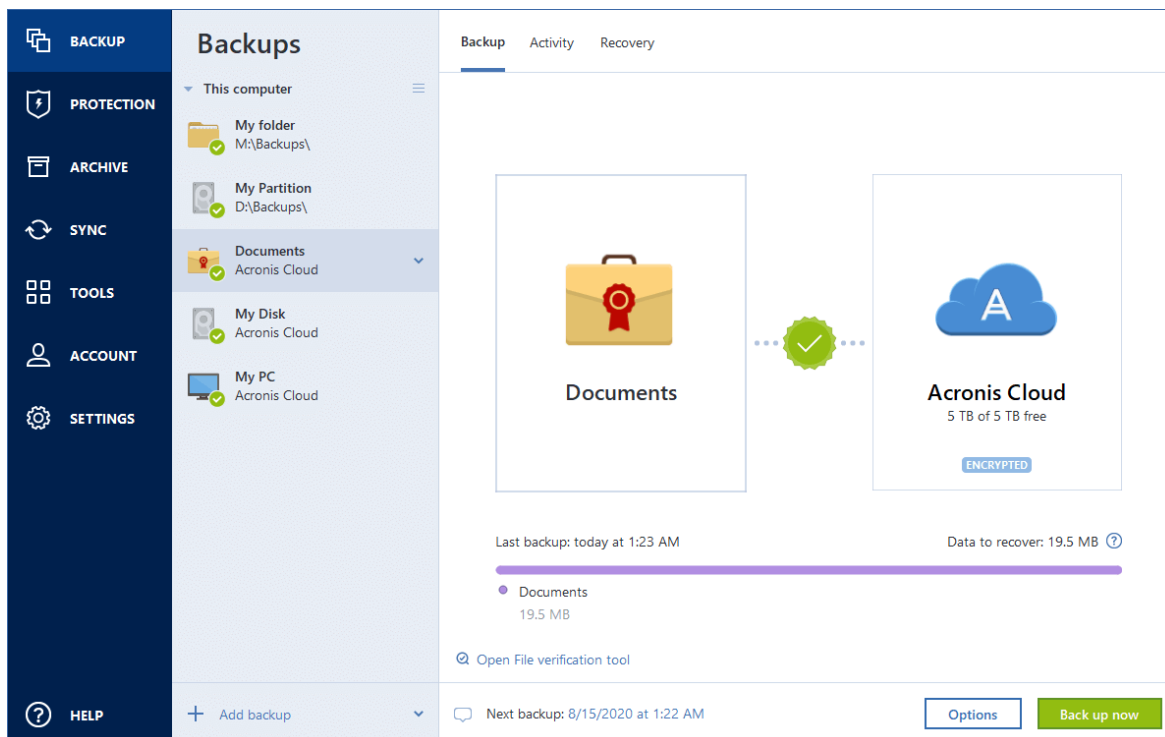
Notarized backup

By using Blockchain technology, Acronis True Image can protect your files from unauthorized modification. This gives you a guarantee that you can recover your data from the same file that was backed up. We recommend that you use this type of backup to protect your legal document files or any other files that require proved authenticity. See [Using Blockchain technology](#) for details.

To create a notarized backup of your files and folders

1. Start Acronis True Image.
2. On the sidebar, click **Backup**.
3. Click **Add backup**.

4. [Optional] To rename the backup, click the arrow next to the backup name, click **Rename**, and then enter a new name.
5. Click the **Backup source** area, and then select **Files to notarize**.
6. In the opened window, select the check boxes next to the files and folders that you want to back up, and then click **OK**.



7. Click the **Backup destination** area, and then select a destination for backup:
 - **Acronis Cloud** – Sign in to your Acronis account, and then click **OK**.
If you do not have an Acronis account, click **Create account**, type your email address, password, and then click the **Create account** button. See [Acronis account](#) for details.
 - **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 will suggest using it as a backup destination by default.
 - **Browse** – Select a destination from the folder tree.
8. [optional step] Click **Options** to set the options for the backup. For more information see [Backup options](#).
To exclude files with a digital signature from the backup, select the **Do not notarize digitally signed files** check box on the **Exclusions** tab. See [Excluding items from backup](#) for details.
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 down arrow to the right of the **Back up now** button, and then click **Later**.

Note

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

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

Using Blockchain technology

Acronis True Image uses the Blockchain technology to provide top-level security for your backed-up files. This technology gives you the guarantee that your files have not been modified by fraudulent software, and when it is time to recover, you recover data from exactly the same file that was backed up.

What is Blockchain?

Blockchain is a database that contains information about transactions and their sequence. In general, a transaction represents an event, such as a financial operation or an operation with different kinds of assets. The transactions are united in blocks, which are written to the database one by one and form a block chain. Every transaction and every block has its own unique identification number. What is very important is that every block stores information about all previous blocks of the chain. Once written to the database, the information about a transaction cannot be changed in any way or by anyone, and the transaction sequence cannot be modified either. Any attempt to change any piece of information in the database can be easily identified by any user of the database, because there would be no information about the false transaction or false block in all subsequent blocks. This technology guarantees that data stored in the database is valid, belongs to a specific person, and has not been modified by anyone. See more information about Blockchain at [https://en.wikipedia.org/wiki/Blockchain_\(database\)](https://en.wikipedia.org/wiki/Blockchain_(database)).

How Acronis True Image uses the Blockchain technology

To protect your files from unauthorized modification, Acronis True Image uses the Acronis Notary technology. This is a universal solution for timestamping and fingerprinting any data objects and streams. Since it is impractical to store large amount of data in a Blockchain database, Acronis True Image sends only file hash codes to the Acronis Notary service.

A hash code is a unique number of fixed size that is produced by a hash function. The code mathematically defines an arbitrary set of data, for example, a backup file. Any change of the backup file leads to a change of its hash code. Therefore, to check if the file was changed, you only need to compare the hash codes generated in the initial and current states of the file. If the codes match, this is a guarantee that the file has not been modified by anyone.

When Acronis Notary receives hash codes of your files, it calculates a new single hash code and sends it to the Ethereum Blockchain-based database. See more information about Ethereum at <https://www.ethereum.org/>.

Once the hash code is in the database, the files that were used to calculate this hash code are notarized by Acronis Notary. You can easily verify the file authenticity at any time by using the procedure described in [Verifying file authenticity](#). Every notarized file has a notarization certificate, which is documentary proof that the file is protected with the Blockchain technology. A certificate contains general information about the file and technical details that allow you to manually verify the file authenticity. See [Manual verification of a file's authenticity](#) for details.

Verifying file authenticity

By using Blockchain technology, Acronis True Image can protect your backed-up files from unauthorized modification. This gives you a guarantee that you can recover data from exactly the same file that was backed up.

To verify a file's authenticity in Acronis True Image

1. Start Acronis True Image.
2. On the sidebar, click **Backup**.
3. From the backup list, select the notarized backup which contains the file that you want to verify.
4. On the right panel, open the **Recovery** tab.
5. Browse to the required file, click the Menu icon (), and then click one of the following:
 - **View certificate** – The certificate containing the detailed information about the file security will be opened in the web browser.
 - **Verify** – Acronis True Image will check the file authenticity.

To verify a file's authenticity in the File verification tool

1. Open the File verification tool with one of the following methods:
 - In a web browser, open <https://notary.acronis.com/verify>.
 - On the sidebar of Acronis True Image, click **Backup**, select a notarized backup, and then click **Open File verification tool** on the right panel.
2. In File Explorer, browse to the file that you want to verify, and then drag it to the web browser window.

If a notarized backup is stored on Acronis Cloud, you can also verify a backed-up file's authenticity in Acronis Cloud.

To verify a file's authenticity in Acronis Cloud

1. Go to <https://www.acronis.com/my/online-backup/webrestore/>, and then log in to your Acronis account.
2. On the sidebar, click **Backups**.
3. From the backup list, select the notarized backup which contains the file that you want to verify.
4. Browse to the required file and select it with a check mark. Then, click **Verify** on the right sidebar.

Manual verification of a file's authenticity

The easiest way to verify a file's authenticity is to use the **Verify** command in Acronis True Image or in Acronis Cloud. See [Verifying file authenticity](#) for details. In addition to this easy method, you can perform the verification procedure yourself, step by step.

To verify a file's authenticity manually

Step 1. Calculate MD5 hash of the file

1. Start Windows PowerShell.
2. For example, to calculate the md5 hash for the picture.png file located in C:\Users\picture.png, type:

```
$($((CertUtil -hashfile "C:\Users\picture.png" MD5)[1] -replace " ", ""))
```

Example of an md5 hash: eea16ade1edf2750a46bb6bffb2e45a2

3. Check that the calculated md5 hash is equal to an eTag in the DATA field in your notarization certificate. See [Verifying file authenticity](#) for details about obtaining a file certificate.

Step 2. Check that a ROOT is stored in the blockchain

1. Open a blockchain explorer, for example <https://etherscan.io/>.
2. Enter the TRANSACTION ID from the certificate into the search field.
3. Check that the Data field in the Event Logs tab is equal to the ROOT value in your certificate.

Step 3. Check that the hash is included in the tree

1. Download the command line utility from the GitHub repository:
<https://github.com/acronis/notary-verifyhash/releases>.
2. Follow the instructions at: <https://github.com/acronis/notary-verifyhash>.

Acronis ASign

What is Acronis ASign?

Acronis ASign is an online-service that allows multiple people to sign a file electronically. The file should be preliminarily uploaded to Acronis Cloud via backup or archiving. To further protect the signed files, they are notarized and protected via Acronis Notary.

The ASign solution can be used for signing any electronic documents, including different kinds of contracts, agreements, certificates, financial documents, and official letters.

Signing a file

To sign a file on Acronis Cloud

1. Go to <https://www.acronis.com/my/online-backup/webrestore/>, and then log in to your Acronis account.

2. Browse to the required file, click the file name, and then select **Send for signature** in the opened menu.
3. Type the email addresses of the people who you want to sign the file, and then send them invitations.

After the file is signed by all signees, Acronis Notary notarizes the file and generates a signature certificate.

Note

You can also start ASign from the desktop app for a backed-up file version: open the file details pane, click **Send for signature**, and then click **Proceed** in the confirmation window. Your browser opens the ASign page, where you add signatories and share the link.

Note

If you do not see **Send for signature**, the feature may be unavailable for your subscription or not enabled for your account.

For the full description of the feature, refer to the English-language Acronis ASign web help at <https://www.acronis.com/en-us/support/documentation/ATI2017ASign/>.

Deleting backups and replicas

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

Acronis True Image 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

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. Note that if you delete a backup completely, the deletion cannot be undone. When you only remove the backup name from Acronis True Image, the backup files remain in their current location and you will be able to add the existing backup to Acronis True Image 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. If you want to delete backup files that you see locally, but not in Acronis True Image, try adding this existing backup to Acronis True Image. After that, you can completely delete this backup and its files by using Acronis True Image.

When you delete a backup, its replica is deleted automatically together with it. You cannot delete a local backup and still save its replica. However, you can delete a replica alone and keep the local backup.

To delete an entire backup replica locally in Acronis True Image

You can delete a replica with its original backup or separately. To delete it with the backup, delete the backup in the way described above.

To delete a replica without deleting the backup, in the **Backup** section, click the down arrow icon next to the backup with the replica to delete, and then click **Delete replica only**.

To delete an entire backup by using Acronis Cloud

1. Go to <https://www.acronis.com/my/online-backup/webrestore/>, and then log in to your Acronis account.
2. On the **Backups** tab, click the size of the backup that you want to delete. Then, the detailed view will appear.
3. 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 application.

See also

"Cleaning up backups, backup versions, and replicas" (p. 111)

"Replicating backups to Acronis Cloud" (p. 162)

Cleaning up backups, backup versions, and replicas

Cleanup rules for backups

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

Note

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

Cleanup rules for backup replicas

For more information on cloud replicas of your local backups, see "Replicating backups to Acronis Cloud" (p. 162).

1. Go to the **Backup** section.
2. From the backup list, select the backup for which you want to clean up replica versions, and then click **Options**.
3. On the **Advanced** tab, open the **Acronis Cloud cleanup** tab.
 - Use the **Store no more than ... recent backup versions** option to enter a value that limits the maximum number of replica versions that are stored.
 - Select the **Delete backup versions that are older than** check box and enter a value that limits the maximum age of the older versions. The most recent versions will be kept and all other versions will be automatically deleted.

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 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.
- Notarized backups.

To clean up backup versions locally in Acronis True Image

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. [Optional] If you want to delete replicas, select **Acronis Cloud** under **Delete versions from**.
3. Select the required versions and click **Delete**.
4. 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.

Cleanup removes backup versions from storage, but does not clear the backup log in the **Activity** tab. To reset the backup log for a backup, remove the backup record (the item in the **Backup** list) in Acronis True Image. New log entries will appear when the next backup operations run. See "Deleting backups and replicas" (p. 110).

Cleaning up versions that have dependent versions

A backup version can be part of a backup version chain¹.

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).

If you delete an incremental version file manually (for example, in File Explorer), recovery from this version and the following incremental versions may fail.

If you use the **Clean up versions** wizard in Acronis True Image, the app keeps the remaining backup data consistent. For backups in the current format (.tibx), you can delete an incremental version in the middle of the chain without deleting all following incremental versions.

- If you select a full version¹, the app also selects all dependent incremental and differential versions until the next full version. In this case, the whole chain is deleted. If the backup contains only full versions, they can be deleted independently.
- If you select a differential version², it can be deleted independently.
- If you select an incremental version³, cleanup behavior depends on backup format and chain consistency.

To clean up backup versions by using Acronis Cloud

1. Go to <https://www.acronis.com/my/online-backup/webrestore/>, and then log in to your Acronis account.
2. On the **Backups** tab, click the size of the backup or the replica whose versions you want to delete.
3. In the details view, click **Clean up**.
You can select to delete versions older than a period selected by you, or clean up all versions except a number of recent ones.
4. Configure what to delete and click **Clean up now**.
5. In the confirmation dialog, click **Delete**.

The status of the cleanup procedure is displayed when the operation is completed.

See also

[Full, incremental and differential backups](#)

"Deleting backups and replicas" (p. 110)

"Cleaning up space on Acronis Cloud" (p. 163)

¹A 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.

²A differential backup version stores changes to the data against the latest full backup version. You need access to the corresponding full backup version to recover the data from a differential backup version.

³A backup version that stores changes to the data against the latest backup version. You need access to other backup versions from the same backup to restore data from an incremental backup version.

Recovering data

Recovering disks and partitions

Recovering your system after a crash

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

Trying to determine the crash cause

A system crash can be due to two basic factors:

- **Hardware failure**

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

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

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

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

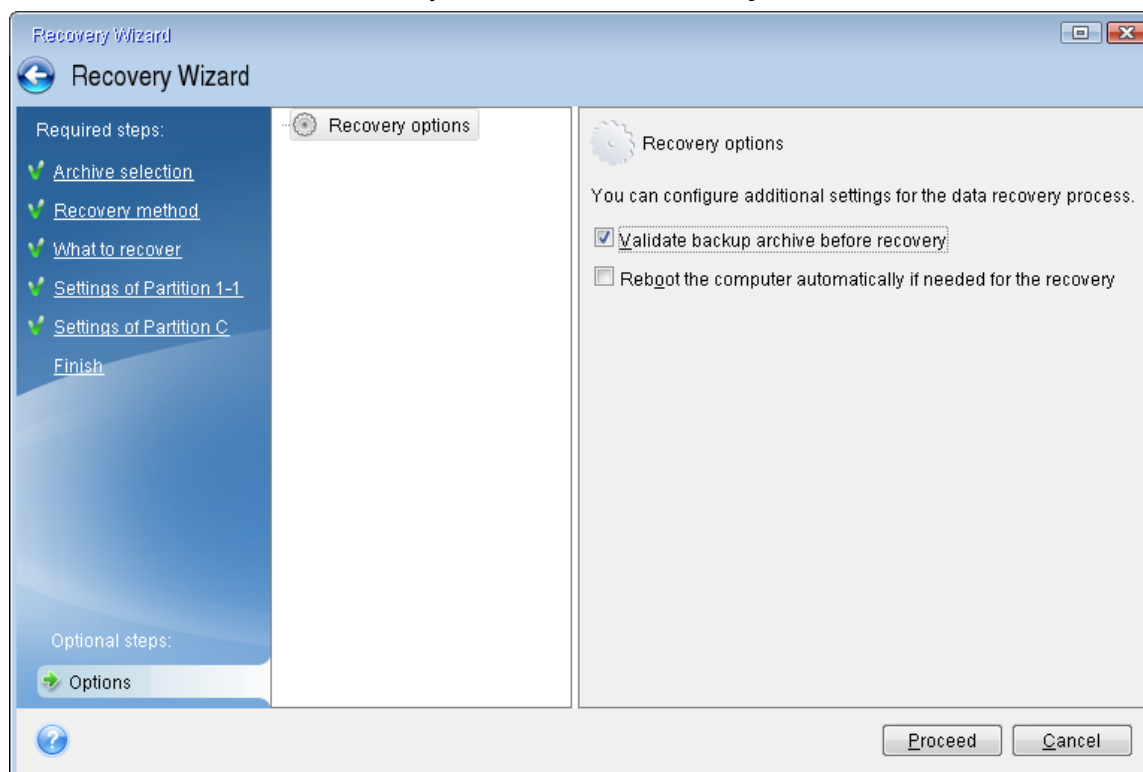
Preparing for recovery

We recommend that you perform the following actions before recovery:

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

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

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



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

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

Recovering your system to the same disk

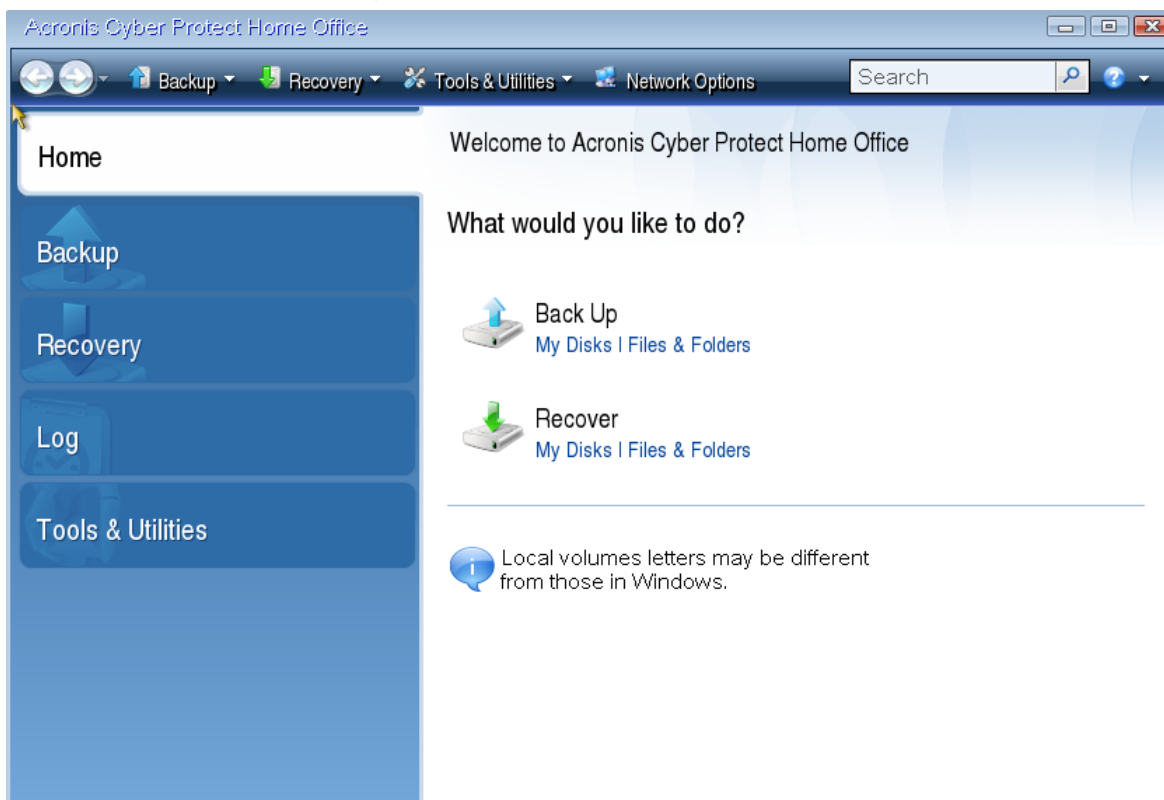
Before you start, we recommend that you complete the procedures described in [Preparing for recovery](#).

To recover your system

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

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

3. Boot from Acronis bootable media and select **Acronis True Image**.
4. On the **Home** screen, select **My disks** below **Recover**.

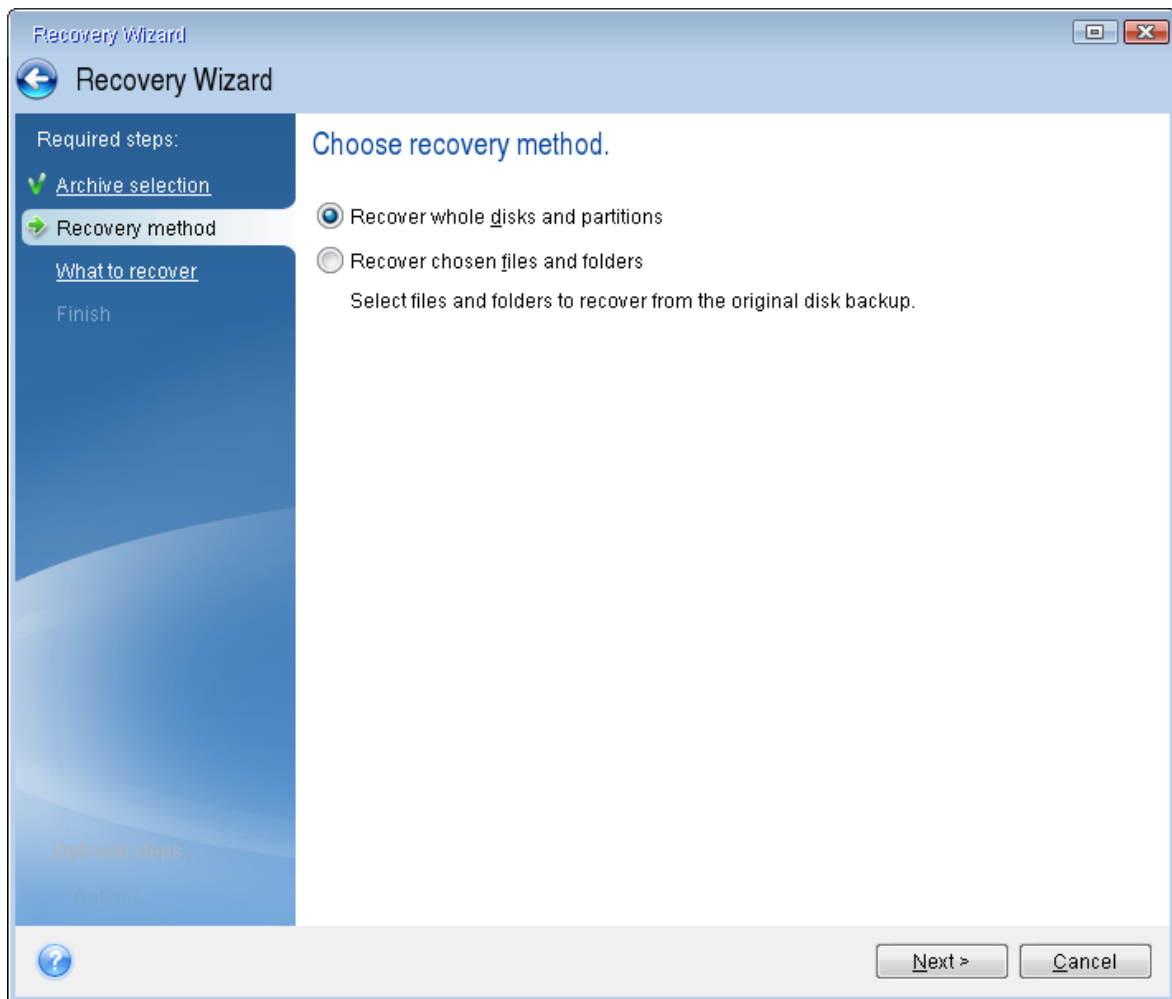


5. Select the system disk or partition backup to be used for recovery.
When the backup is not displayed, click **Browse** and specify path to the backup manually.

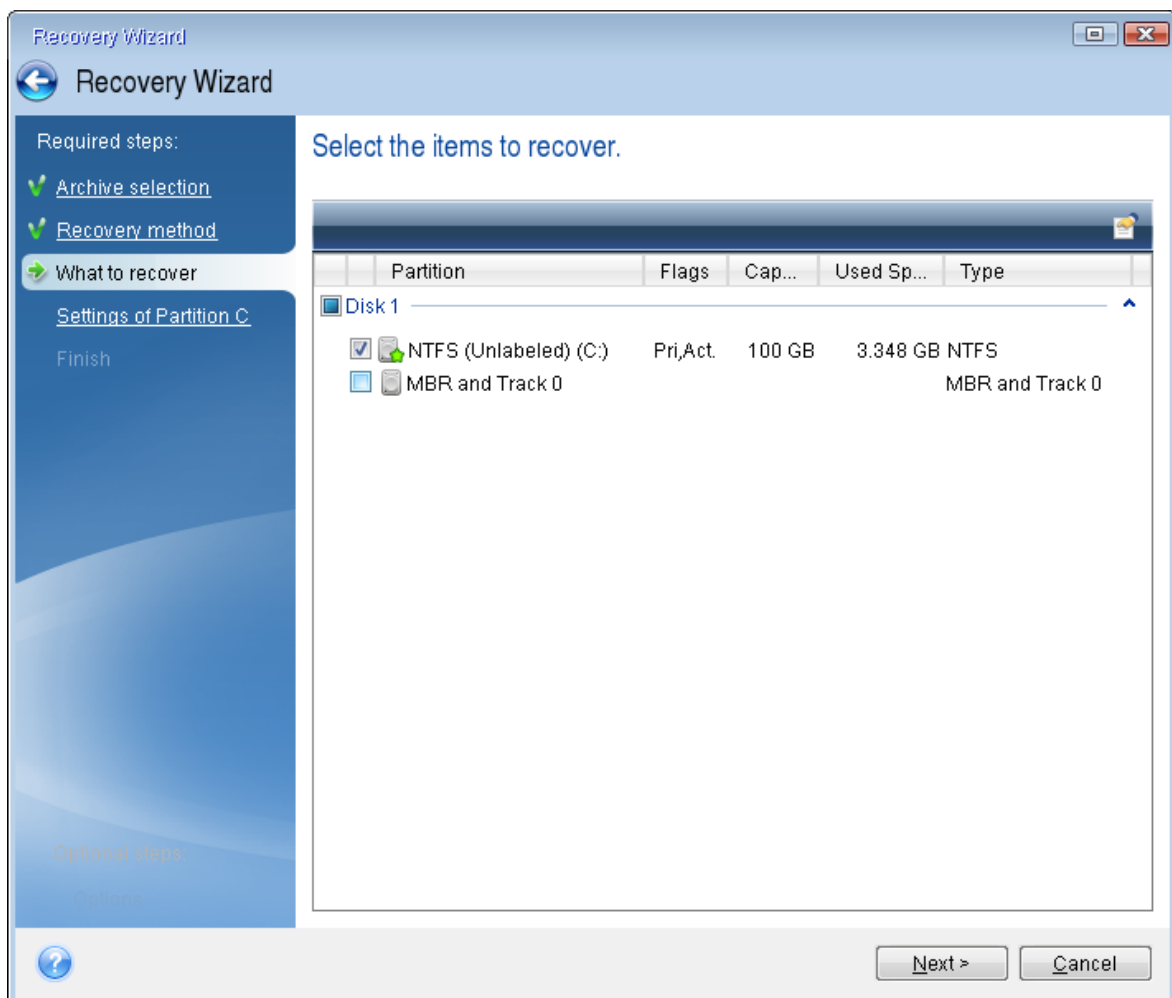
Note

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.

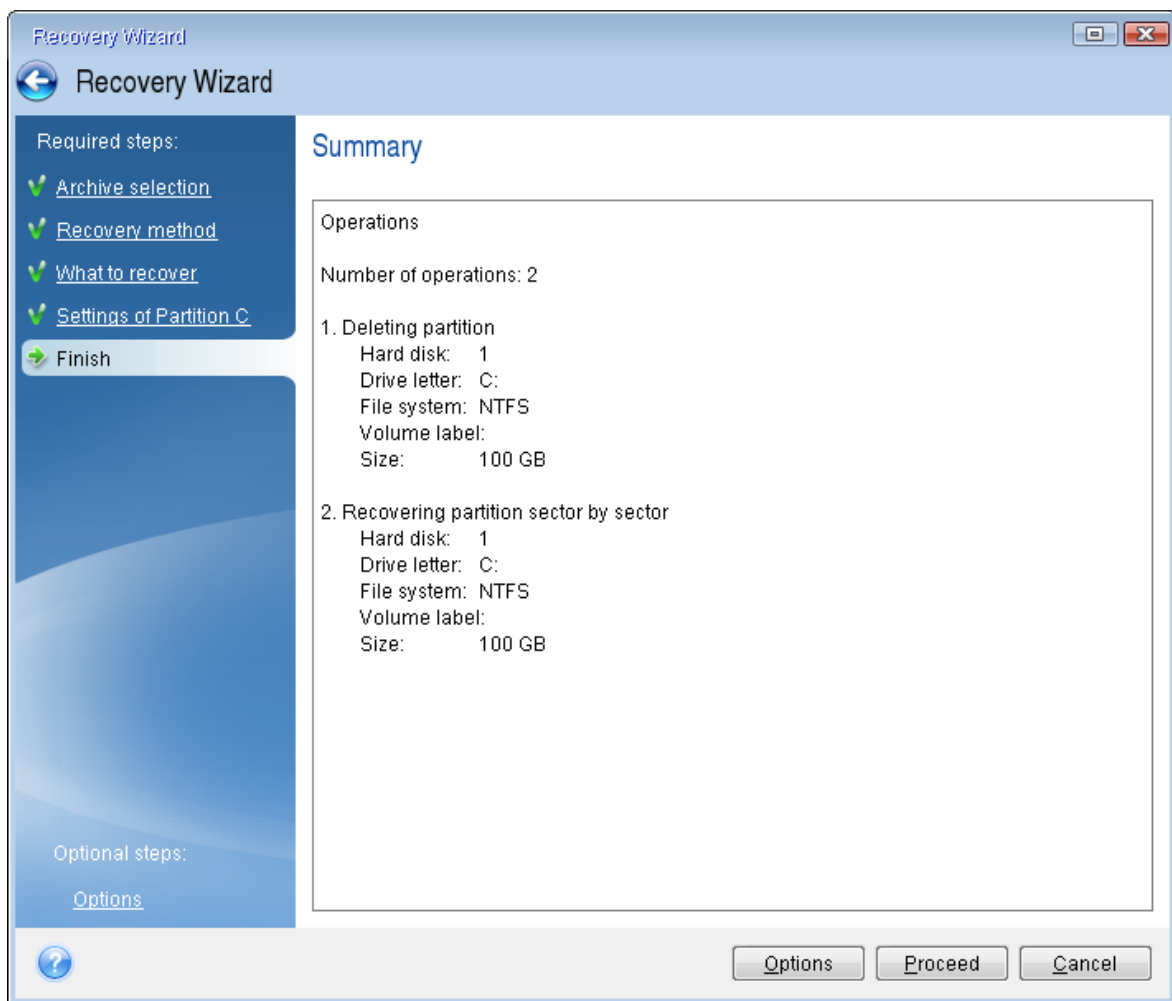
6. Select **Recover whole disks and partitions** at the **Recovery method** step.



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, 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

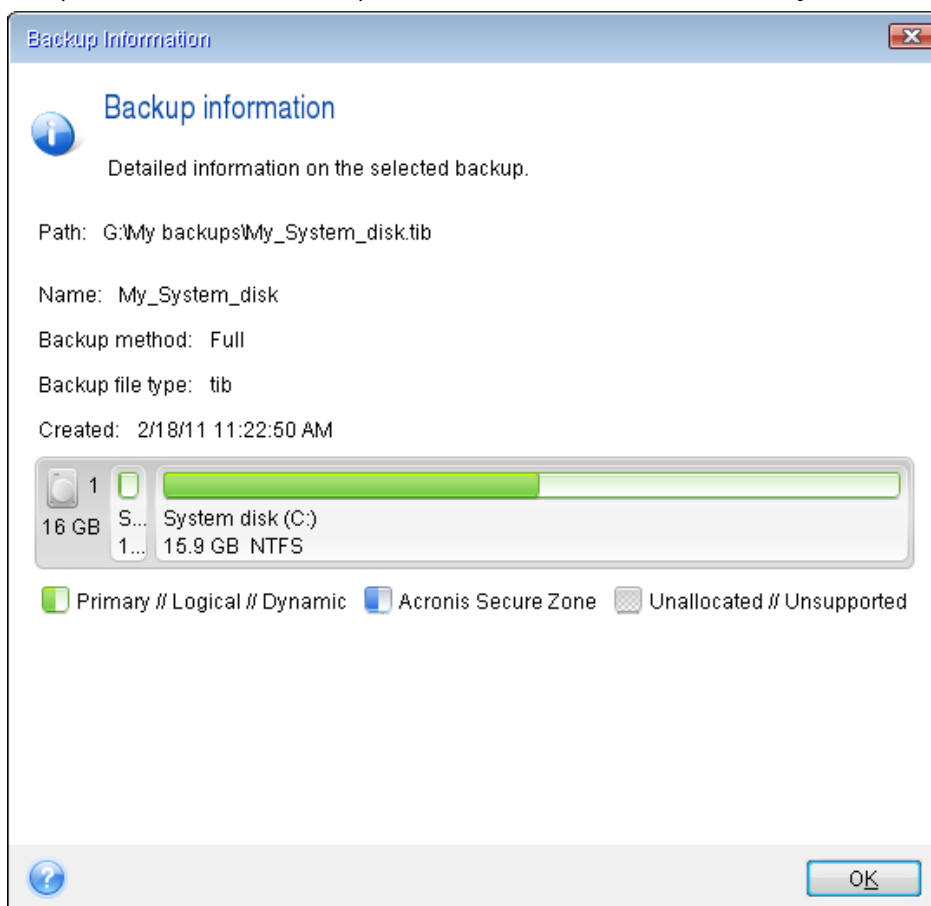
1. Install the new hard drive to the same position in the computer and use the same cable and connector that was used for the original drive. If this is not possible, install the new drive to where it will be used.
2. Attach the external drive if it contains the backup to be used for recovery and make 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**.
5. On the **Home** screen, select **My disks** below **Recover**.
6. Select the system disk or partition backup to be used for recovery. When the backup is not displayed, click **Browse** and specify path to the backup manually.

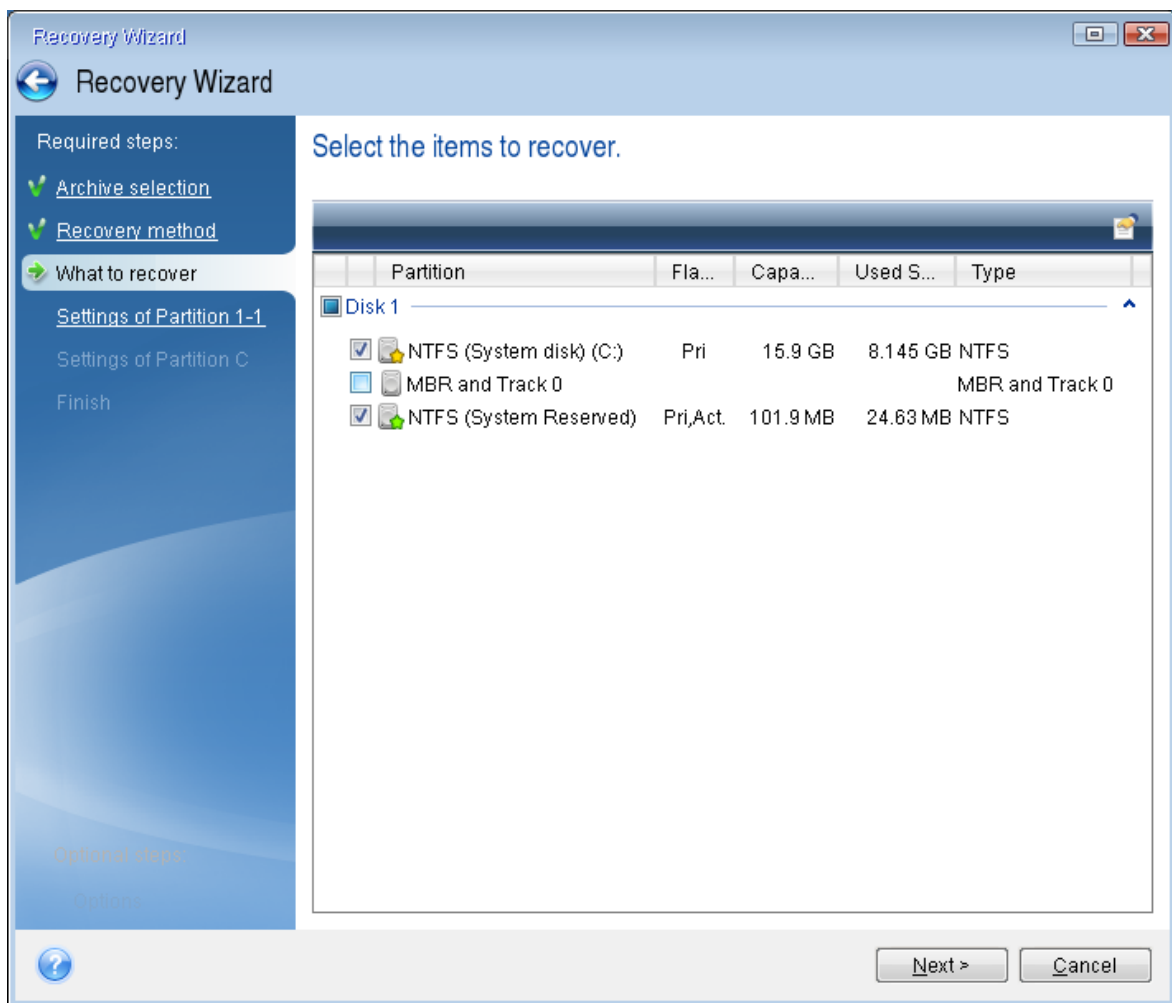
Note

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

7. If you have a hidden partition (for example, the System Reserved partition or a partition created by the PC manufacturer), click **Details** on the wizard's toolbar. Remember the location and size of the hidden partition, because these parameters need to be the same on your new disk.

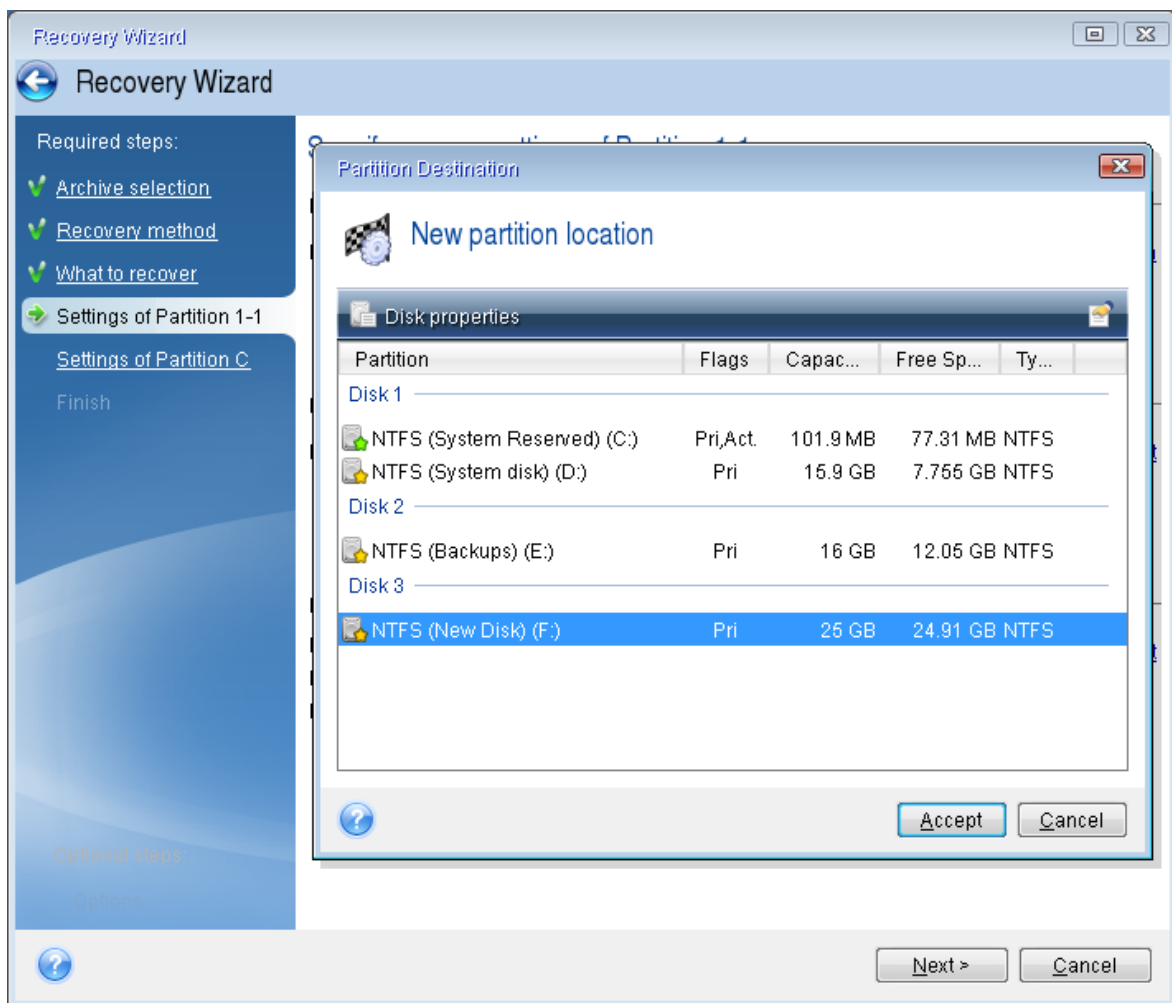


8. Select **Recover whole disks and partitions** at the **Recovery method** step.
9. On the **What to recover** step, select the boxes of the partitions to be recovered.
If you select an entire disk, MBR and Track 0 of the disk will also be recovered.

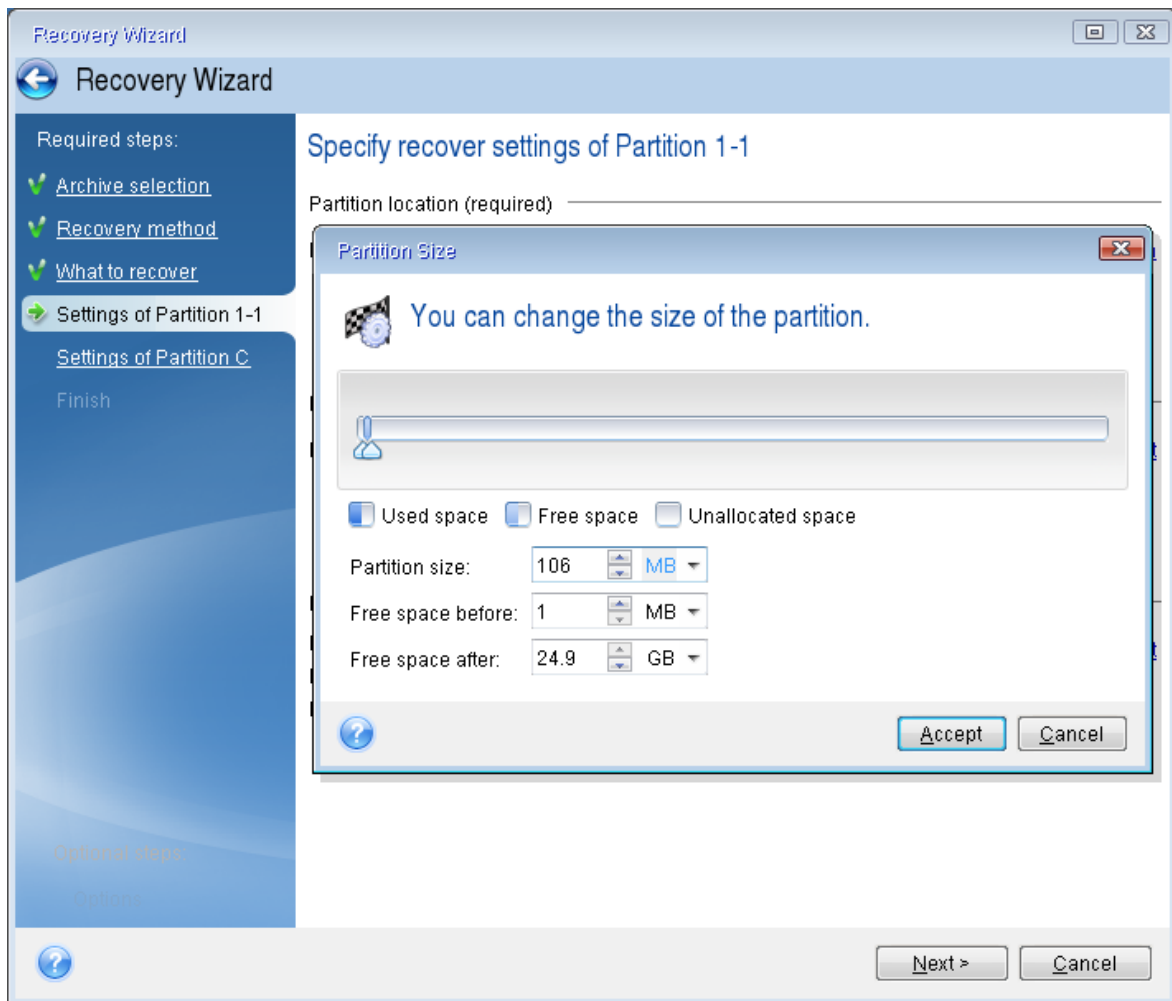


Selecting partitions leads to appearance of the relevant steps **Settings of partition**. Note that these steps start with partitions which do not have an assigned disk letter (as usually is the case with hidden partitions). The partitions then take an ascending order of partition disk letters. This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

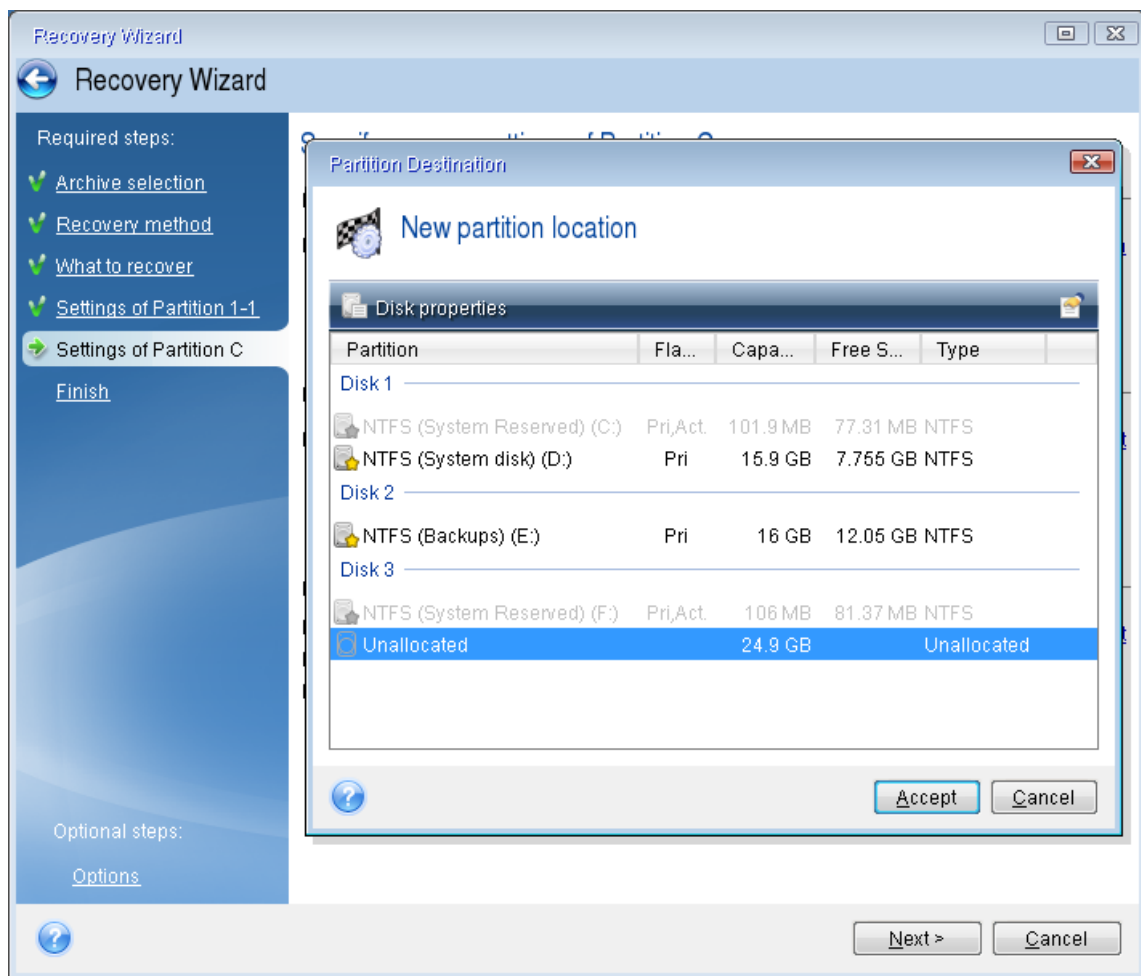
10. On the Settings of the hidden partition step (usually named Settings of Partition 1-1), specify the following settings:
 - **Location** – Click **New location**, select your new disk by either its assigned name or capacity, and then click **Accept**.



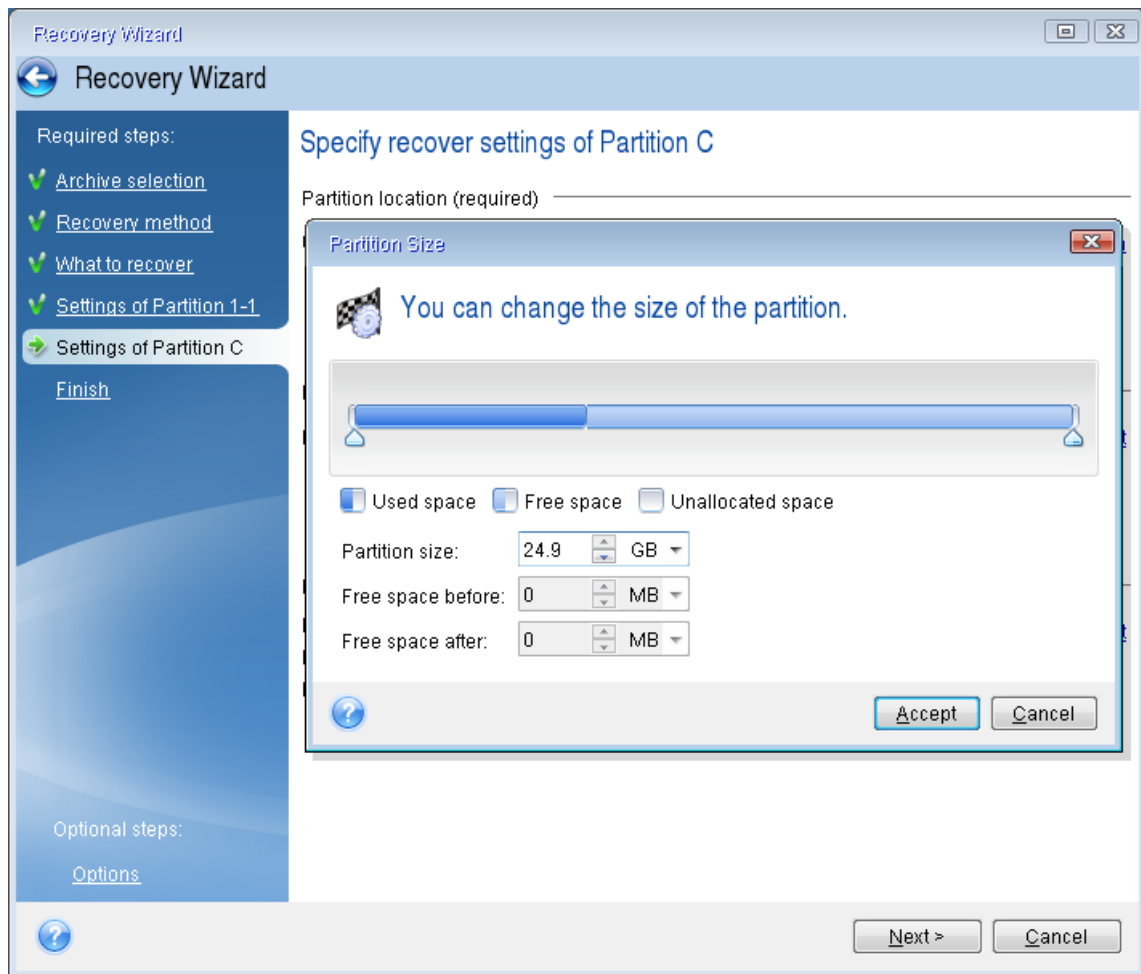
- **Type** – Check the partition type and change it, if necessary. Ensure that the System Reserved partition (if any) is primary and marked as active.
- **Size** – Click **Change default** in the Partition size area. By default the partition occupies the entire new disk. Enter the correct size in the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



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



- Change the partition type, if necessary. The system partition must be primary.
- Specify the partition size, which by default equals the original size. Usually there is no free space after the partition, so allocate all the unallocated space on the new disk to the second partition. Click **Accept**, and then click **Next**.



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

When the recovery is complete

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

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

Acronis Universal Restore

When you recover your system to dissimilar hardware, the target computer could fail to boot. This is because the new hardware is incompatible with critical drivers included in the image. Acronis Universal Restore will help you make the target computer bootable. See [Acronis Universal Restore](#) for details.

Recovering partitions and disks

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

Note

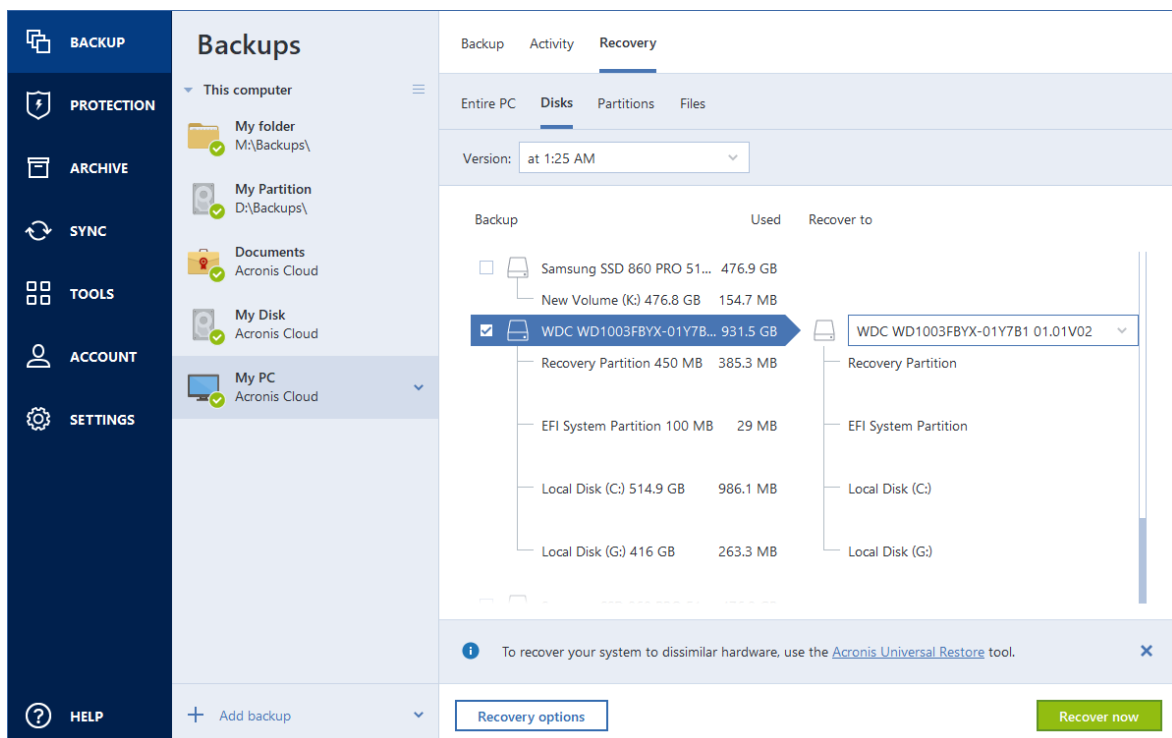
Before starting disk or partition recovery, make sure that the target disk has the same logical sector size as the original disk. Recovery to a disk with a different logical sector size is not supported and will fail. Older drives usually use a logical sector size of 512 bytes, while many newer HDDs and SSDs use 4096 bytes (depending on the drive and controller configuration).

Note

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

To recover partitions or disks

1. Start Acronis True Image.
2. If you want to recover your data from Acronis Cloud, make sure that you are signed in to your Acronis account.
3. 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**.
4. In the **Backup version** list, select the backup version you want to recover by its backup date and time.



5. Select the **Disks** tab to recover disks or **Partitions** tab to recover specific partitions. Select the objects you need to recover.
6. 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.

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

Partition properties

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

Manage Partition

×

Letter

G

Label

New Volume

Type

Primary

Used: 1.2 GB

Partition size:

9.0

GB

Unallocated space

Place after partition

7.0

GB

i

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

Ok

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.

Unified Extensible Firmware Interface (UEFI)

With Acronis True Image you also can convert **BIOS** to **UEFI** systems.

What is UEFI?

Unified Extensible Firmware Interface (UEFI) is a specification that provides a better software interoperability by setting standard syntax for boot and runtime services. For more information on UEFI, visit <https://www.uefi.org>.

The following operating systems support UEFI technology:

- Windows 10 (x86) and later x86 editions of Windows.
- Windows 10 (x64) and later x64 editions of Windows.

Why UEFI?

- **Compatibility with BIOS** - UEFI-based systems still can boot BIOS-based operating systems due to a Compatibility Support Module (CSM).
- **Booting from large disks** - UEFI-based systems support a GPT partitions layout that allows a disk size larger than 2^{32} sectors.
- **CPU-independent architecture** - UEFI is similar for all processor architectures.
- **CPU-independent drivers** - UEFI specification includes an EFI Byte Code (EBC) and allows creating EBC images (drivers), that can be run on any system.
- **Flexible pre-OS environment** - UEFI-based systems can boot on any hardware.
- **Modular design** - UEFI allows updating its single component while not affecting the others.

Note

Since UEFI is a new technology, not all systems support working with it. Please, apply to your hardware manufacturer to find out, whether your computer supports UEFI.

How to enable UEFI in BIOS?

Below a typical approach to turn on/off UEFI in BIOS is described:

1. Enter a BIOS setup program by pressing a key, mentioned in a message on the screen, during boot-up. Usually this key is [Del] or [F2].
2. Invoke a **Boot Options** menu using arrow keys.
3. Enter **UEFI Booting** item and select *Enable* (or *Disable* if you need to turn **OFF** UEFI in your system).
4. Navigate to **Save & Exit Setup** and press **Enter** to save changes and boot the system.

If you need assistance with turning UEFI on, contact your hardware manufacturer.

How to migrate an original system to a larger hard drive?

Acronis True Image now allows migrating or restoring systems from a previously created archive, to hard drives larger than 2^{32} bytes (2 TB for disks with standard 512-bytes sized logical sector or 16 TB for disks with 4 KB (4096-bytes) sized logical sector).

You can do it using Acronis media or booting to UEFI-based operating systems with Acronis True Image installed:

To migrate a system using Acronis Media

1. Boot your system from an Acronis media.
2. Select **Acronis True Image (Full version)** in the boot menu to continue booting from the media.
3. Navigate to the required wizard (**Restore** or **Clone**) and follow instructions.

To migrate a system in UEFI-based operating system

1. Boot to an UEFI-capable Windows operating system.
2. Run Acronis True Image, go to the **Backup and recovery** tab, click **Recover** on the toolbar and follow instructions.

Partition layouts

A partition layout defines how an operating system organizes partitions on a hard drive:

- **MBR (Master Boot Record)** - a legacy partitioning scheme that uses a 512-byte boot sector to store the primary partition table of the disk.
MBR is supported by all modern operating systems but is considered outdated. Its main limitation is that it supports hard disk's size up to 2 TB only, that makes it impossible to use modern large size hard drives - the space beyond 2 TB remains inaccessible for the users.
- **GPT (GUID Partition Table)** - a modern standard for partition layout used by default on UEFI-based systems. GPT supports disks and partitions up to 9.4 ZB (9.4×10^{21} bytes) and overcomes the limitations of MBR.

The table below displays which operating systems support reading GPT disks and/or booting from such a disk:

	OS can read GPT disks	OS can boot from GPT disks
Windows 10 x32	YES	YES
Windows 10 x64	YES	YES
Windows 11	YES	YES

Table 1. Destination disk is larger than 2 TB

A table below displays the available options if you want to migrate a source disk to a large size (more than 2 TB) hard disk.

If your source disk is MBR, you have to select whether you want the destination disk to remain MBR, or you want to convert it to GPT using Acronis True Image.

Each selection has its own advantages and limitations depending on your system parameters. Mostly it concerns the destination disk's bootability and capability of using the entire space on large disks.

	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	The partition style will remain MBR after cloning, Acronis Bus driver will be installed to the cloned operating system. Also, you will not be able to use the disk	<i>You can select one of the required migration methods:</i> • Copy a source partition without changes

support UEFI	space beyond 2 TB since MBR does not support hard drives larger than 2 TB. To use the entire disk space, you need to change a partition style to GPT or restart Acronis True Image after operation completion and use Acronis Extended Capacity Manager to make disk space beyond 2 TB visible for Add New Disk tool.	The partition style will remain MBR, but on operation completion, the operating system will not boot from UEFI. Acronis Bus driver will be installed to the cloned operating system. Also, you will not be able to use the disk space beyond 2 TB since MBR does not support hard drives larger than 2 TB. To use the entire disk space, you need to change a partition style to GPT or restart Acronis True Image after operation completion and use Acronis Extended Capacity Manager to make disk space beyond 2 TB visible for Add New Disk tool. • Convert the partition style to GPT The destination partition will be converted to GPT style. It can be used as a non-system disk, because your operating system does not support UEFI. The entire disk space will be available.
My source disk is MBR and my OS supports UEFI	The partition style will remain MBR after migration. Acronis Bus driver will be installed to the cloned operating system. You will not be able to use the disk space beyond 2 TB since MBR does not support hard drives larger than 2 TB. To use the entire disk space, you need to change a partition style to GPT or restart Acronis True Image after operation completion and use Acronis Extended Capacity Manager to make disk space beyond 2 TB visible for Add New Disk tool.	A partition style on your destination disk will be converted to GPT automatically. This disk may be used for booting in UEFI. Also, the entire disk space will be available.
My source disk is MBR and OS is non-Windows, or no OS	<i>You can select one of the required migration methods:</i> • Copy a source partition without changes The partition style will remain MBR, but you will not be able to use the disk space beyond 2 TB since MBR does not support hard drives larger than 2 TB. To use the entire disk space, you need to change a partition style to GPT or restart Acronis True Image after operation completion and use Acronis Extended Capacity Manager to make disk space beyond 2 TB visible for Add New Disk tool.	<i>You can select one of the required migration methods:</i> • Copy a source partition without changes The partition style will remain MBR, but you will not be able to use the disk space beyond 2 TB since MBR does not support hard drives larger than 2 TB. To use the entire disk space, you need to change a partition style to GPT or restart Acronis True Image after operation completion and use Acronis Extended Capacity Manager to make disk space beyond 2 TB visible for Add New Disk tool. • Convert the partition style to GPT

	• Convert the partition style to GPT On operation completion, partition style will be converted to GPT. The destination disk cannot be used for booting, since no Windows operating system is installed on your source disk. The entire disk space will be available.	The destination partition will be converted to GPT style. The destination disk cannot be used for booting, since no Windows operating system is installed on your source disk. Also, the entire disk space will be available.
My source disk is GPT and my OS supports UEFI	The partition style will remain GPT after migration. After operation completion, the system will fail booting from BIOS, because your operating system cannot support booting from GPT on BIOS. The entire disk space will be available.	The operation will not affect neither partition layout nor bootability of the disk: partition style will remain GPT, the destination disk will be bootable in UEFI. The entire disk space will be available.
My source disk is GPT and OS is non-Windows, or no OS	The operation will not affect neither partition layout nor bootability of the disk: partition style will remain GPT, the destination disk will not be bootable. The entire disk space will be available.	The operation will not affect neither partition layout nor bootability of the disk: partition style will remain GPT, the destination disk will not be bootable in UEFI. The entire disk space will be available.

Table 2. Destination disk is less than 2 TB

A table below displays the available option if you want to migrate a source disk to a hard disk less than 2 TB.

If your source disk is MBR, you have to select whether you want the destination disk to remain MBR, or you want to convert it to GPT using Acronis True Image.

Each selection has its own advantages and limitations depending on your system parameters. Mostly it concerns a destination disk's bootability.

	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. The entire disk space will be available.	After operation completion, the partition style will remain MBR, 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 entire disk space will be available.	The destination partition will be converted to GPT style that will make the destination disk bootable in UEFI. The entire disk space will be available.
My source	<i>You can select one of the required migration</i>	<i>You can select one of the required</i>

disk is MBR and OS is non-Windows, or no OS	<i>methods:</i> • Copy a source partition without changes The partition style will remain MBR. The destination disk will not be bootable, because there is no Windows operating system detected in your system. • Convert the partition style to GPT The destination disk will be converted to GPT style and used as a non-system disk, because your operating system does not support booting from GPT on BIOS.	<i>migration methods:</i> • Copy a source partition without changes The partition style will remain MBR. The destination disk will not be bootable, because there is no Windows operating system detected in your system. • Convert the partition style to GPT The destination partition will be converted to GPT style and used as a non-system disk, because there is no Windows operating system detected in your 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.
My source disk is GPT and OS is non-Windows, or no OS	After operation completion, the partition style will remain GPT, the system will fail booting from BIOS, because your operating system does not support booting from GPT on BIOS.	After operation completion, the partition style will remain GPT, the system will fail booting, because there is no Windows operating system detected in your system.

Migration method

Acronis True Image allows you to select a partition layout for a target disk after recovery operation completion:

- **MBR (Master Boot Sector)** - a 512-byte boot sector, which is the first sector of a hard disk, used to hold a disk's primary partition table.
- **GPT (GUID Partition Table)** - a standard for a partition table layout for hard disks. GPT allows disks/partitions size up to 9.4 ZB (9.4 x 10²¹ bytes).

Using this wizard you may convert your partitions layout while recovering or recover them as is, not changing the layout.

- **Copy partitions without changes** - select this option to migrate your system as is, not changing the partition layout. Note, in this case the disk space in excess of 2TB will be inaccessible. To allocate the disk space beyond 2TB, you may use Acronis Extended Capacity Manager.
- **Copy partitions and use a disk as non-system, GPT style** - select this option to convert your partition to a GPT layout.

With Acronis True Image you also can convert **BIOS** to **UEFI** systems.

BIOS-booted system, MBR, UEFI not supported

In this step of the wizard, you need to select the destination hard disk.

Currently your system contains:

System: BIOS-booted

Source partition style: MBR

Operating system on the source disk: Windows, booting in UEFI is not supported

Destination disk size: less than 2 TB

If you migrate the system to the selected disk:

System: BIOS-booted

Partition style: MBR

Operating system: Windows, booting in UEFI is not supported

Disk size: the entire disk space is available

You can find more information about the migration procedure in [Migration method](#) section.

BIOS-booted system, MBR, UEFI supported

In this step of the wizard, you need to select the destination hard disk.

Currently your system contains:

System: BIOS-booted

Source partition style: MBR

Operating system on the source disk: Windows, booting in UEFI is supported

Destination disk size: less than 2 TB

If you migrate the system to the selected disk:

System: BIOS-booted

Partition style: MBR

Operating system: Windows, booting in UEFI is supported

Disk size: the entire disk space is available

You can find more information about the migration procedure in [Migration method](#) section.

BIOS-booted system, MBR, no Windows

Acronis True Image allows you to select a partition layout for a destination disk after the operation completion.

Currently your system contains:

System: BIOS-booted

Source partition style: MBR

Operating system on the source disk: non-Windows or no OS

Destination disk size: less than 2 TB

With these system parameters, you can select one of the following:

1. Copy partitions without changes

You may leave MBR partition style on the destination disk.

Destination disk after migration:

System: BIOS-booted

Partition style: MBR

Operating system: non-Windows or no OS

Disk size: the entire disk space is available

2. Copy partitions and use a disk as non-system, GPT style

You may convert the partition style to GPT.

Destination disk after migration:

System: not bootable in BIOS

Partition style: GPT

Operating system: non-Windows or no OS

Disk size: the entire disk space is available

Warning!

After migration, the destination disk can be used only as non-system. This option is not available if Acronis True Image is run in Windows XP x32 operating system.

You can find more information about the migration procedure in [Migration method](#) section.

BIOS-booted system, GPT, UEFI supported

In this step of the wizard, you need to select the destination hard disk.

Currently your system contains:

System: BIOS-booted

Source partition style: GPT

Operating system on the source disk: Windows, booting in UEFI is supported

If you migrate the system to the selected disk:

System: not bootable in BIOS

Partition style: GPT

Operating system: Windows, booting in UEFI is supported

Disk size: the entire disk space is available

Warning!

After migration, the operating system will not be able to boot from the destination disk in BIOS. If you want to boot from the destination disk after migration, you need to enable UEFI booting in your system (see Unified Extensible Firmware Interface section), and then restart the operation.

You can find more information about the migration procedure in [Migration method](#) section.

BIOS-booted system, GPT, no Windows

In this step of the wizard, you need to select the destination hard disk.

Currently your system contains:

System: BIOS-booted

Source partition style: GPT

Operating system on the source disk: non-Windows or no OS

If you migrate the system to the selected disk:

System: BIOS-booted

Partition style: GPT

Operating system: non-Windows or no OS

Disk size: the entire disk space is available

You can find more information about the migration procedure in [Migration method](#) section.

UEFI-booted system, MBR, UEFI not supported

In this step of the wizard, you need to select the destination hard disk.

Currently your system contains:

System: UEFI-booted

Source partition style: MBR

Operating system on the source disk: Windows, booting in UEFI is not supported

Destination disk size: less than 2 TB

If you migrate the system to the selected disk:

System: not bootable in UEFI

Partition style: MBR

Operating system: Windows, booting in UEFI is not supported

Disk size: the entire disk space is available

Warning!

The operating system may fail booting in UEFI from the destination disk.

You can find more information about the migration procedure in [Migration method](#) section.

UEFI-booted system, MBR, UEFI supported

In this step of the wizard, you need to select the destination hard disk.

Currently your system contains:

System: UEFI-booted

Source partition style: MBR

Operating system on the source disk: Windows, booting in UEFI is supported

If you migrate the system to the selected disk:

After migration, the destination partition style will be converted to GPT and you will be able to boot from it.

Destination disk after migration:

System: UEFI-booted

Partition style: GPT

Operating system: Windows, booting in UEFI is supported

Disk size: the entire disk space is available

You can find more information about the migration procedure in [Migration method](#) section.

UEFI-booted system, MBR, no Windows

Acronis True Image allows you to select a partition layout for a destination disk after the operation completion.

Currently your system contains:

System: UEFI-booted

Source partition style: MBR

Operating system on the source disk: non-Windows or no OS

Destination disk size: less than 2 TB

With these system parameters, you can select one of the following:

1. Copy partitions without changes

You may leave MBR partition style on the destination disk.

Destination disk after migration:

System: UEFI-booted

Partition style: MBR

Operating system: non-Windows or no OS

Disk size: the entire disk space is available

2. Copy partitions and use a disk as non-system, GPT style

You may convert the partition style to GPT.

Destination disk after migration:

System: not bootable in UEFI

Partition style: GPT

Operating system: non-Windows or no OS

Disk size: the entire disk space is available

Warning!

After migration, the destination disk can be used only as non-system.

You can find more information about the migration procedure in [Migration method](#) section.

UEFI-booted system, GPT, UEFI supported

In this step of the wizard, you need to select the destination hard disk.

Currently your system contains:

System: UEFI-booted

Source partition style: GPT

Operating system: Windows, booting in UEFI is supported

If you migrate the system to the selected disk:

System: UEFI-booted

Partition style: GPT

Disk size: the entire disk space is available

You can find more information about the migration procedure in [Migration method](#) section.

UEFI-booted system, GPT, no Windows

In this step of the wizard, you need to select the destination hard disk.

Currently your system contains:

System: UEFI-booted

Source partition style: GPT

Operating system: non-Windows or no OS

If you migrate the system to the selected disk:

System: UEFI-booted

Partition style: GPT

Disk size: the entire disk space is available

You can find more information about the migration procedure in [Migration method](#) section.

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

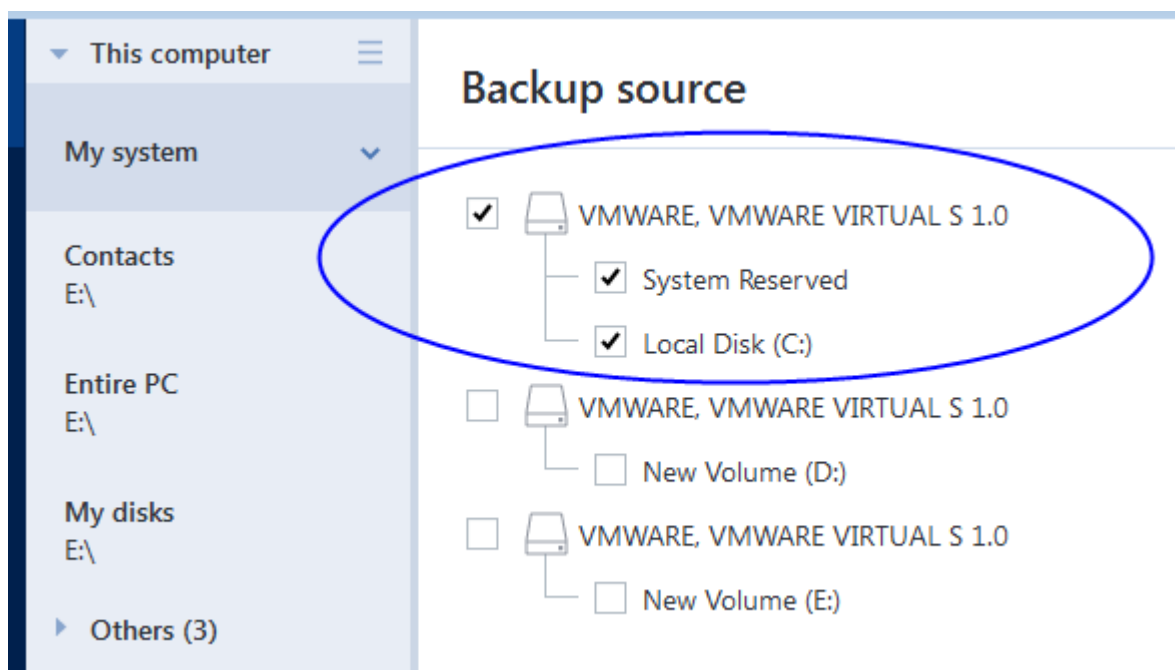
Here is an example for transferring a system with the following conditions:

- 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.**
See [Creating Acronis bootable media](#) for details.
- **Backup of your system disk created in disk mode.**

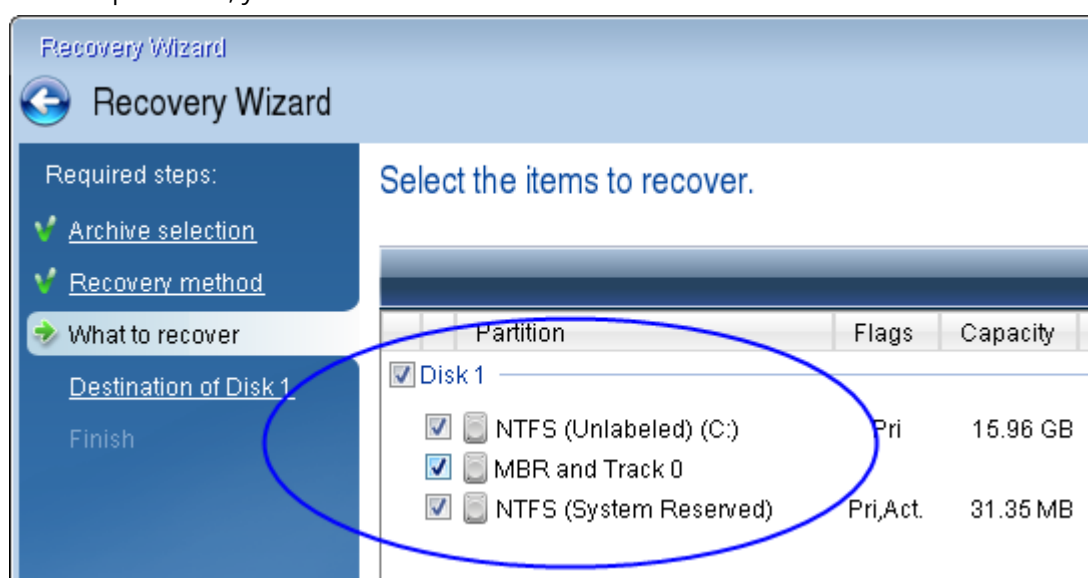
To create this backup, switch to disk mode, and then select the hard drive that contains your system partition. See [Backing up disks and partitions](#) for details.



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

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

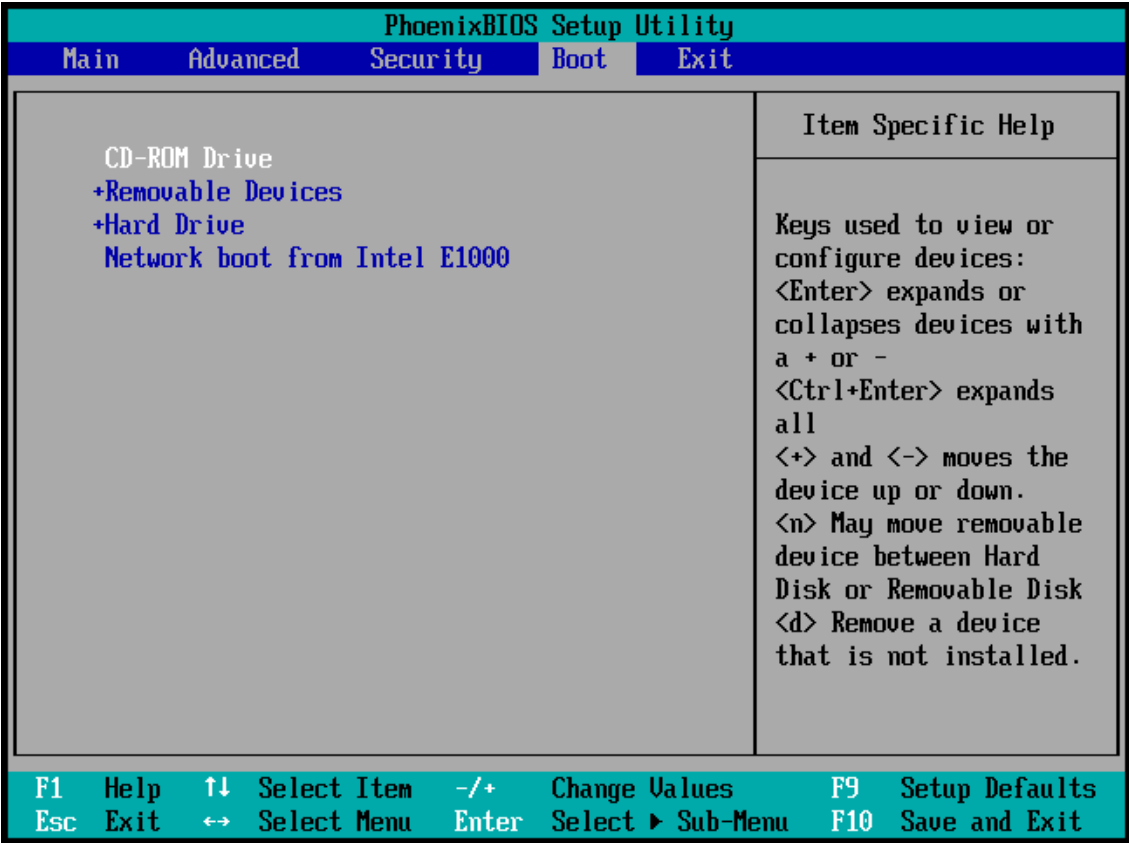
1. If you use a USB flash drive or external drive as a bootable media, plug it into the USB port.
2. Turn your computer on. During the Power-On Self Test (POST), you will see the key combination that you need to press in order to enter BIOS or UEFI BIOS.
3. Press the key combination (such as, **Del**,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

Disk recovery from Cloud

Disk recovery from Acronis Cloud is very similar to the recovery from an ordinary hard disk drive.

- When you can start Windows and Acronis True Image, see [Recovering partitions and disks](#).
- When Windows cannot start, see [Recovering your system from Acronis Cloud](#).

How it works

Your computer should be connected to the internet either by an Ethernet cable or via Wi-Fi. Acronis True Image supports several wireless security protocols, including WPA-Personal, WPA2-Personal, and WPA2-Enterprise.

Recovery to the original location

When you recover a disk to the original location, Acronis True Image does not download the entire disk space to your computer. Acronis True Image scans your disk searching for data changes and

recovers only those files that are different from files in the image. This technology significantly reduces the amount of data you need to download in order to recover your disk.

Recovery to a new location

When you recover a disk to a different location or to an unallocated space, the process is very similar to a recovery from a local storage. The only difference is in the data writing method. Acronis True Image downloads and writes data by separate blocks, and not continuously. This technology increases recovery speed and reliability of the entire process.

What if recovery has been interrupted

Since disk recovery from Acronis Cloud uses an internet connection and usually takes a long time, the probability of the recovery interruption is higher comparing to recovery from an ordinary hard disk.

Possible reasons of recovery interruption:

- internet connection has been lost.
- Connection to Acronis Cloud has been lost.
- You canceled the recovery, deliberately or accidentally.
- Electricity supply problem.

When recovery is not complete due to a connection problem, Acronis True Image automatically tries to reconnect to Acronis Cloud and resume the recovery process. It is recommended that you check your internet connection settings in this case. If all the automatic attempts fail, run the recovery again manually when connection is restored.

In other cases run recovery again manually and make sure the recovery is complete.

Regardless of an interruption reason, Acronis True Image does not start recovery from the very beginning. Acronis True Image resumes the process and downloads only the data that was not recovered.

Recovering your system from Acronis Cloud

Note

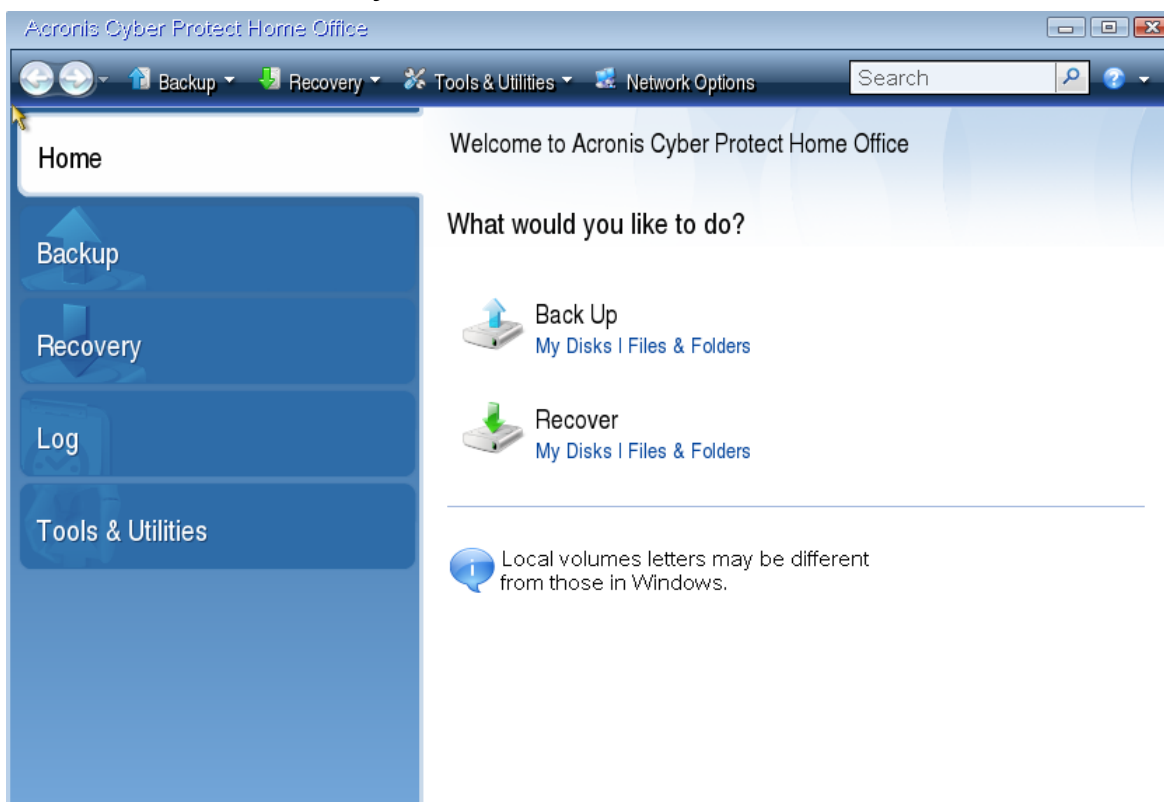
Depending on your internet connection speed, disk recovery from Acronis Cloud may take a long time.

Before you start, we recommend that you complete the preparations described in [Preparing for recovery](#). If you recover your system to a new disk, you do not need to format the new disk, as this will be done in the process of recovery.

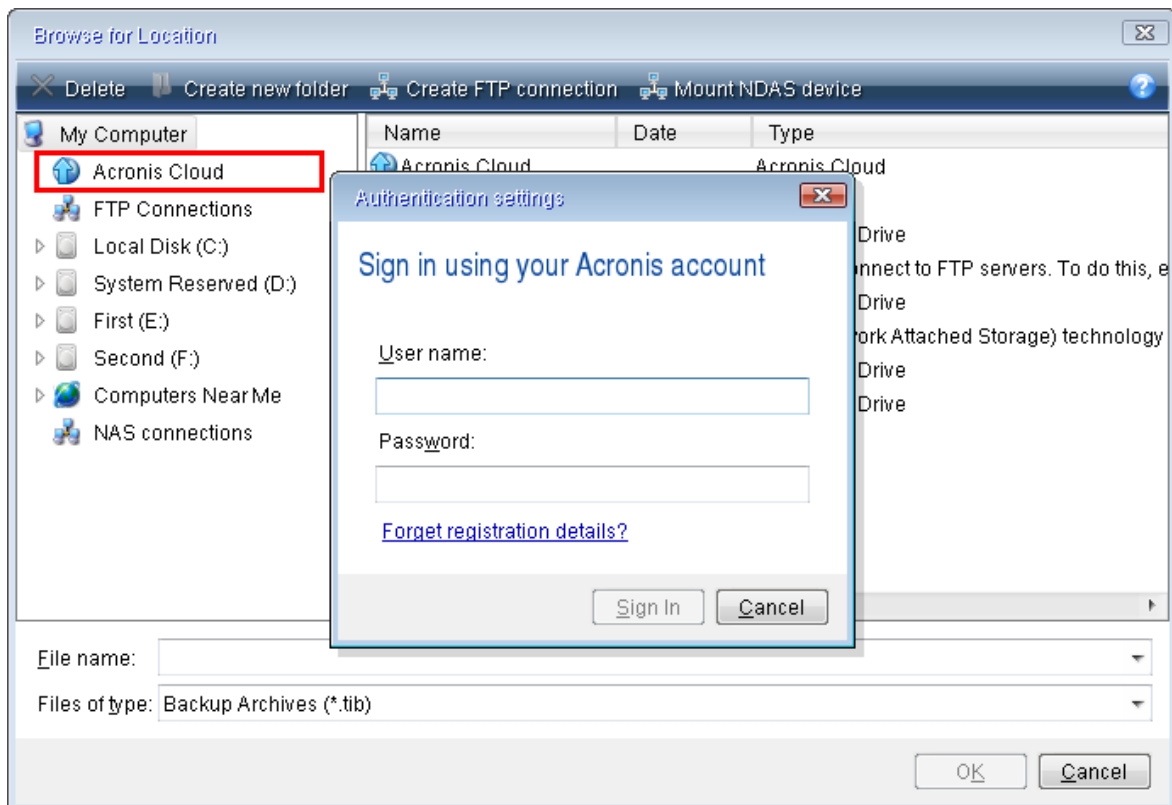
Before starting this procedure, make sure that your computer is connected to the internet by an Ethernet cable or over Wi-Fi.

To recover a system disk from Acronis Cloud

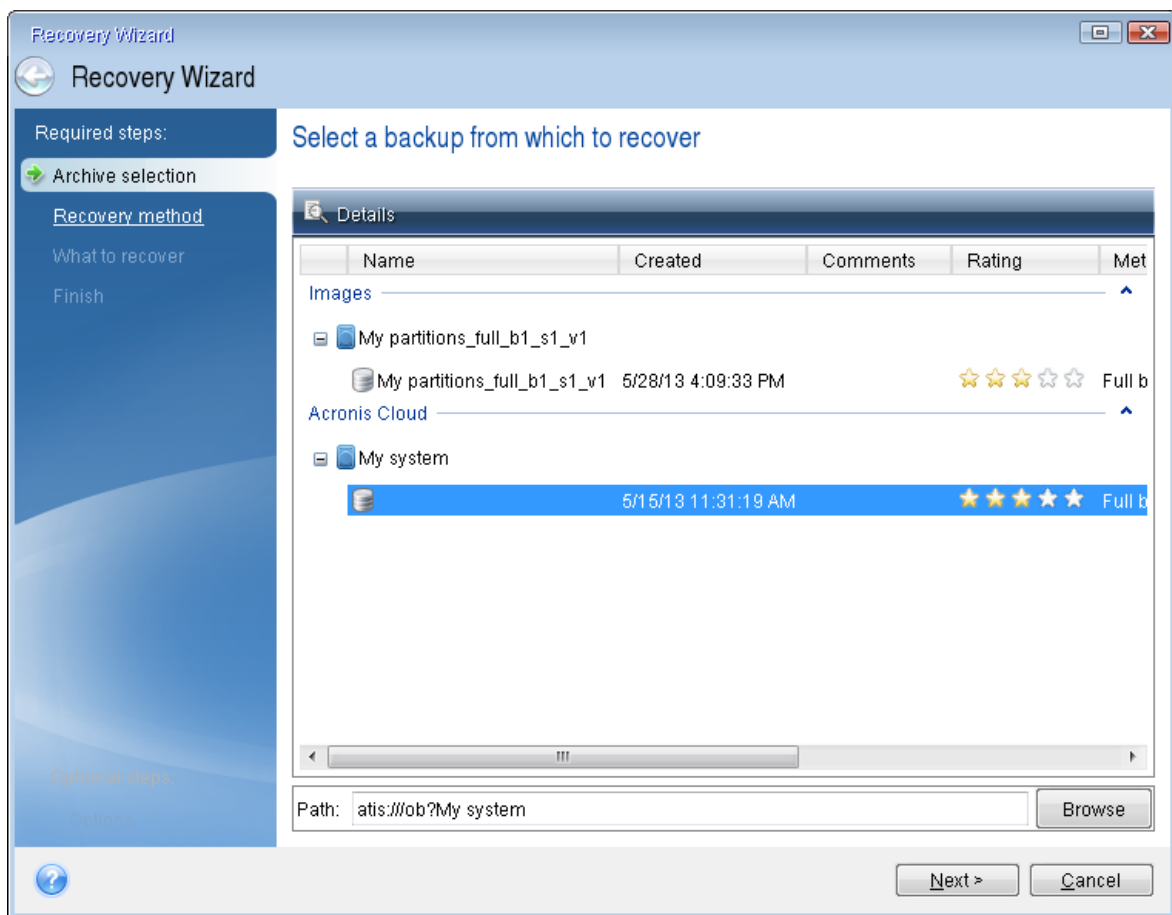
1. Arrange the boot order in BIOS so as to make your Acronis bootable media (CD, DVD or USB stick) the first boot device. See [Arranging boot order in BIOS](#).
2. Boot from the bootable media and select **Acronis True Image**.
3. On the **Home** screen, select **My disks** below **Recover**.



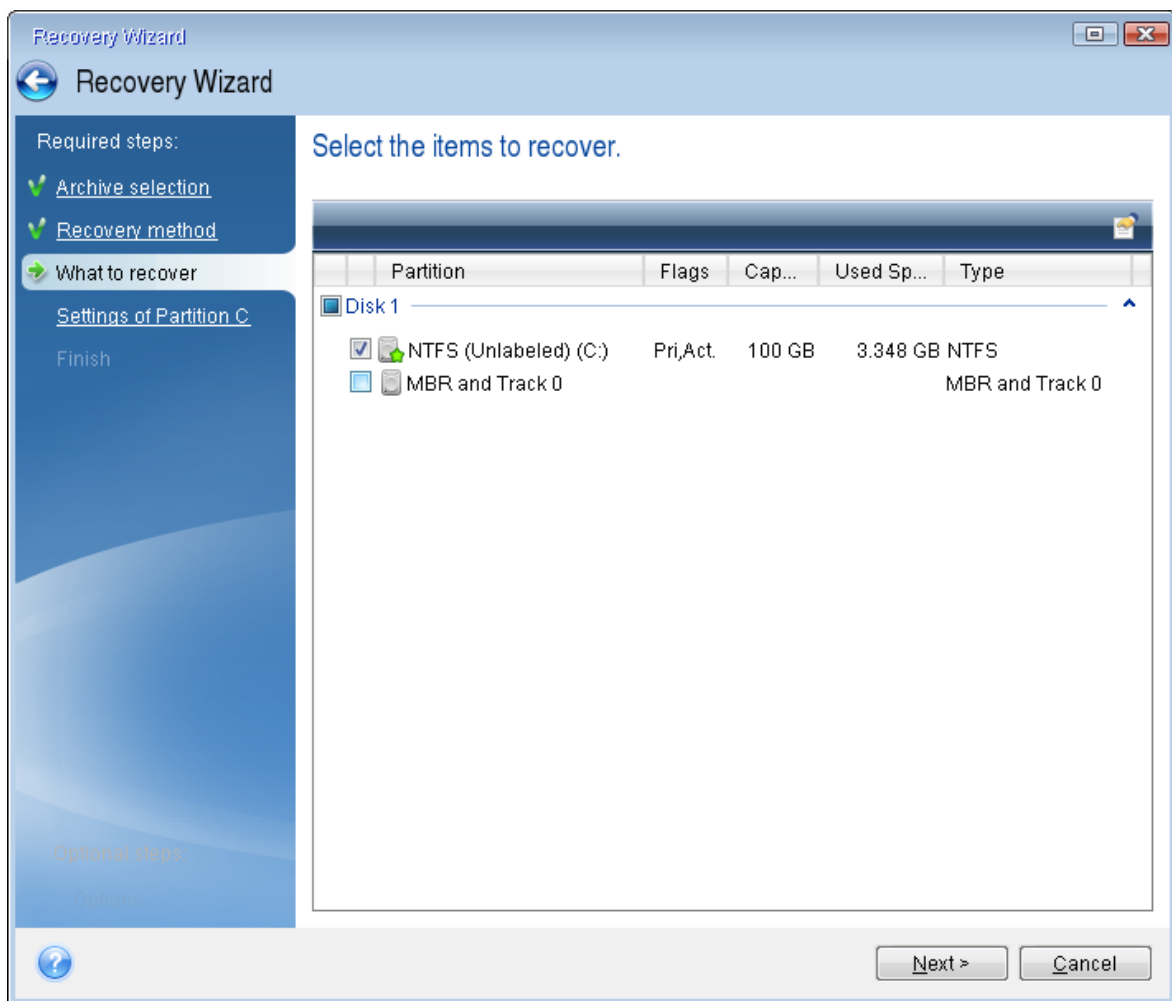
4. To add the online backup of the system disk or system partition to the list of available backups, click **Browse**.
5. In the directory tree of the opened window, select Acronis Cloud and enter credentials of your Acronis account.



6. Select the backup you want to use for recovery, and click **OK**.
7. On the **Archive selection** step, select the online backup and click **Next**.



8. On the **Recovery method** step, select **Recover whole disks and partitions**.
9. On the **What to recover** step, select the system partition (usually C) and the System Reserved partition (if any). You can also recognize these partitions by the **Pri, Act** flags.



10. On the **Settings of partition C** (or the letter of the system partition, if it is different) step, change the settings, if necessary. For example, you need to change settings when recovering to the new hard disk of a different capacity.
11. 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. Click **Proceed**.
12. When recovery is complete, exit the standalone version of Acronis True Image, remove the bootable media. Boot from the recovered system partition. After you check that you have recovered Windows to the state you need, [restore the original boot order](#).

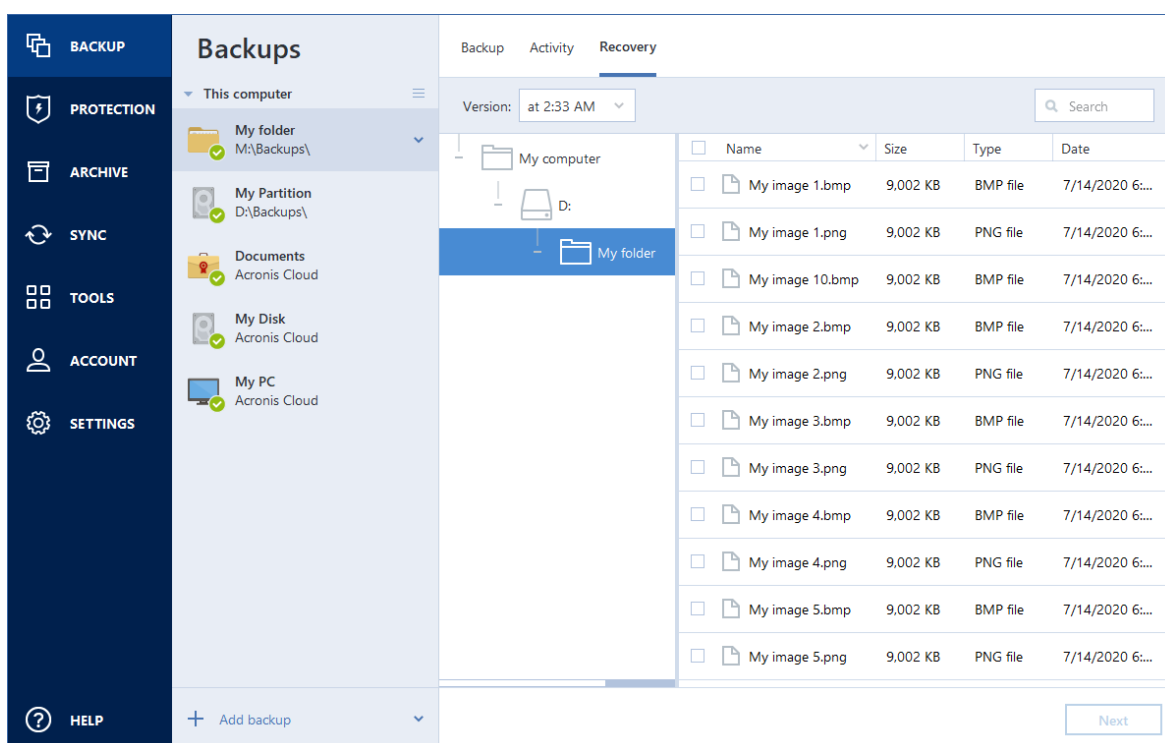
Recovering files and folders

You can browse and recover backed-up files and folders in Acronis True Image, in File Explorer, or in Acronis Cloud. You can recover files and folders both from file-level and disk-level backups.

To recover data in Acronis True Image

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.

- [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.
- Select the check box for the corresponding files or folders that you want to recover, and click **Next**.



- [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.

To recover data in Acronis Cloud

1. On left sidebar, click **BACKUPS**.
2. From the backups list, select the cloud backup which contains the files or folders that you want to recover.
3. From the list of files and folders, select the ones that you want to recover.
4. [Optional] You can recover a specific version of a file (not a folder). To do this, click **Versions** on the right sidebar, and then click the download icon on the required version line.
5. To start the recovery, click **DOWNLOAD** on the right sidebar.
The selected data will be copied to the default downloads folder.

Note

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

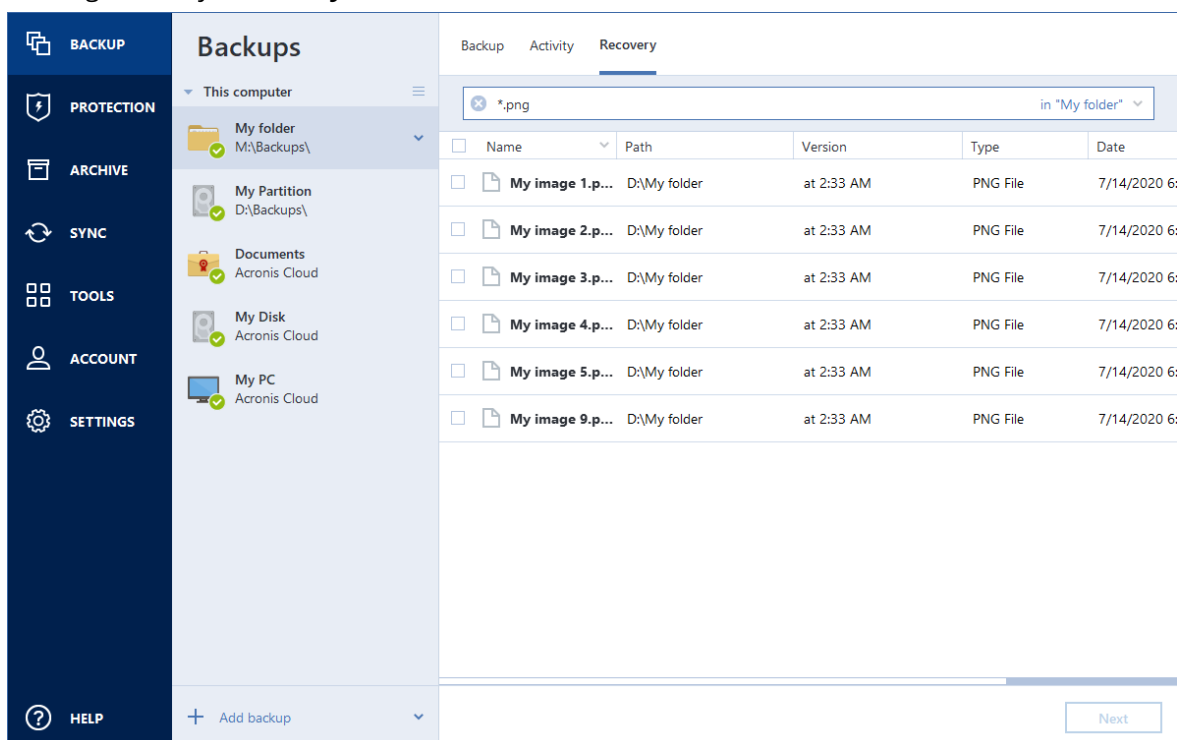
Searching backup content

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

To search for files and folders

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

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



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

Note

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

Recovering Microsoft 365 data

Acronis True Image allows you to protect your personal Microsoft 365 account from losing your e-mail messages, files and folders, profile information, and other data. When you have a cloud backup of your account data, you can browse it and recover specific items.

What items can be recovered?

The following items can be recovered from a mailbox backup:

- Entire mailbox
- E-mail messages
- Attachments

The following items can be recovered from a OneDrive backup:

- Entire OneDrive
- Any files and folders that were backed up

Recovering Microsoft 365 data

To browse and recover your data

1. Open Online Dashboard by doing one of the following:
 - Follow the link: <https://cloud.acronis.com>.
 - On the sidebar of Acronis True Image, click **Account**, and then click **Open Online Dashboard**.
2. Sign in to your Acronis account.
3. On the sidebar, click **Resources**, find the Microsoft 365 backup, and then click **Recover**.
4. Browse a list of your backups. If needed, use the filter to find a backup by content.
5. After selecting a backup, click **Recover...**, and choose the data that you want to restore:
 - Entire OneDrive or specific files and folders.
 - Entire mailbox or specific messages.

When you choose to recover specific items, the Online Dashboard opens the list of the backed-up items. You can browse them, view their contents, and use search to find a specific item (not available for some data types).

After selecting items, you can choose an operation to perform (depending on data type, some operations may be unavailable):

- **Show content** – click to view the item details or open it in full size.
- **Send as email** – click to send the message to selected recipients.
- **Show versions** – click to view the versions of the item.
- **Recover** – click to specify a location for the items that you recover. You can also recover sharing permissions for some items.
- **Download** – click to download the selected file.

6. Click **Start recovery**.

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.

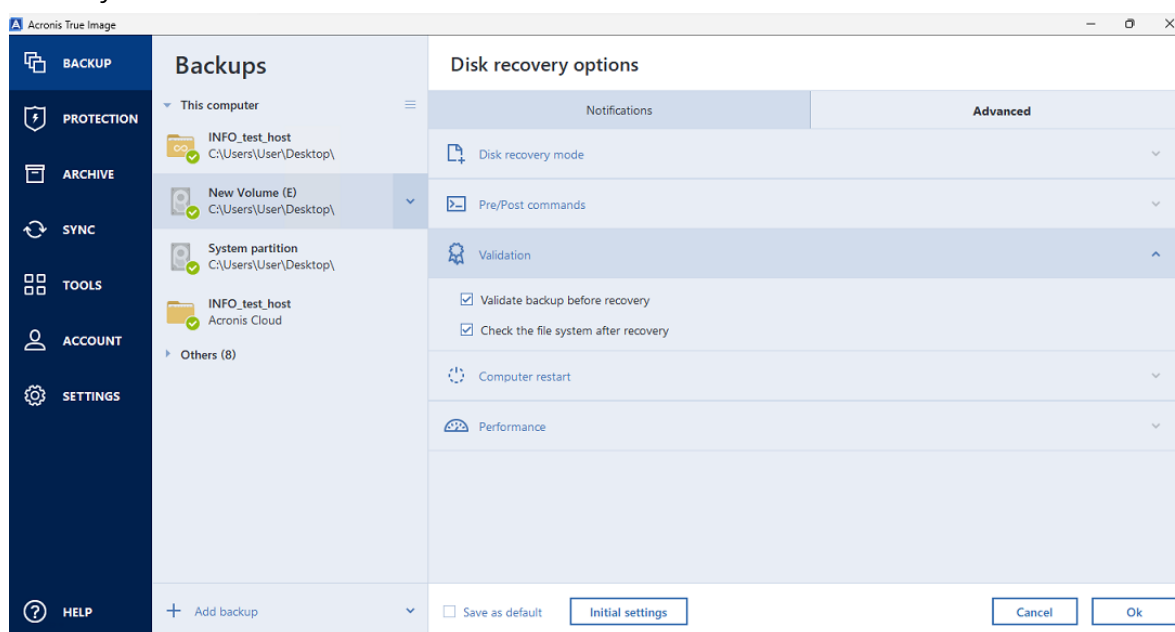
The **Abort the operation if the user command fails** (enabled by default) parameter will abort the operation if any errors occur in command execution.

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

Validation option

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

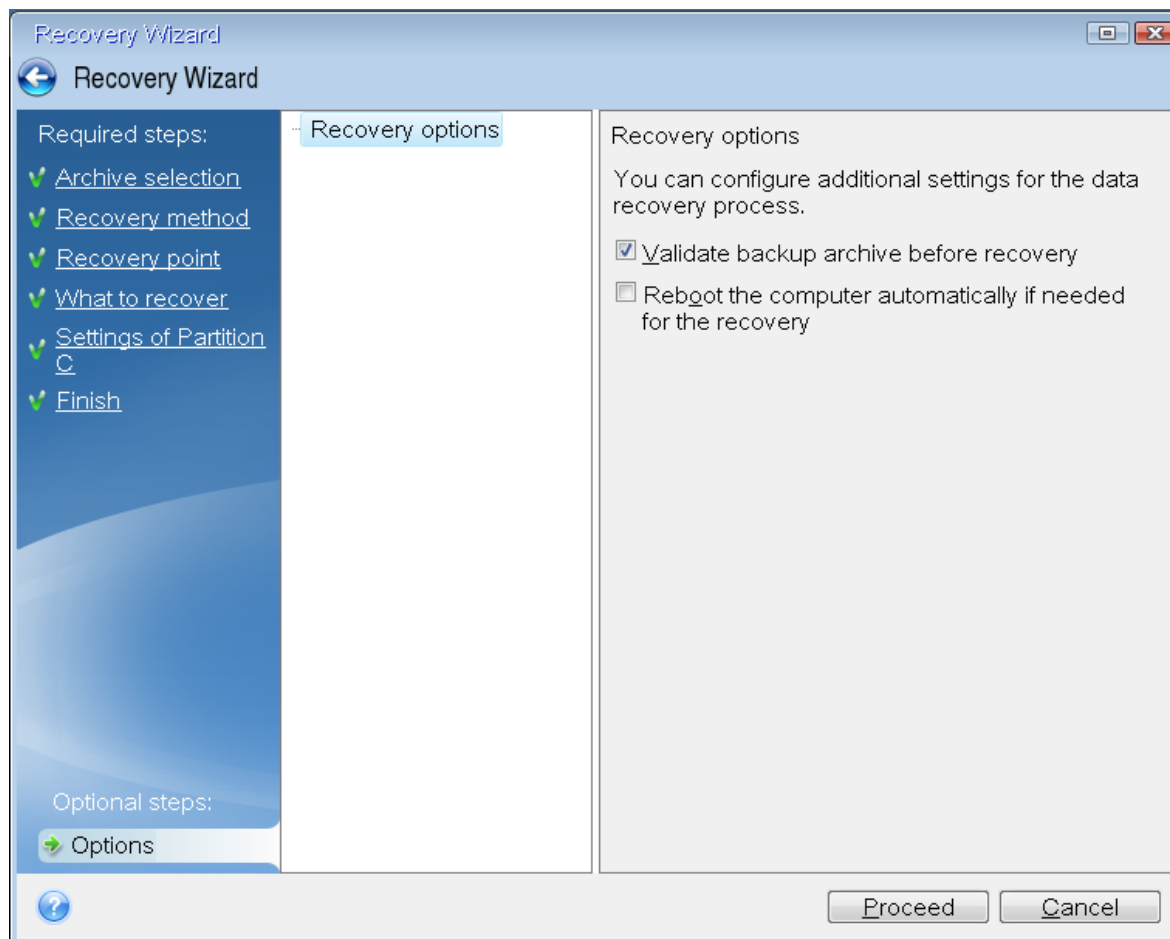
- **Validate backup before recovery** – Enable this option to check the backup integrity before recovery.



- **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 (see [File-level security settings for backup](#)), you can choose whether to recover them or let the files inherit the security settings of the folder where they will be recovered to. This option is effective only when recovering files from file/folder backups.
- **Set current date and time for recovered files** - you can choose whether to recover the file date and time from the backup or assign the files the current date and time. By default the file date and time from the backup will be assigned.

Overwrite file options

Location: **Recovery options > Advanced > Overwrite file options**

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

Note

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

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

If you do not need to overwrite some files:

- Select the **Hidden files and folders** check box to turn off overwriting of all hidden files and folders. This option is available for file-level backups to local destinations and network shares.
- Select the **System files and folders** check box to turn off overwriting of all system files and folders. This option is available for file-level backups to local destinations and network shares.
- Select the **More recent files and folders** check box to turn off overwriting of new files and folders.
- Click **Add specific files and folders** to manage the list of custom files and folders that you do not want to overwrite. This option is available for file-level backups to local destinations and network shares.
 - To turn off overwriting of specific files, click the plus sign to create an exclusion criterion.
 - While specifying the criteria, you can use the common Windows wildcard characters. For example, to preserve all files with extension **.exe**, you can add ***.exe**. Adding **My???.exe** will preserve all .exe files with names consisting of five symbols and starting with "my".

To delete a criterion, select it in the list, and then click the minus sign.

Performance of recovery operation

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

You can configure the following settings:

Operation priority

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

You can set up the operation priority:

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

Notifications for recovery operation

Location: **Recovery options > Notifications**

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

Note

For cloud backups, email notification settings can also be managed in the Online Dashboard: open the profile menu and go to **Email Notification Settings** to select notification types and the email address.

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.

Online Dashboard and Acronis Cloud

What is Online Dashboard?

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

- Control the current statuses of all backups on all devices running Windows, macOS, iOS, and Android.
- Add a new device to the list.
- Manually start any backup on any computer.
- Create new backups of any type (entire machine, file-level, disk-level) on PCs and Macs.
- Change settings of existing backups.
- Recover data from any backup located in Acronis Cloud, including backups from PCs, Macs, and devices running iOS and Android.
- Resolve some product-related issues.
 - Enable two-factor authentication (2FA).
For more information, see "Two-factor authentication (2FA)" (p. 33).
 - Monitor the safety of your personal information in the Identity protection dashboard.
For more information, see "Identity protection" (p. 171).

Adding a new device to Online Dashboard

To use all of the advantages of Online Dashboard, including remote management of your backups, you first need to add your devices to the device list.

To add a new device

1. Install Acronis True Image on your device.
 - You can download the installation files for Windows and macOS at the Acronis website.
 - To install Acronis True Image on iOS and Android devices, follow the instructions in Installing Acronis True Image for mobile devices.
2. Start Acronis True Image and sign in to your account.

Alternatively, you can add a device via the Online Dashboard interface.

To add a new device via Online Dashboard

1. On the device that you want to add, open Online Dashboard at: <https://cloud.acronis.com>.
2. Sign in with your account.
3. On the **Resources** tab, click **Add**.

4. Download and install Acronis True Image.
5. Start Acronis True Image and sign in to the same Acronis account.

Backing up data remotely

With the web-based Online Dashboard, you can configure and run a backup on any computer (PC or Mac) that shares the same account.

Before backing up, ensure that you have access to a computer

1. Open Online Dashboard at: <https://cloud.acronis.com>.
2. Sign in with your account.
3. On the **Resources** tab, find the computer that you want to back up.
 - If you cannot find the computer, you first need to add it to the list. To do this, install Acronis True Image on that computer, start the application, and then sign in with your account. See [Adding a new device](#) for details.
 - If the computer is offline, make sure that it is turned on and connected to the internet.

To create the first backup on a computer

1. Open Online Dashboard, and then find the computer that contains the data that you want to back up.
2. Click **Enable backup**, and then configure settings for the new backup, including:
 - Backup type (entire machine, disk-level, or file-level)
 - Data to back up
 - Backup destination
 - Schedule
 - Retention rules
 - Data encryption
3. When the backup is configured, click **Apply**, and then click **Run now**.

To create a new version of an existing backup

1. Open Online Dashboard, and then find the computer that contains the data that you want to back up.
2. Click **Back up now**, and then select the backup that you want to update.

To change settings of an existing backup

1. Open Online Dashboard, and then find the computer that is the source of the backup.
2. Click the gear icon, click **Backup**, and then find the backup that you want to reconfigure.
3. Click the gear icon next to the backup name, and then click one of the following:
 - To change the main settings, click **Edit**.
 - To change additional options, click **Backup options**.
4. Click **Save changes**.

To create a new backup

1. Open Online Dashboard, and then find the computer that contains the data that you want to back up.
2. Click the gear icon, and then click **Backup**.
3. Click **Add backup plan**.
 - To create a backup with the predefined settings, click **Apply**. The entire machine will be backed up to Acronis Cloud.
 - To create a backup with custom settings, click **Create new**, change the settings, and then click **Apply**.
4. To start backup, click **Run now**.

Recovering data with Online Dashboard

The web-based Online Dashboard allows you to recover data from any online backup¹ uploaded from your devices, including PCs, Macs, smartphones, and tablets.

To recover data from an online backup

1. Open Online Dashboard at: <https://cloud.acronis.com>.
2. Sign in with your account.
3. On the **Resources** tab, find the device that is the source of the data that you want to recover. If the device is offline, make sure that it is turned on and connected to the internet.
4. If you recover data from:
 - A computer – Click **Recover** to browse and recover your data.
 - A mobile device – Click **Recover**. On the left panel, select the backup version by the backup date and time. Then, on the right panel, select the items that you want to recover, and then click **Download**.

Email notifications

Sometimes a backup operation can last a long time. To track the status of your backups and when they are finished, you can configure email notifications via the Online Dashboard.

To configure email notifications

1. Open Email notifications on the Online Dashboard. You can do it in two ways:
 - On the Online Dashboard, click the account icon in the top-right corner, and then select **Email notifications**.
 - In your Acronis True Image application, click **Settings**, and then click **Change email notification settings**.
2. In **Send notifications about**, choose the information you are interested in:
 - Errors
 - Warnings

¹A backup whose destination is Acronis Cloud. Online backups are stored remotely and accessible over the Internet.

- Successful backups
3. In the **Recipients' email addresses** field, type the destination address. You can enter several addresses, separated by semicolons.
 4. [Optional step] In **Subject**, change the email notification subject.
You can use the following variables:
 - [computer_name] – name of computer
 - [operation_status] – status with which operation was completed
 - [backup_name] – name of backupThe default subject is [computer_name] - [operation_status] - [backup_name].

After saving the settings, you will receive information from Acronis servers about all backups on all of your devices running Windows and macOS.

Replicating backups to Acronis Cloud

Why replicate?

A replica is a copy of your local backup of disk, partition or entire machine, that is sent to Acronis Cloud. It can be used as a safeguard and accessed from anywhere. Even though backing up your data provides protection, we recommend that you also replicate all local backups to Acronis Cloud, to protect from incidental corruption of your computer. Of course, you can create two backups, one to back up to your local computer and another one to Acronis Cloud. But creating a replica is faster than creating another backup with a cloud destination.

Replication activation

Replication is not activated by default. You can activate it for any local backup of a disk, partition, or entire machine, that uses the local destination (to an external or internal disk) that you configured in Acronis True Image (2020 or later).

To activate the replication of a backup to Acronis Cloud:

1. From the backup list, select the backup that you want to replicate, and then open the **Replica** tab.
2. Click **Replicate**. Now, replication is activated and will start once the normal backup is created. You are free to close Acronis True Image. Both the backup and replication processes will continue in background mode.
3. [optional step] Click **Options > Advanced > Replication to Acronis Cloud** to see the data center where your backup replication is stored and to [configure the cleanup settings](#) for Acronis Cloud to optimize usage of its space.

Protection of replicated data

Replicated data is uploaded to Acronis Cloud by using Secure Socket Layer (SSL).

In the Cloud, data is stored according to your encryption settings. If no encryption password is set, the replicated data is stored unencrypted. Otherwise, data is encrypted by using AES-256.

Cleaning up space on Acronis Cloud

1. To go to Acronis Cloud, click **Account** on the Acronis True Image sidebar, and then click **Browse my data**. The Acronis Cloud webpage will open in a browser.
2. On the Acronis Cloud webpage, on the left sidebar, click **Account**.
3. On the Acronis Cloud line, click **Clean up**.
4. Choose which versions you want to delete:
 - Versions older than some period.
 - All old versions except for several recent ones.

Warning!

Be careful! Deleted versions cannot be restored.

One more way to clean up is to delete a cloud backup that you no longer need. In this case, all version history for the backup is deleted from Acronis Cloud.

See also

"Cleaning up backups, backup versions, and replicas" (p. 111)

"Deleting backups and replicas" (p. 110)

Removing data from Acronis Cloud

Because the available space on Acronis Cloud is limited, you need to manage your cloud space by cleaning up the obsolete data or the data you do not need anymore. Cleanup can be done in Acronis True Image and also via the Acronis Cloud web application.

Deleting an entire backup

The most drastic option is deleting the entire backup from Acronis Cloud. When a backup is deleted, all of its data is permanently erased. Deleted data cannot be recovered.

In **Acronis True Image**:

Click the down arrow icon next to the backup to delete, and then click **Delete**. The backup and all its versions, settings, and schedule will be deleted.

In the **Acronis Cloud web application**:

1. Go to <https://www.acronis.com/my/online-backup/webrestore/>, and then log in to your Acronis account.
2. On the **Backups** tab, move over the backup that you want to delete.

3. Click the size of the backup, and then the detailed view will appear.
4. Click **Delete** in the detailed view.

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

Deleting the versions of a backup to cloud

In **Acronis True Image**:

1. Click the down arrow icon next to the backup which versions you want to delete, and then click **Clean up versions**.

The list of backup versions opens.

2. Select the versions that you want to delete and click **Delete**.

Note

The quota in Acronis Cloud could take up to one day to update.

In the **Acronis Cloud web application**:

1. Go to <https://www.acronis.com/my/online-backup/webrestore/>, and then log in to your Acronis account.
2. On the **Backups** tab, click on the size of the backup which versions you want to delete.
The details view of the backup opens.
3. In the details view, click **Clean up**.
You can select to delete versions older than a period selected by you, or clean up all versions except a number of recent ones.
4. Configure what to delete and click **Clean up now**.
5. In the confirmation dialog, click **Delete**.

The status of the cleanup procedure is displayed when the operation is completed.

Deleting the versions of a backup replica to cloud

In **Acronis True Image**:

1. In the **Backup** section, locate a local backup that is replicated to cloud, click the down arrow and select **Clean up versions**.
The Clean up backup versions dialog opens.
2. Under **Delete versions from**, select **Acronis Cloud**.
The list of backup replica versions appears.
3. Select the replica versions that you want to delete and click **Delete**.
4. In the confirmation dialog, click **Delete**.

Note

The quota in Acronis Cloud could take up to one day to update.

In the **Acronis Cloud web application**:

1. Go to <https://www.acronis.com/my/online-backup/webrestore/>, and then log in to your Acronis account.
2. On the **Backups** tab, click on the size of the backup replica which versions you want to delete. The details view of the backup replica opens.
3. In the details view, click **Clean up**.
You can select to delete versions older than a period selected by you, or clean up all versions except a number of recent ones.
4. Configure what to delete and click **Clean up now**.
5. In the confirmation dialog, click **Delete**.

The status of the cleanup procedure is displayed when the operation is completed.

One-time cleanup

When your Acronis Cloud is full or is running out of space, we recommend that you use the cleanup tool in the Acronis Cloud web application. This tool allows you to free up a considerable amount of space in the cloud, fast and easy.

Note

You can clean up the backups one by one separately, even the encrypted ones. The password will be requested.

1. Go to <https://www.acronis.com/my/online-backup/webrestore/>, and then log in to your Acronis account.
2. On the **Backups** tab, move over the backup that you want to delete.
3. Click **Clean up** button.
4. In the opened window, configure the cleanup settings, and then click **Clean up now**.

To perform a one-time clean-up for all non-encrypted backups, use the following option:

1. Go to **Account** tab.
2. Click **Clean up** button.

Protection

Acronis True Image provides the following protection for your data:

- Active Protection runs constantly in the background to protect your machines in real time while you work as usual.
- Antivirus scans run on-demand to perform in-depth search for malicious software throughout the whole system.
- Vulnerability assessment is a daily scan that runs in the background, detects vulnerabilities in your system and apps, and then assesses their severity.

Note

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

If you have a license covering Active Protection, but the corresponding component was not installed, you can add it. For more information, see "Configuring Active Protection" (p. 169).

If you have a license covering Real-time Protection, Antivirus scan, Videoconference protection, and Web filtering, but the corresponding component was not installed, you can add it. For more information, see "Configuring Active Protection" (p. 169).

The Protection dashboard

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

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

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

- Install missing protection components. To do this, click **Install** and follow the instructions displayed.
- View statistics about the active protection status.
- View the number of detected issues, quarantined items, and protection exclusions.
- View the latest report of the **Antivirus scan**. To view this, click **Scan report**.
- View the next scheduled scan time.
- Manually run full or quick **Antivirus scan**. To do this, click **Run full scan** or **Run quick scan**.
- View the latest report of the detected vulnerabilities, and run a new scan from it. To view this, click **Detected vulnerabilities**.
- 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. Scheduled on-demand scans will not start.

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 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 application files, your backups, and the Master Boot Records of your hard drives.

Active protection consists of several protection levels that you can enable independently from each other:

- Anti-ransomware protection
- Real-time protection
- Web filtering

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 will search the following locations for the latest file versions to recover.

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

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

Note

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

To configure Acronis True Image 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](#).

Real-time Protection

When **Real-time Protection** is enabled, it constantly checks the files you interact with to protect your machine from suspicious activity, viruses, and other malicious threats in real time.

Real-time Protection comes with the following additional protection options:

- Behavior analysis – to identify malicious processes, Active Protection uses behavioral heuristics. It compares the chain of actions performed by a process with the chains of events recorded in the database of malicious behavior patterns. This approach enables Active Protection to detect new malware by its typical behavior.
- Exploit prevention – Active Protection analyzes the behavior of processes running on the machine and detects abnormal activity. It prevents infected processes from spreading and exploiting the vulnerabilities of other software installed on the system. Active Protection employs several exploit prevention methods:
 - Memory protection detects and prevents suspicious modifications of the execution rights on memory pages. Malicious processes apply such modifications to page properties, to enable the execution of shellcodes from non-executable memory areas like stack and heaps.
 - Privilege escalation protection detects and prevents attempts for elevation of privileges made by an unauthorized code or application. Privilege escalation is used by malicious code to gain full access of the attacked machine, and then perform critical and sensitive tasks. Unauthorized code is not allowed to access critical system resources or modify system settings.
 - Code injection protection detects and prevents malicious code injection into remote processes. Code injection is used to hide malicious intent of an application behind clean or benign processes, to evade detection by anti-malware products.

You can choose one of the following types of scanning:

- **Smart on-access** detection means that the program runs in the background and actively and constantly scans your machine system for viruses and other malicious threats for the entire duration that your system is powered on. Malware will be detected in both cases when a file is being executed and during various operations with the file such as opening it for reading/editing.

- **On execution** detection means that only executable files will be scanned at the moment they are run to ensure they are clean and will not cause any damage to your machine or data. Copying of an infected file will remain unnoticed.

You can view the results of real-time protection checks in the **Activity** tab of the Protection dashboard.

Web filtering

Malware is often distributed by malicious or infected sites and uses the so called "Drive-by download" method of infection.

Web filtering helps to protect you from potentially harmful websites and untrusted web resources by blocking the access when you try to open them. To determine which websites are potentially harmful, Web filtering uses the Protection updates database. The Web filtering database also includes information about websites that contain scam and phishing URLs. You can modify the rules defined in the database by configuring exceptions to the Web filtering list.

Web filtering has two modes of operation:

- **Complete block** – the access to the website will be completely blocked.
- **Notify only** – a notification will be displayed, but users will be able to access the website.

Configuring Active Protection

To access Active Protection settings

1. Click **Protection** on the sidebar, then click **Settings**, and go to the **Active Protection** tab.
2. [optional step] If Active Protection is not installed, click **Install** under **Get Active Protection and Antivirus scan**, and then follow the instructions displayed.

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 recovers the files as follows.
Acronis True Image searches the following locations for the latest file versions to recover.
 - Temporary file copies that were preliminarily created during the process verification
 - Local backups
 - Cloud backups
 If Acronis True Image finds a good temporary copy, the file is restored from that copy. If temporary file copies are not suitable for restore, Acronis True Image searches for backup

copies locally and in the cloud, compares the creation dates of the copies found in both locations, and restores your file from the latest available unmodified copy.

Note

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

- **Protect backup files from ransomware** – Acronis True Image will protect its own processes and your backups from ransomware. Your archives are also protected.
- **Protect network shares and NAS** – Acronis True Image 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**.

To configure Real-time Protection

1. [optional step] If Real-time Protection is not installed, click **Install** under **Get full protection**, and then follow the instructions displayed.
2. Switch on the **Real-time Protection** toggle to enable Real-time Protection.
When enabled, Real-time Protection checks for malware all the files you interact with.
3. Select when the files should be checked.
 - **Smart on-access** – all system activities are monitored, and the files are scanned once you access them.
 - **On execution** – only executable files are scanned as they are launched to make sure that they will not damage your machine.
4. Select from the drop-down list what to do with detected objects.
 - **Block and notify** – The process suspected of malware activity will be blocked, and you will get a notification.
 - **Quarantine** – The process suspected of malware activity will be blocked, and the executable file will be moved to the quarantine folder.
5. Enable the additional protection options.
 - **Detect malicious behavior in processes** – enables Active Protection to detect new malware by its typical behavior and block it.
 - **Detect and prevent malicious processes from exploiting the software vulnerabilities on a system (experimental)** – enables Active protection to detect and block processes that try to exploit bugs and vulnerabilities of other processes on the system.

Note

All detected objects are blocked immediately. They will not be moved to quarantine, nor added to the detected issues list.

To configure Web filtering

1. [optional step] If Web filtering is not installed, click **Install** under **Get full protection**, and then follow the instructions displayed.
2. Switch on the **Web filtering** toggle to protect you from potentially harmful websites and untrusted web resources.
3. From the **Action on malicious URL detection** drop-down menu, select what to do with detected malicious URLs.
 - **Complete block** – The access to the website will be completely blocked.
 - **Block and notify** – The website will be blocked with the ability to proceed.
4. To configure the list of trusted or blocked websites, click **Manage exceptions**.
 - a. To add a new URL to the list, click **Add URL**.
 - b. Enter a valid URL name. Its domain will be added to exceptions.

Note

All addresses from the domain that you entered will be treated as trusted or blocked. For example, if you entered xyz.com as a trusted domain, all paths or sub-domains under xyz.com are treated as trusted.

- c. From the drop-down menu, select **Allowed** or **Blocked**. The allowed websites will not be scanned for threats. The blocked websites will not open, or you will get notified at such an attempt.
- d. Click **Add URL**.
- e. Click **Apply**.

Identity protection

Important

Identity protection is currently available only for the Advanced and Premium licenses. For a list of countries where this feature is supported, see the [Support Portal article](#).

Identity protection is a set of measures to prevent cybercriminals from stealing your personal information. The following information is monitored:

- Essentials like the national ID number, passports, driver's license, addresses, phone numbers, email addresses, and credentials
- Financial information about cards and bank accounts
- Insurance documents, like health and vehicle insurance

This information can be leaked as a result of a data breach, phishing, or a malware attack. Identity protection helps you detect the data exposure and any suspicious activity related to your information. In a dedicated Identity protection dashboard, you can do the following:

- Add and update your personal information to be monitored
- Monitor the safety of your data
- Configure alerts about data exposure

- Request assistance in case of identity data theft. You can also contact the Support team via support@info.idprotectiononline.com.
- Get reimbursement in case of identity data theft

To configure Identity protection for the first time

1. In the left sidebar of Acronis True Image, click **Protection**.
2. Under **Identity protection**, click **Manage protection**. Online Dashboard opens in the browser.
For more information, see "What is Online Dashboard?" (p. 159)
3. Sign in to Online Dashboard.
4. On the **Identity protection** tab, click **Manage protection**.
5. In the **Enter your identity data** window, enter your personal information.

Important

Ensure that the information is complete and accurate. Otherwise, you might not be notified when your actual identity data is compromised.

Once you have entered the data, we start running regular checks of its safety.

The Identity protection dashboard opens in your browser.

To open Identity protection dashboard from Acronis True Image

1. In the left sidebar of Acronis True Image, click **Protection**.
2. Under **Identity protection**, click **Manage protection**.
Online Dashboard opens in the browser.
3. Sign in to Online Dashboard.
4. On the **Identity protection** tab, click **Manage protection**.
The Identity protection dashboard opens in the browser.

To open Identity protection dashboard from Online Dashboard

1. Open Online Dashboard at <https://cloud.acronis.com>.
For more information, see "What is Online Dashboard?" (p. 159)
2. In the left sidebar of Online Dashboard, click **Protection > Identity protection**.
3. On the **Identity protection** tab, click **Manage protection**.
The Identity protection dashboard opens in your browser.

Antivirus scans

Antivirus scan is one of the components of Acronis True Image Antivirus and Anti-malware Protection. It protects your computer by checking for malware on demand – manually or at predefined intervals that you can configure.

You can select between two types of scans.

- **Full** scan checks the entire machine for viruses. Full scan will detect malware by examining all files and processes (or a subset of files and processes), except for excluded files or folders that you defined in the excludes lists.
- **Quick** scan checks only specific files and folders. Quick scan will detect malware by examining specific folders which are considered the most likely virus storages.

You can also choose what to scan: archive files, external drives, or only new and changed files.

Note

You can configure Acronis True Image to prevent your computer from entering sleep or hibernate mode if a scan operation is running. Keep in mind that this option is selected by default.

By default, when the CPU load is high, the priority of antivirus scans is decreased to let other applications perform properly. This results in slower scans. You can disable this option to speed up the scanning.

To view the **Scan details report** window, containing antivirus scan details, click the **Scan report** button.

Configuring Antivirus scans

To access the **Antivirus** settings, click **Protection** on the side bar, then click **Settings**, and go to the **Antivirus** tab.

To configure Action on detection:

Select the options that you want to enable.

- **Quarantine** – This option is set by default. When Acronis True Image detects a potential malware threat, it stops the process and moves the suspicious file to the quarantine folder.
- **Notify only** – When a suspicious process is detected, you will get a notification about the potential malware threat.

To configure scan type:

Select the type of scan you want to perform:

- **Full** – This option is set by default. Acronis True Image will check the entire PC.
- **Quick** – Acronis True Image will check only the specific folders that are considered the most likely storages of threats.

To schedule antivirus scans:

Select one of the check boxes to configure the time when the scanning process shall start.

- **Daily** – the scan will be run every day at a specified time.
- **Weekly** – the scan will be run on a specified day of week. Set the day of week and time.
- **Monthly** – the scan will be run on a specified day of month.
- **At system startup** – the scan will be run at each start of your operating system.
- **Do not schedule** – the scan run is not planned for a specific time.

To configure what to scan:

Select the following check boxes:

- **Do not scan archive files larger than.** Select a value by using the arrows.
- **Scan external drives**
- **Scan network shares and NAS**
- **Scan only new and changed files**

To configure system behavior during Antivirus scans:

Sometimes, the system might be shut down before the Antivirus scan is completed. For such cases, select the **Run missed tasks at the startup** check box to configure Acronis True Image to resume the scan when the system starts again by selecting.

Moreover, you can enable the **Prevent the sleep or hibernate mode** option to prevent your computer from shutting down if a scan operation is running.

The priority of antivirus scans can be decreased in case of a CPU overload to let other applications perform properly. This option is enabled by default which might slow down the scanning. To speed up the scans, clear the **Give priority to other applications** check box.

After configuring the Antivirus scans, click **OK**.

Vulnerability assessment

Vulnerability assessment is one of the components of Acronis True Image Antivirus and Anti-malware Protection. It is a daily scan that runs in the background, detects vulnerabilities in your system and apps, and then assesses their severity. You can also run the scan manually when needed.

Note

To update the vulnerabilities database, a stable internet connection is required.

To view the vulnerabilities:

1. On the left sidebar, click **PROTECTION**.
2. On the **Overview** tab, under **Vulnerability assessment**, click **Detected vulnerabilities**. The report is displayed.
3. To run a new scan, click **Run scan**.
4. [optional] To display the **Detailed information** window, click the info icon next to the vulnerability name.
5. [optional] To view a detailed description of the vulnerability, click the arrow next to its name. A webpage containing this information will be displayed.
6. To resolve the detected issues, install the latest updates of the affected applications. Then, scan again to ensure that the vulnerabilities are fixed. If they persist, it means that some apps might

still put your system at risk. To protect your data fully, back up the operating system and enable Anti-malware Protection.

To configure the vulnerability assessment:

1. On the left sidebar, click **PROTECTION**, then click **Settings**.
2. Go to the **Vulnerability assessment** tab, and switch the toggle on or off to enable or disable the vulnerability scan.

Patch management

Patch management is an extension of the **Vulnerability assessment** feature in Acronis True Image. It enables you not only to detect vulnerabilities in your system and applications, but also to automatically or manually install software updates (patches) that fix these vulnerabilities.

Patch management is available only in Acronis True Image for Windows. If **Vulnerability assessment** is disabled, **Patch management** will not work.

With Patch management, you can:

- Scan your system for missing patches together with vulnerability scanning (manual or scheduled).
- View a list of patches grouped by affected applications, including details such as patch version, severity, and release date.
- Install patches manually in bulk or one by one.
- Configure automatic patch installation by schedule (daily, weekly, or monthly).

How scan and installation progress is shown

- When patch scanning or installation starts, the app shows progress in the **Protection** tab.
- While scanning, the status message shows **Scanning for vulnerabilities... XX% progress**.
- While installing, the status message shows **Installing patches... XX% progress**.
- Progress continues in the background even if you close the patch list window or navigate away from it.
- No loader modal is used for patch scanning or installation in progress.

Scan and installation notifications

- After a successful scan, a notification confirms that detected vulnerabilities are ready for review.
- When installation starts, a notification indicates that patches are being downloaded and installed.
- After successful installation, a notification confirms that patch installation is complete.
- If installation fails, a notification asks you to try again, and you can retry with **Install patches**.

Important behavior

- If a restart is required and postponed, the applied updates are preserved and installation completes on the next restart.
- If the computer is shut down during scanning or installation, restart the operation after startup.

- Each time you open **View patches**, the patch list is refreshed and shows only patches that are not yet installed.

After a vulnerability scan, open the details for a detected vulnerability, click **View patches**, review available updates, and click **Install patches**. To configure automatic patch installation, go to **Protection settings**.

Note

If the internet connection is unavailable during installation, patch installation may fail. You can retry after connectivity is restored.

Automatic patch installation

To configure automatic patch installation

1. On the left sidebar, select **PROTECTION**, then click **Settings**.
2. Go to the **Vulnerability assessment** tab.
3. Enable **Vulnerability assessment** and **Automatic patch installation**.
4. Under **Scheduled patch installation**, choose one of the following:
 - **Daily**: select the time of day.
 - **Weekly**: select one or more days and the time of day.
By default, patches are installed weekly on Mondays at 18:00.
 - **Monthly**: select one or more days of the month and the time of day.
5. Under **Patches to install for Microsoft products**, choose:
 - **All updates**
 - **Only security and critical updates**
6. Under **Patches to install for Windows third-party products**, choose:
 - **All updates**
 - **Only major updates**
 - **Only minor updates**

What to expect during automatic installation

- Automatic patch installation runs in the background and progress is shown in the **Protection** tab.
- No loader modal is displayed while patch installation is in progress.
- If installation fails, retry patch installation after the issue is resolved.
- If a restart is required and postponed, installation is completed on the next restart.

Manual patch installation

To install patches manually

1. On the left sidebar, select **PROTECTION**.
2. On the **Overview** tab, under **Vulnerability assessment**, click **Detected vulnerabilities**.
3. Click **View patches**.

4. Select one or more patches to install.
5. [Optional] Click **Agreement** next to each selected patch to read the license agreement.
6. [Optional] Select whether to restart the computer: **Don't restart**, **Restart if required**, or **Always restart**.
7. Click **Install patches**.
8. [Optional] You can close the **Install patches** window. Installation continues in the background. To check the status, open the **Detected vulnerabilities** list again.
9. No loader modal is displayed while installation is in progress. Progress is shown in the **Protection** tab.
10. You will get a notification when installation starts, and another one when installation finishes or fails.
11. If the warning message about restart appears, save your work, close applications, and restart the computer to complete the installation.

Viewing patch installation results

To view patch installation results

1. On the left sidebar, select **PROTECTION**, then select the **Activity** tab.
2. Review the list of patches. The list shows the application names, patch versions, and installation time.

Troubleshooting patch installation

To troubleshoot installation issues

- If the error message says that the installation failed due to no internet connection, reconnect to the internet and run the installation again.
- If the installation was interrupted by a system restart or product update, run the installation again after the restart is complete.
- If the issue persists, reinstall the affected application manually.

Managing detected issues

The list of detected issues is populated when the Antivirus scans are configured to **Block and notify** action on detection. You should review the list and decide whether to trust or move to quarantine.

To check and manage the detected issues:

1. There are two ways to access the detected issues:
 - On the **Protection** dashboard, click **Detected issues**.
 - On the **Protection** dashboard, click **Settings**, and go to the **Advanced** tab:
 - a. [optional step] If the Real-time Protection, Antivirus scan, Videoconference protection, and Web filtering component is missing, click **Install** and follow the instructions displayed.
 - b. Under **Detected issues**, click **Manage**.

2. Select a check box of an issue in the list and select how to process it.
 - To add the file or process to the list of Protection excludes, click **Trust**.

Note

If you select to trust a file or process, it will be excluded from future Antivirus scans.

- To move a file or process to quarantine, click **Quarantine**.
3. Click **Close**.

Managing files in Quarantine

Based on your settings, Active protection and Antivirus scans 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 will skip them during scanning.

Note

If the Real-time Protection, Antivirus scan, and Web filtering component is not installed, you can only add executable files to Protection exclusions, not folders.

After you install this component, the existing Active protection exclusions will also apply to the Antivirus scan.

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.
 - **Add folder** — [optional, if the Real-time Protection, Antivirus scan, and Web filtering component is installed] to exclude folders 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.

To configure protection exclusions for Web filtering, see [Configuring Active Protection](#).

Videoconference app protection

Zoom, Cisco Webex Meetings, and Microsoft Teams are widely used for web conferencing and communication. Anti-ransomware by Acronis True Image protects these collaboration applications by default as follows.

- Protecting application processes from code injections
- Preventing suspicious operations by application processes

Note

When a supported application is detected or a session starts, a notification appears in **Tray Center**. In the **Protection** tab, **Active Protection** lists currently monitored applications. For settings, see [Configuring Active Protection](#).

Note

After you uninstall an application, the corresponding entry is removed from the **Protection** tab. For Microsoft Teams, the entry may remain until
`%USERPROFILE%\AppData\Local\Microsoft\Teams\current\Teams.exe` is removed.

Downloading Protection updates

By default, Acronis True Image downloads Protection updates automatically. You can check the status of the Protection databases and components or disable the automatic downloads of Protection updates.

To check the status of Protection updates:

1. On the **Protection** dashboard, click **Settings**, then click the **Advanced** tab.
2. Locate the **Protection updates** section in the bottom.

The latest database version and download date are displayed in the bottom of the section.

To disable automatic downloading of Protection updates:

Note

To ensure maximum protection, we do not recommend disabling the automatic protection updates.

1. On the **Protection** dashboard, click **Settings**, then click the **Advanced** tab.
2. Locate the **Protection updates** section in the bottom.
3. Clear the **Download Protection updates automatically** check box.

To download the latest Protection updates:

If the automatic downloading of Protection updates is disabled, you can check for updates and download them manually.

1. On the **Protection** dashboard, click **Settings**, then click the **Advanced** tab.
2. Locate the **Protection updates** section in the bottom.
3. Click **Check for updates**. This option is available only when the **Download Protection updates automatically** check box is not selected.
4. If the Protection updates are not latest, click **Update**.

Archiving data

What is data archiving?

Data archiving is a tool that allows you to move your big or rarely used files to Acronis Cloud, NAS, an external hard drive, or a USB flash drive. Every time you run this tool, it analyzes the data in the selected folder and suggests uploading the found files to Acronis Cloud or moving them to local storage. You can select the files and folders that you want to archive. After moving to an archive, the local copies of these files will be deleted. The links to the files are stored in a special location called Acronis Drive. You can access the location as an ordinary folder in File Explorer. Double-clicking a file link will open the file as if it was stored in the local folder. If the file is archived to Acronis Cloud, it will be downloaded back to your computer, first. You can also access and manage it right in Acronis Cloud.

Data archiving has the following main features:

- **Free storage space saving**

As a rule, storage space of modern high-capacity hard drives is mostly occupied by user data, such as photographs and documents, and not by the operating system or applications. Since most of the data is used occasionally, there is no need to keep them on a local drive. Data archiving helps you free up storage space for frequently used files.

- **Cloud archiving and local archiving**

You can choose a destination type for your archive: Acronis Cloud or local storage, such as an internal hard drive, external hard drive, NAS, or a USB flash drive. Every time you choose Acronis Cloud as a destination, the selected data is stored in the same cloud archive. Local archives are independent from each other and may have different names, destinations, encryption settings, and so on, though you can select an existing archive as a destination instead of creating a new one. The number of local archives is not limited.

- **Easy access of cloud archive from any device**

When you archive your files to Acronis Cloud, you can access them with Acronis True Image, Acronis Mobile, or Acronis Cloud from any device running Windows, macOS, iOS, and Android, including tablets and smartphones.

- **Data protection in the cloud archive**

Your data stored in Acronis Cloud is protected from corruption or disaster. For example, in case of your local hard drive failure, you can download your files to your new hard drive. Moreover, your data is stored in encrypted state. You can be sure that no one except you can access your data.

- **File sharing**

When your files are uploaded to Acronis Cloud, you can create public links to share the files with your friends or to post them to forums and social networks.

- **File versions**

For the files that have been changed and uploaded to Acronis Cloud several times, Acronis True Image keeps all the modifications in different file versions. You can choose a previous file version and download it to your device.

What is excluded from archives?

To reduce archive size and eliminate a possibility to corrupt your system, by default Acronis True Image excludes the following data from archives:

- pagefile.sys
- swapfile.sys
- The Temp folder
- The System Volume Information folder
- The Recycle Bin
- Web browser temporary data:
 - Temporary internet files
 - Cache
- .tibx files
- .tib.metadata files
- .tmp files
- .~ files

See the full file list in the [Support Portal article](#).

Cloud archiving vs. Online backup

When you archive your data to Acronis Cloud, it is similar to an online backup¹, but there are a number of differences.

	Online backup	Cloud archiving
Feature purpose	Data protection from operating system corruption, hardware failures, and loss of separate files.	Cleanup of local storage device and moving data to Acronis Cloud.
Data protection	• Overall protection of all data on a computer, especially an operating system. • Protection of frequently used files.	Protection of rarely used and old files, mostly your personal documents, photographs, and so on.
Source data selection	Manual selection.	Manual selection of automatically found files.

¹A backup whose destination is Acronis Cloud. Online backups are stored remotely and accessible over the Internet.

	Online backup	Cloud archiving
Source data handling	The source data is kept in the original location.	The source data is deleted from the original location. This gives you a guarantee that your data will not get into the wrong hands if your hard drive or laptop is stolen.
Data change frequency	The data to back up is changed frequently. Usually a backup has many versions updated from time to time.	The data to archive is changed rarely. The files have few versions.

Archiving your data

Data archiving helps you free up your storage space by moving your old or rarely used files to Acronis Cloud or local storage. See [What is data archiving](#) for details.

To archive your data

1. Start Acronis True Image, and then go to the **Archive** section.
2. [Optional step] To learn basics of the data archiving feature, view the Getting Started slides.
3. Do one of the following:
 - To analyze files in your default Windows user folder, usually located at C:\Users\[username], click **Analyze Home folder**.
 - To analyze files in a custom folder, click the down-arrow, click **Select different folder**, and then select the folder to analyze.

Acronis True Image analyzes files on your computer. Note that this process may take several minutes.
4. In the left area, select a data category. Then, in the right area, select the files and folders that you want to archive.

When selecting found files, you can sort them, for example, by size or by age (last modified date). To sort the files, click the appropriate column header.
5. Click **Select destination**, and then select Acronis Cloud or a custom local destination for the archived files.
6. [optional step] Click **Options** to set the options for the archive, including **Data center** and **Encryption**. See [Data archiving options](#) for details.
7. Click **Archive**.
8. Confirm that you want to move your files to the archive and automatically delete them from your computer.

Additionally, watch the English-language video instructions at <https://goo.gl/eEkNj2>.

Data archiving options

Data center

When you archive your files to Acronis Cloud, they are uploaded to one of the Acronis data centers located in different countries. Initially, the data center is defined as the one closest to your location when you create your Acronis account. Afterwards, your archived files are stored in the same data center, by default.

We recommend that you set the data center for an archive manually, when you are in a different country and your default data center is not the closest to your current location. This will significantly increase the data upload rate.

Note

You cannot change the data center after starting the archiving process.

To select a data center

1. When configuring the first archiving process, click **Options**.
2. Select the country that is closest to your current location.

Encryption

To protect the archived data from unauthorized access, you can encrypt the archive with industry-standard AES (Advanced Encryption Standard) cryptographic algorithm with a 256-bit long key.

Note

You cannot set or change the archive encryption option for a pre-existing archive.

To encrypt an archive:

1. When configuring the first archiving process, click **Options**.
2. Select the **Encrypt archive by using the AES-256 algorithm** check box.
3. Enter the password for the archive into the corresponding field. We recommend that you use a password longer than seven symbols and containing both letters (in upper and lower cases preferably) and numbers to make it more difficult to guess.

Note

A password cannot be retrieved. Memorize the password that you specify for an archive protection.

Acronis True Image asks for the password every time you try to modify the archive. To access the archive, you must specify the correct password.

Accessing your archived files

When your files are successfully archived, you can access them in:

- **File Explorer**

Start File Explorer, and then click **Acronis Drive** under **Favorites**.

You can work with the files in read-only mode. To modify a file, copy it to a different folder, first.

- **Acronis Cloud** (applicable to the cloud archive only)

Go to Acronis Cloud in one of the following ways:

- Start Acronis True Image, click **Archive**, and then click **View in your web browser**.
- Go to <https://www.acronis.com/my/online-backup/webrestore/>, and then log in to your account.

Sharing data

You can share files and folders stored in backups and archives in Acronis Cloud.

1. On the Acronis True Image sidebar, click **Account**.
2. In the **Acronis Cloud Storage** section, click **Browse my data**.
You are redirected to the Acronis Cloud browser page.
3. Depending on what you want to share, do the following:
 - If you want to share a file or folder from a backup, on the left sidebar, click **BACKUPS**. Select the required file or folder with a check mark.
 - If you want to share a file or folder from an archive, on the left sidebar, click **ARCHIVES**. Select the required file or folder with a check mark.
4. On the right sidebar, click **Share link**.
5. [Optional] You can configure the sharing options. To do that, in the link window, click **Link settings**. You can apply a password, set the expiration date, and limit the amount of downloads.
6. In the link window, click **Copy link** and close it.

You can now share this link. To see the shared files, on the left sidebar, click **SHARING**. You can select any file here, and on the right sidebar copy its link, configure the link settings, or delete it.

Disk cloning and migration

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

- [Use the Clone disk utility.](#)
- [Back up your old disk drive, and then recover it to the new one.](#)

See also: [Difference between Backup and Disk Clone](#)

Disk cloning utility

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

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, NVMe, or HDD drive instead.

- The Clone disk utility does not support multiboot systems.
- On program screens, damaged partitions are marked with a red circle and a white cross inside in the upper left corner. Before you start cloning, you should check such disks for errors and correct the errors by using the appropriate operating system tools.
- We strongly recommend that you create a backup of the entire original disk as a safety precaution. It could be your data saver if something goes wrong with your original hard disk during cloning. For information on how to create such a backup, see [Backing up partitions and disks](#). After creating the backup, make sure that you validate it.

Note

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

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

Clone Disk wizard

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

To clone a disk

1. Start Acronis True Image.
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 does not support cloning of dynamic disks.

Both the source and destination disks must have the same logical sector size. Common logical sector sizes are 512 bytes and 4096 bytes, depending on the drive and controller configuration. Cloning to a disk with a different logical sector size is not supported. For information about verifying these prerequisites, see the [Support Portal article](#).

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

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

Note

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

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

Note

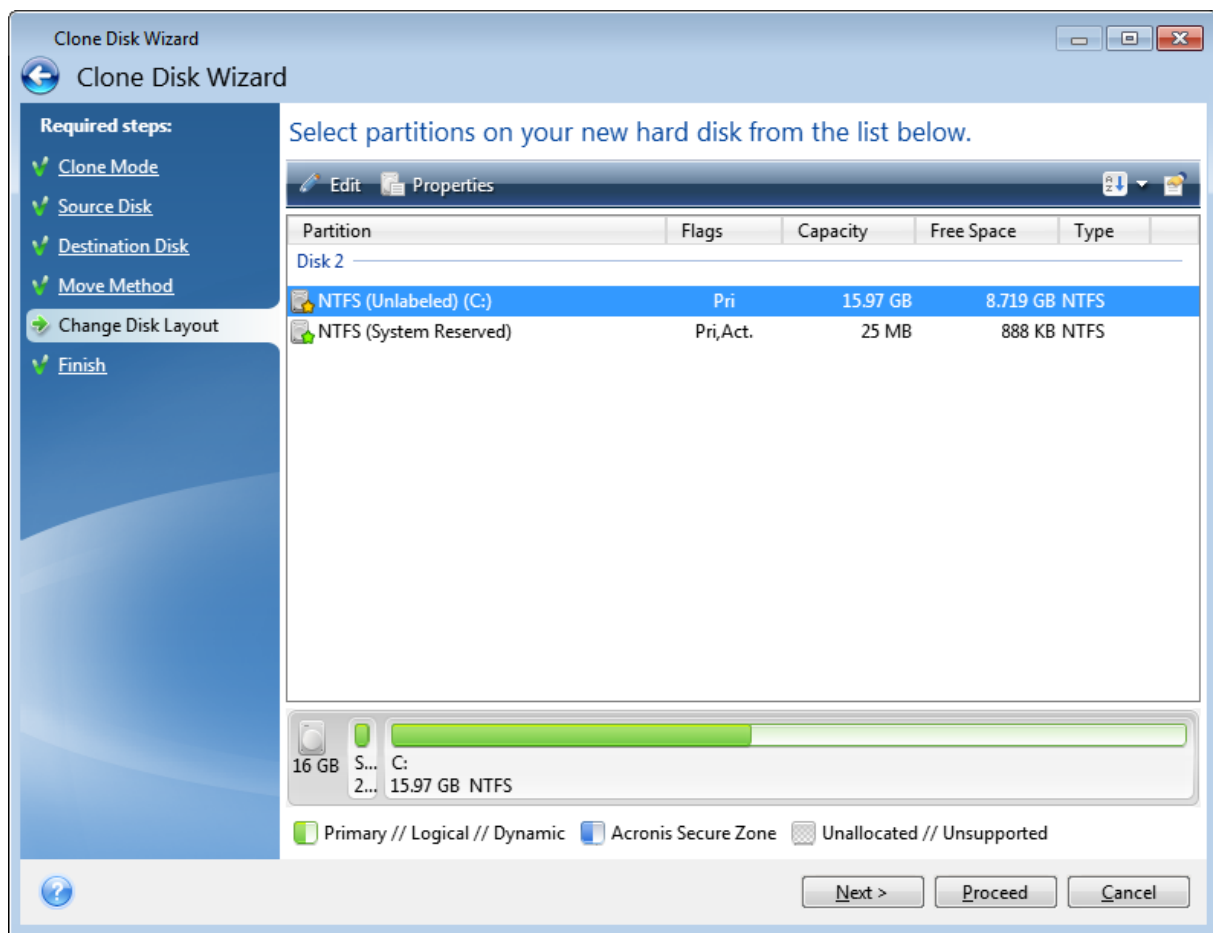
The clone may not be bootable on a computer with different hardware. To make the cloned disk bootable, prepare necessary drivers and use Acronis True Image Universal Restore. For details, see [Acronis True Image Active cloning in Windows](#).

- **To use as a data disk** – the disk data will be copied. Use this clone as a non-bootable data drive.
7. [This step is only available in the manual cloning mode]. On the **Move method** step, choose a data move method.
- **As is** – a new partition will be created for every old one with the same size and type, file system and label. The unused space will become unallocated.
 - **Proportional** – the new disk space will be proportionally distributed between cloned partitions.
 - **Manual** – you will specify a new size and other parameters yourself.
8. [This step is only available in the manual cloning mode]. On the **Change disk layout** step, you can edit settings of the partitions that will be created on the destination disk. See [Manual partitioning](#) for details.
9. [Optional step] On the **What to exclude** step, you can specify files and folders that you do not want to clone. See [Excluding items from cloning](#) for details.
10. On the **Finish** step, ensure that the configured settings suit your needs, and then click **Proceed**.

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

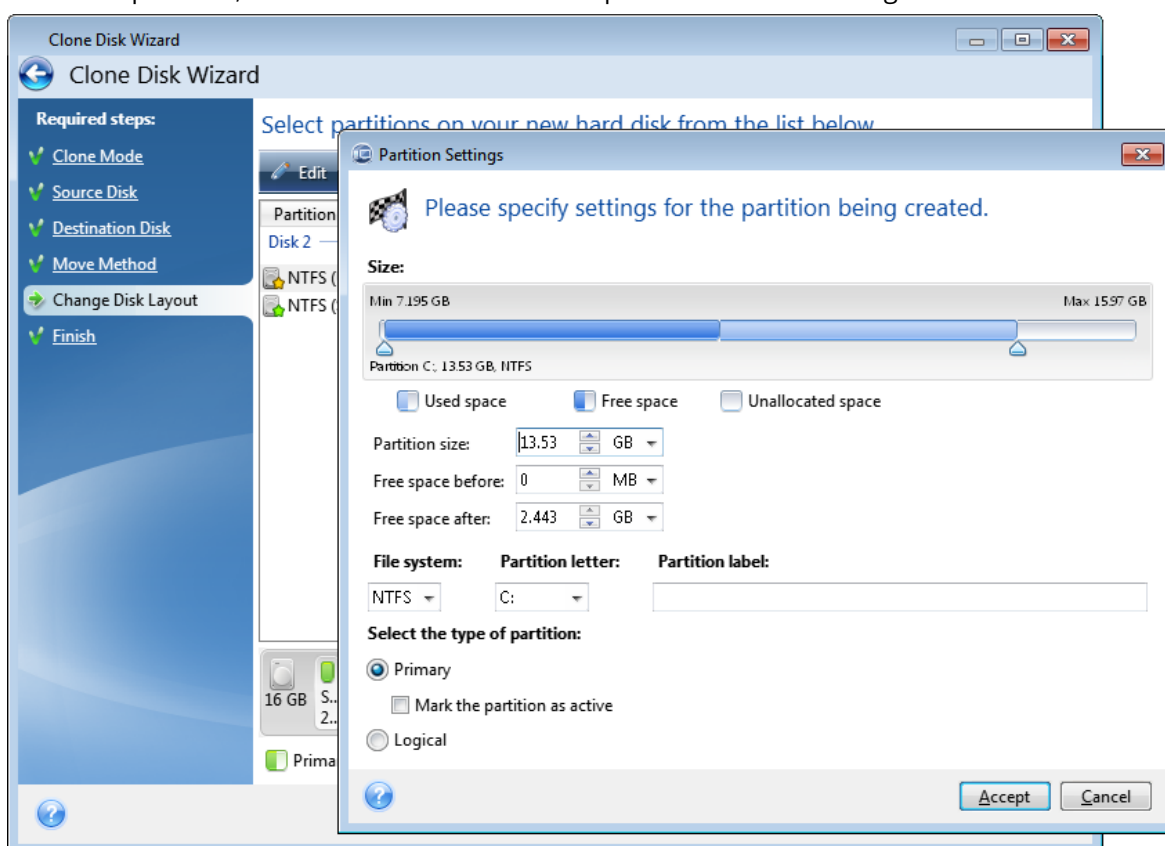
Manual partitioning

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



To edit a partition

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



2. Specify the following settings for the partition:

- Size and position
- File system
- Partition type (available only for MBR disks)
- Partition letter and label

See [Partition settings](#) for details.

3. Click **Accept**.

Warning!

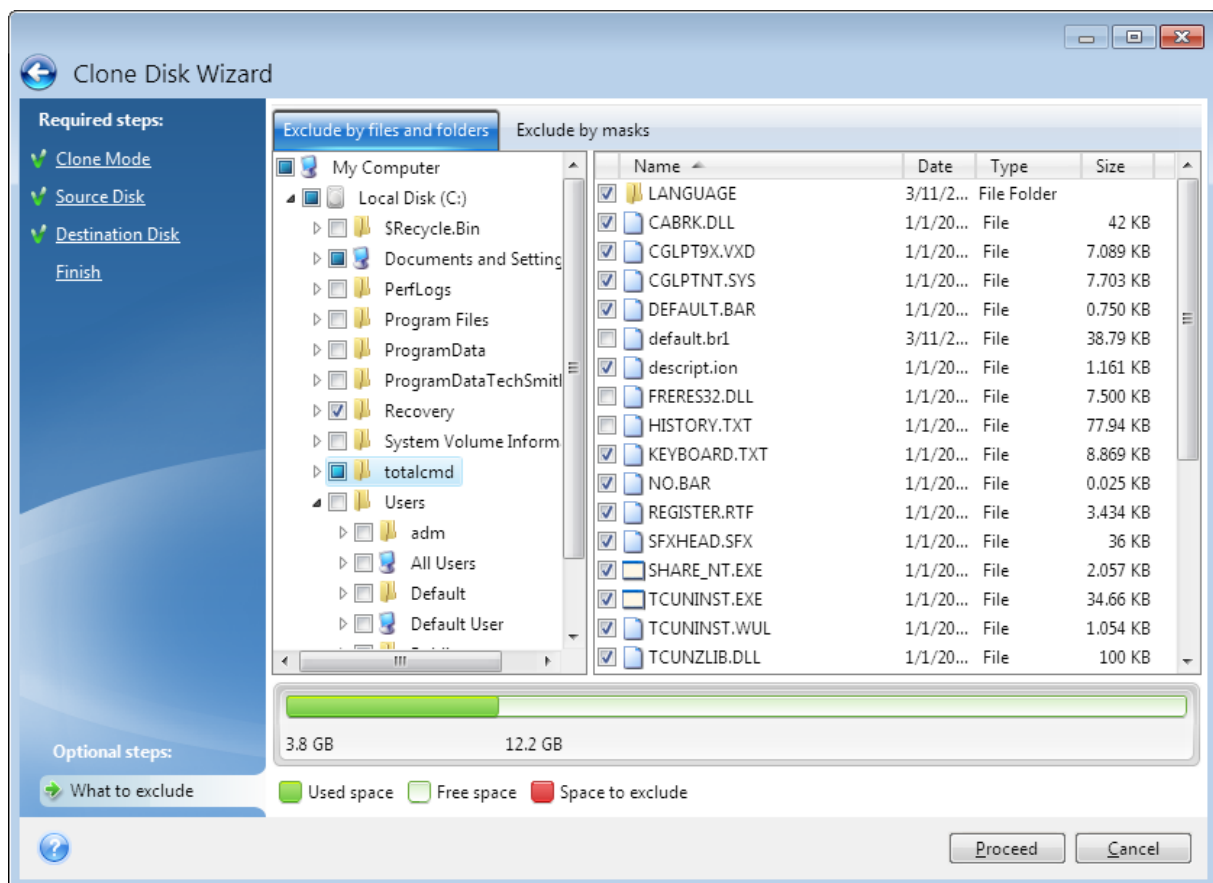
Clicking any previous wizard step on the sidebar in this window will reset all size and location changes that you've selected, so you will have to specify them again.

Excluding items from cloning

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

Note

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



You have two ways to exclude files and folders:

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

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

Examples of exclusion criteria:

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

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

Migration method

Acronis True Image allows you to select a partition layout for a target disk after clone operation completion:

- **MBR (Master Boot Sector)** - a 512-byte boot sector, which is the first sector of a hard disk, used to hold a disk's primary partition table.
- **GPT (GUID Partition Table)** - a standard for a partition table layout for hard disks. GPT allows disks/partitions size up to 9.4 ZB (9.4×10^{21} bytes).

Using this wizard you may convert your partitions layout while cloning operation or clone them as is, not changing the layout.

- **Copy partitions without changes** - select this option to migrate your system as is, not changing the partition layout. Note, in this case the disk space in excess of 2TB will be inaccessible. To allocate the disk space beyond 2TB, you may use Acronis Extended Capacity Manager.
- **Copy partitions and use a disk as non-system, GPT style** - select this option to convert your partition to a GPT layout.

With Acronis True Image you also can convert **BIOS** to **UEFI** systems. For more information, see [Unified Extensible Firmware Interface](#).

BIOS-booted system, MBR, UEFI not supported

In this step of the wizard, you need to select the destination hard disk.

Currently your system contains:

System: BIOS-booted

Source partition style: MBR

Operating system on the source disk: Windows, booting in UEFI is not supported

Destination disk size: less than 2 TB

If you migrate the system to the selected disk:

System: BIOS-booted

Partition style: MBR

Operating system: Windows, booting in UEFI is not supported

Disk size: the entire disk space is available

You can find more information about the migration procedure in [Migration method](#) section.

BIOS-booted system, MBR, UEFI supported

In this step of the wizard, you need to select the destination hard disk.

Currently your system contains:

System: BIOS-booted

Source partition style: MBR

Operating system on the source disk: Windows, booting in UEFI is supported

Destination disk size: less than 2 TB

If you migrate the system to the selected disk:

System: BIOS-booted

Partition style: MBR

Operating system: Windows, booting in UEFI is supported

Disk size: the entire disk space is available

You can find more information about the migration procedure in [Migration method](#) section.

BIOS-booted system, MBR, no Windows

Acronis True Image allows you to select a partition layout for a destination disk after the operation completion.

Currently your system contains:

System: BIOS-booted

Source partition style: MBR

Operating system on the source disk: non-Windows or no OS

Destination disk size: less than 2 TB

With these system parameters, you can select one of the following:

1. Copy partitions without changes

You may leave MBR partition style on the destination disk.

Destination disk after migration:

System: BIOS-booted

Partition style: MBR

Operating system: non-Windows or no OS

Disk size: the entire disk space is available

2. Copy partitions and use a disk as non-system, GPT style

You may convert the partition style to GPT.

Destination disk after migration:

System: not bootable in BIOS

Partition style: GPT

Operating system: non-Windows or no OS

Disk size: the entire disk space is available

Warning!

After migration, the destination disk can be used only as non-system. This option is not available if Acronis True Image is run in Windows XP x32 operating system.

You can find more information about the migration procedure in [Migration method](#) section.

BIOS-booted system, GPT, UEFI supported

In this step of the wizard, you need to select the destination hard disk.

Currently your system contains:

System: BIOS-booted

Source partition style: GPT

Operating system on the source disk: Windows, booting in UEFI is supported

If you migrate the system to the selected disk:

System: not bootable in BIOS

Partition style: GPT

Operating system: Windows, booting in UEFI is supported

Disk size: the entire disk space is available

Warning!

After migration, the operating system will not be able to boot from the destination disk in BIOS. If you want to boot from the destination disk after migration, you need to enable UEFI booting in your system (see Unified Extensible Firmware Interface section), and then restart the operation.

You can find more information about the migration procedure in [Migration method](#) section.

BIOS-booted system, GPT, no Windows

In this step of the wizard, you need to select the destination hard disk.

Currently your system contains:

System: BIOS-booted

Source partition style: GPT

Operating system on the source disk: non-Windows or no OS

If you migrate the system to the selected disk:

System: BIOS-booted

Partition style: GPT

Operating system: non-Windows or no OS

Disk size: the entire disk space is available

You can find more information about the migration procedure in [Migration method](#) section.

UEFI-booted system, MBR, UEFI not supported

In this step of the wizard, you need to select the destination hard disk.

Currently your system contains:

System: UEFI-booted

Source partition style: MBR

Operating system on the source disk: Windows, booting in UEFI is not supported

Destination disk size: less than 2 TB

If you migrate the system to the selected disk:

System: not bootable in UEFI

Partition style: MBR

Operating system: Windows, booting in UEFI is not supported

Disk size: the entire disk space is available

Warning!

The operating system may fail booting in UEFI from the destination disk.

You can find more information about the migration procedure in [Migration method](#) section.

UEFI-booted system, MBR, UEFI supported

In this step of the wizard, you need to select the destination hard disk.

Currently your system contains:

System: UEFI-booted

Source partition style: MBR

Operating system on the source disk: Windows, booting in UEFI is supported

If you migrate the system to the selected disk:

After migration, the destination partition style will be converted to GPT and you will be able to boot from it.

Destination disk after migration:

System: UEFI-booted

Partition style: GPT

Operating system: Windows, booting in UEFI is supported

Disk size: the entire disk space is available

You can find more information about the migration procedure in [Migration method](#) section.

UEFI-booted system, MBR, no Windows

Acronis True Image allows you to select a partition layout for a destination disk after the operation completion.

Currently your system contains:

System: UEFI-booted

Source partition style: MBR

Operating system on the source disk: non-Windows or no OS

Destination disk size: less than 2 TB

With these system parameters, you can select one of the following:

1. Copy partitions without changes

You may leave MBR partition style on the destination disk.

Destination disk after migration:

System: UEFI-booted

Partition style: MBR

Operating system: non-Windows or no OS

Disk size: the entire disk space is available

2. Copy partitions and use a disk as non-system, GPT style

You may convert the partition style to GPT.

Destination disk after migration:

System: not bootable in UEFI

Partition style: GPT

Operating system: non-Windows or no OS

Disk size: the entire disk space is available

Warning!

After migration, the destination disk can be used only as non-system.

You can find more information about the migration procedure in [Migration method](#) section.

UEFI-booted system, GPT, UEFI supported

In this step of the wizard, you need to select the destination hard disk.

Currently your system contains:

System: UEFI-booted

Source partition style: GPT

Operating system: Windows, booting in UEFI is supported

If you migrate the system to the selected disk:

System: UEFI-booted

Partition style: GPT

Disk size: the entire disk space is available

You can find more information about the migration procedure in [Migration method](#) section.

UEFI-booted system, GPT, no Windows

In this step of the wizard, you need to select the destination hard disk.

Currently your system contains:

System: UEFI-booted

Source partition style: GPT

Operating system: non-Windows or no OS

If you migrate the system to the selected disk:

System: UEFI-booted

Partition style: GPT

Disk size: the entire disk space is available

You can find more information about the migration procedure in [Migration method](#) section.

Migrating your system from an HDD to an SSD or NVMe drive

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

Target drive size

If the occupied space on your old hard disk exceeds the size of your target drive, 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 target drive 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 or NVMe drive using the backup and recovery method](#).

What to do if Acronis True Image does not recognize your SSD or NVMe drive

When you migrate your system from an HDD to an SSD or NVMe drive, it is possible that Acronis True Image does not recognize the new target drive.

In such a case, check whether the drive is recognized in BIOS/UEFI firmware.

If BIOS/UEFI does not show the drive, verify the physical connection (for example, SATA cable/port or M.2 slot seating). You may also try to update BIOS/UEFI and storage chipset drivers. If these suggestions do not help, contact the support team of your drive or system manufacturer.

If BIOS/UEFI does show your new drive

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 target drive. 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 target drive.
4. To remove all partition information from the target drive, run the command:

```
clean  
exit  
exit
```

Important

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

Start Acronis True Image and check whether it detects the target drive. If it does, 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 target drive

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 target drive is detected in the recovery environment.
3. If the screen shows your drive, 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 an SSD or NVMe drive using the backup and recovery method

You can use the following procedure for all supported operating systems. First, let's consider a simple case: your system disk consists of a single partition. Note that for Windows 10 and later, the system disk may have a hidden System Reserved partition.

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

To migrate your system to an SSD or NVMe drive

1. Start Acronis True Image.
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 target SSD or NVMe drive.
4. Switch off the computer and remove your system hard disk.
5. Mount the target SSD or NVMe drive into the slot where the hard disk was.

Note

For some SSD or NVMe drive models, you may need to use a PCI Express slot or adapter.

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 target SSD or NVMe drive 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.
14. Try to boot from the target SSD or NVMe drive 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 target SSD or NVMe drive. For instructions see [Recovering a disk with a hidden partition](#).

Tools

Protection tools

- "Acronis Universal Restore" (p. 248)
- "Acronis Startup Recovery Manager" (p. 215)
- "Acronis Media Builder" (p. 203)
- "Acronis Secure Zone" (p. 222)
- "Try&Decide" (p. 217)

Disk cloning

- "Disk cloning utility" (p. 187)

Security and privacy

- "Acronis DriveCleanser" (p. 232)
- "System Clean-up" (p. 237)

Disk management

- "Adding a new hard disk" (p. 227)

Image mounting

- "Mounting a backup image" (p. 244)
- "Unmounting an image" (p. 246)

Acronis Cloud Backup Download

Acronis Cloud Backup Download is a tool that lets you safely download cloud backups even if the internet connection is unstable. The download will not be canceled halfway through if the connection drops, it will be paused and can be resumed later. In addition, recovery from a downloaded backup is significantly faster than recovery from the cloud.

To install Acronis Cloud Backup Download

1. Download the tool in one of the following ways:
 - In Acronis True Image, go to the **Tools** section. Click **Acronis Cloud Backup Download** to go to the download page. Then, select and download the required version of the tool.
 - Go to <https://www.acronis.com/my/online-backup/webrestore/>, and then log in to your Acronis account. On the sidebar, click **Backups**, and then select the backup whose files you want to recover. In the details view, click **Download**. Then, in the **Download cloud backups** window, click **Download the tool**. Then, select and download the required version of the tool.
 - Go to the download page at <https://go.acronis.com/cloud-backup-download>. Then, select and download the required version of the tool.

Note

The tool will be downloaded even if you already have installed it previously.

2. Extract and run the executable file.
3. Accept the license agreement and sign in.

To download a cloud backup

Important

You can only download backups of disks, partitions, or the entire machine in the .tibx format. File or folder backups cannot be downloaded with Acronis Cloud Backup Download.

1. Start the Acronis Cloud Backup Download tool and sign in.
2. In the **Acronis Cloud Backup Download** window, select the backup that you want to download.
3. In the **Select backup to download** window, select particular backups or the entire backup set.
4. [optional step] If the backup is encrypted, enter the password.
5. Select the download destination, and then click **Save**.

The download of the .tibx file starts. You can pause or cancel it if needed.

How to use the downloaded backup

- To continue backing up the data, add the backup to Acronis True Image as described in "Adding an existing backup to the list" (p. 105).
- Recover the data from the backup as described in "Recovering disks and partitions" (p. 114).
- Create Bootable Media as described in "Creating Acronis bootable media" (p. 204).
- Create an Acronis Survival Kit as described in "Creating an Acronis Survival Kit" (p. 24).
- Mount the downloaded backup as described in "Mounting a backup image" (p. 244).

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 and recover your computer.

You can create several types of bootable media:

- **Acronis bootable media**

This type is recommended for most users.

- **WinPE-based media with the Acronis plug-in**

Running Acronis True Image in the preinstallation environment may provide better compatibility with your computer's hardware because the preinstallation environment uses Windows drivers.

We recommend that you create this type of media, when Acronis bootable media did not help you boot your computer.

To use this option, you need the following component to be installed:

- Windows Assessment and Deployment Kit (ADK).

This component is required for creating WinPE 4.0, WinPE 5.0, and WinPE 10.0.

- **WinRE-based media with the Acronis plug-in**

This type of bootable media is similar to WinPE-based media, but it has an important advantage – you do not need to download ADK (formerly known as WADK or WAIK) from the Microsoft website. Windows Recovery Environment is included in supported versions of Windows (starting from Windows 10 and later). Acronis True Image uses these files from your system to create WinRE-based media. Similar to WinPE-based media, you can add your drivers for better compatibility with your hardware. However, WinRE-based media can be used only on the computer where it was created or on a computer with the same Windows version and bitness (for example, Windows 10 x64).

Notes

- We recommend that you create a new bootable media after each Acronis True Image update.
- If you use non-optical media, the media must have a FAT16 or FAT32 file system.
- Acronis Media Builder supports only x64 WinPE 4.0, WinPE 5.0, and WinPE 10.0.
- Your computer must have:
 - For WinPE 4.0 – at least 512 MB RAM
 - For WinPE 5.0 – at least 1 GB RAM
 - For WinPE 10.0 – at least 512 MB RAM
- If Acronis Media Builder does not recognize your USB flash drive, you can try using the procedure described in the [Support Portal article](#).
- When booting from the bootable media, you cannot perform backups to disks or partitions with Ext2/Ext3/Ext4, ReiserFS, and Linux SWAP file systems.
- When booting from the bootable media and using a standalone version of Acronis True Image, you cannot recover files and folders encrypted with the encryption available in Windows operating systems. For more information, see [File-level security settings for backup](#). However, backups encrypted using the Acronis True Image encryption feature can be recovered.
- If you decide to create a bootable media on a drive that already has a Survival Kit, Acronis Media Builder will attempt to overwrite and update only the hidden partition with the bootable media without formatting the whole drive.

Creating Acronis bootable media

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

version. See [Acronis Media Builder](#) for details.

If you select a Linux-based media, choose Acronis True Image components to be placed on the media. Ensure that the components that you select are compatible with the target computer architecture. See [Removable media settings](#) for details.

If you select a WinRE-based or WinPE-based media, then:

- Select an architecture type of the media – 32-bit or 64-bit. Note that 32-bit bootable media can work only on 32-bit computers, and 64-bit media is compatible with both 32-bit and 64-bit computers.
- Select a toolkit that you want to be used for creating the bootable media. If you choose WAIK or WADK and you do not have the selected kit installed on your computer, then you first need to download it from the Microsoft website, and then install the required components – Deployment Tools and Windows Preinstallation Environment (Windows PE). If you already have WinPE files on your computer and they are stored in a non-default folder, then just specify their location and the Acronis plug-in will be added to the existing WinPE image.
- For better compatibility with your hardware, you can select drivers to be added to the media. Acronis True Image searches for and suggests drivers suitable for your system. If the search process takes too long, you can stop it by clicking the **Cancel search** button and confirming your choice.

5. Select a destination for the media:

- **CD**
- **DVD**
- **External drive**
- **USB flash drive**

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

Warning!

Formatting permanently erases all data on a disk.

Note

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

- **ISO image file**

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

When the .iso file is created, you can burn it onto a CD or DVD. For example, in Windows 10 and later, you can do this by using a built-in burning tool. In File Explorer, double-click the created ISO image file, and then click **Burn**.

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

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

To create a bootable media by using a .wim file, you first need to convert it to an .iso file. See [Creating an .iso file from a .wim file](#) for details.

Note

If Acronis Media Builder detects a previously created Survival Kit on this drive, it will attempt to overwrite and update only the hidden partition with the bootable media without formatting the whole drive.

6. Click **Proceed**.

Acronis bootable media startup parameters

Here, you can set Acronis bootable media startup parameters in order to configure the media boot options for better compatibility with different hardware. Several options are available (nousb, nomouse, noapic, etc.). These parameters are provided for advanced users. If you encounter any hardware compatibility problems while testing boot from the Acronis bootable media, it may be best to contact the Acronis Support team.

To add startup parameters

1. Enter a command into the **Parameters** field. You can type several commands, separated by spaces.
2. Click **Next** to continue.

Additional parameters that can be applied prior to booting Linux kernel

Description

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

- **acpi=off**

Disables [ACPI](#) and may help with a particular hardware configuration.

- **noapic**

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

- **nousb**

Disables loading of USB modules.

- **nousb2**

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

- **quiet**

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

- **nodma**

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

- **nofw**

Disables FireWire (IEEE1394) support.

- **nopcmcia**

Disables PCMCIA hardware detection.

- **nomouse**

Disables mouse support.

- **[module name]=off**

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

- **pci=bios**

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

- **pci=nobios**

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

- **pci=biosirq**

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

- **vga=ask**

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

Adding drivers to an existing .wim image

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

Warning!

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

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

To create a custom Windows PE image

1. If you don't have the .wim file with the Acronis plug-in, start Acronis Media Builder and create it by choosing **WIM file** as a destination for the WinPE-based media. See [Creating Acronis bootable media](#) for details.
2. Depending on your version of Windows AIK or Windows ADK, do one of the following:
 - In the **Start** menu, click **Microsoft Windows AIK**, right-click **Windows PE Tools Command Prompt**, and then select **Run as administrator**.
 - In the **Start** menu, click **Microsoft Windows AIK**, right-click **Deployment Tools Command Prompt**, and then select **Run as administrator**.
 - In the **Start** menu, click **Windows Kits**, click **Windows ADK**, right-click **Deployment and Imaging Tools Environment**, and then select **Run as administrator**.
3. Run the Copyype.cmd script to create a folder with Windows PE files. For example, from a command prompt, type:

```
copyype amd64 C:\winpe_x64
```

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

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

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

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

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

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

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

Creating an .iso file from a .wim file

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

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

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

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

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

For WinPE 3.0, type:

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

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

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

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

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

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

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

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

Making sure that your bootable media can be used when needed

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

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

To test the bootable media

Note

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

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

Note

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

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

Note

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

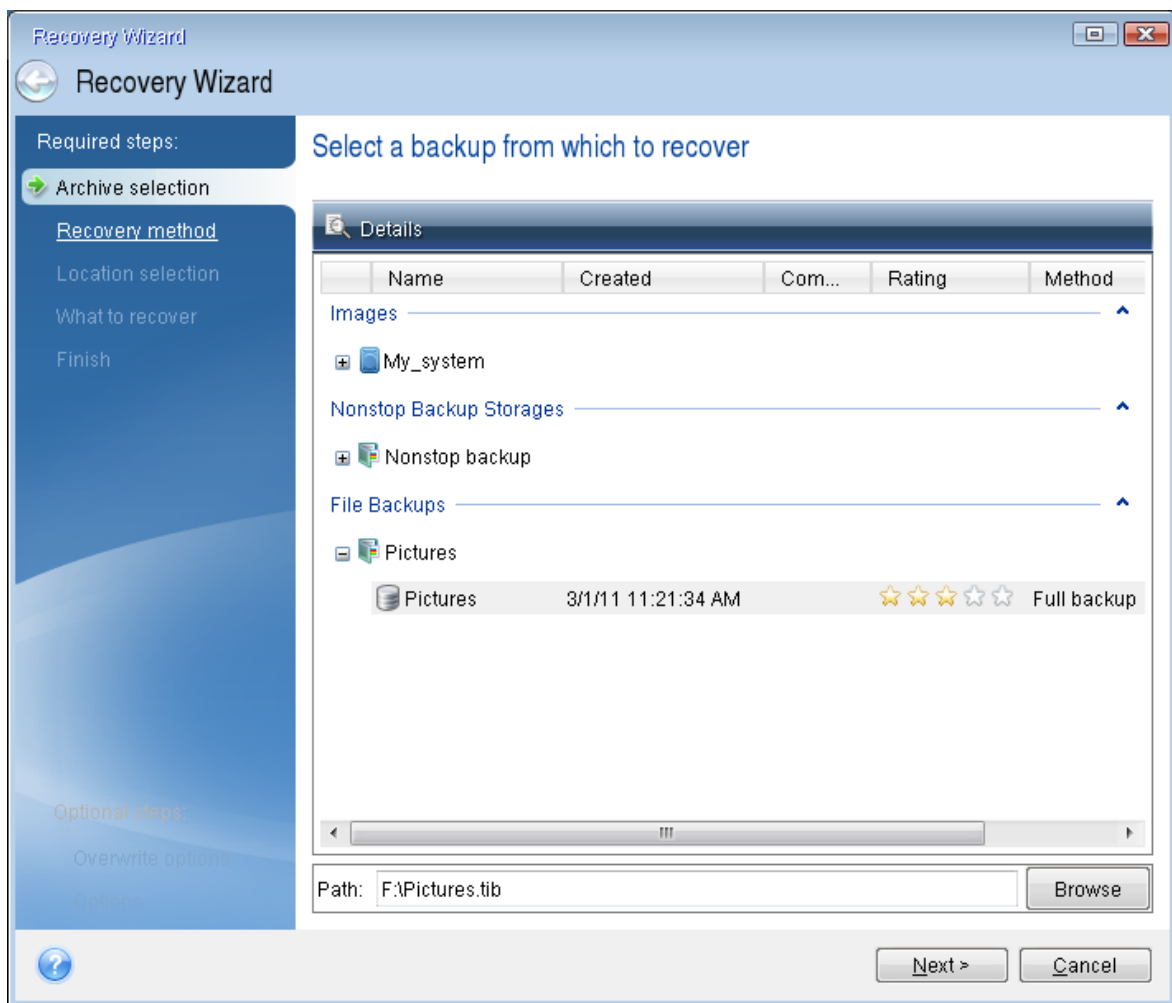
To test recovery, as well as check the drives and network adapter

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

Note

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

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



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

Note

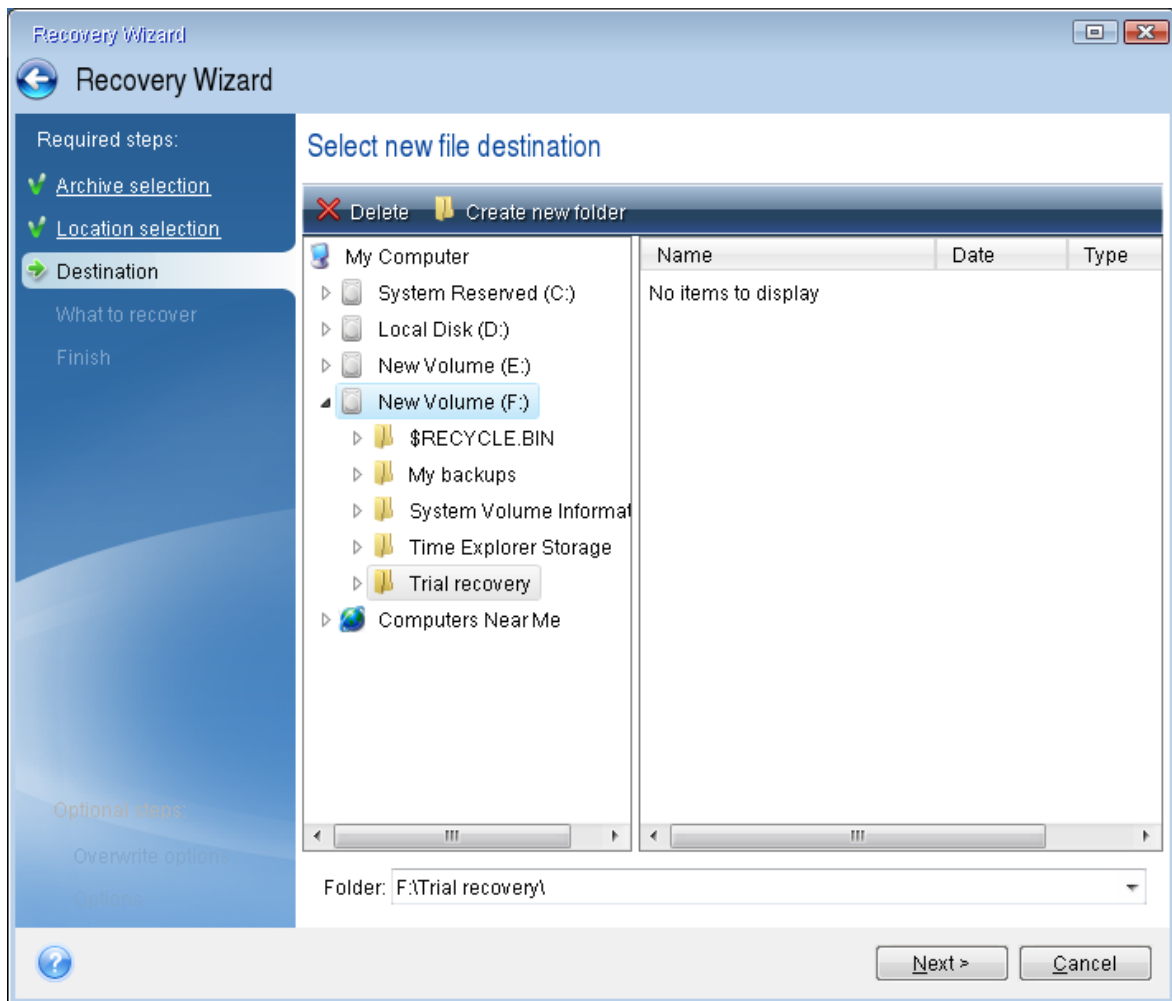
If you store your backups on the network, verify that you can access the network.

Note

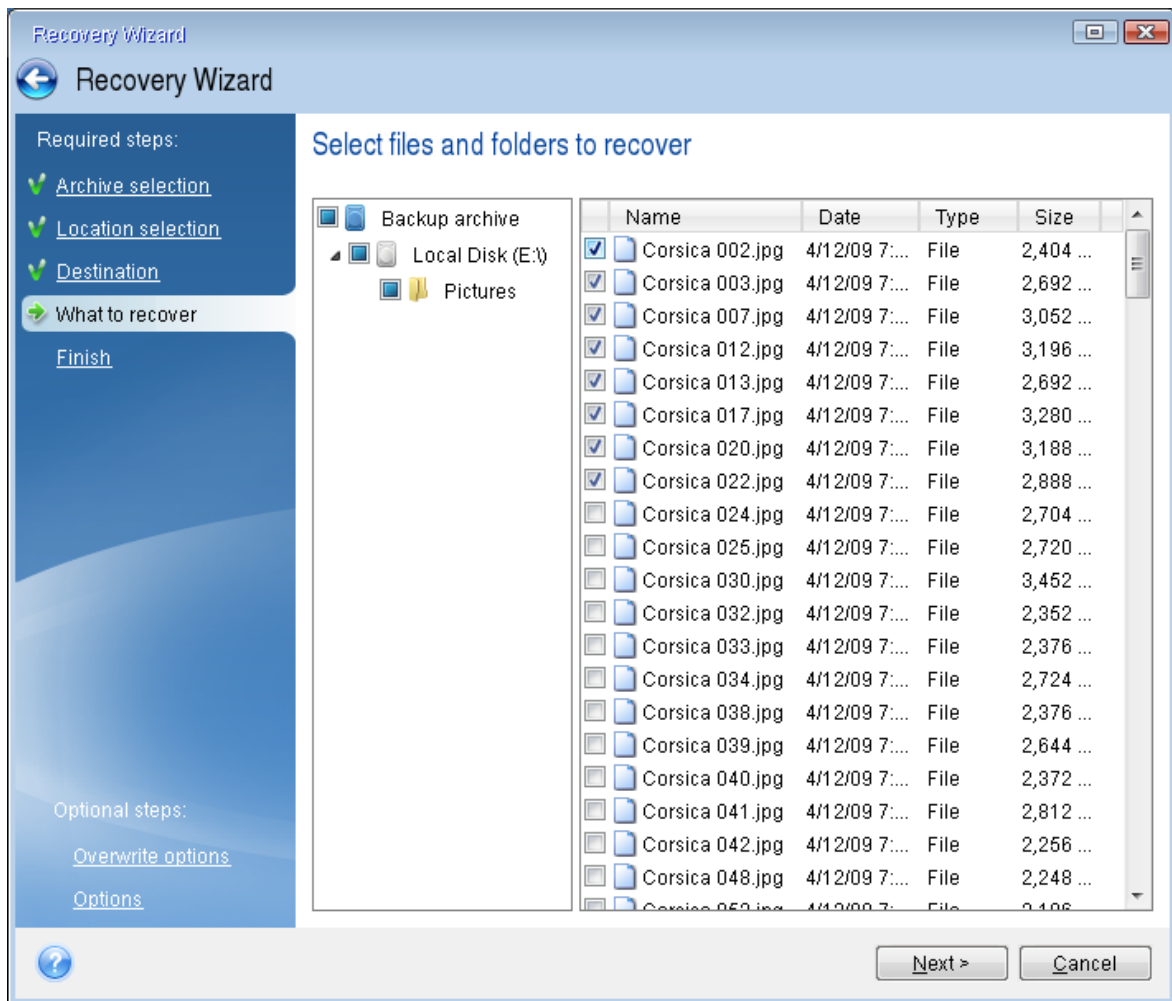
If no computers are visible on the network, but the **Computers Near Me** icon is found under **My Computer**, specify the network settings manually. To do this, open the window available at **Tools & Utilities > Options > Network adapters**.

Note

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



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



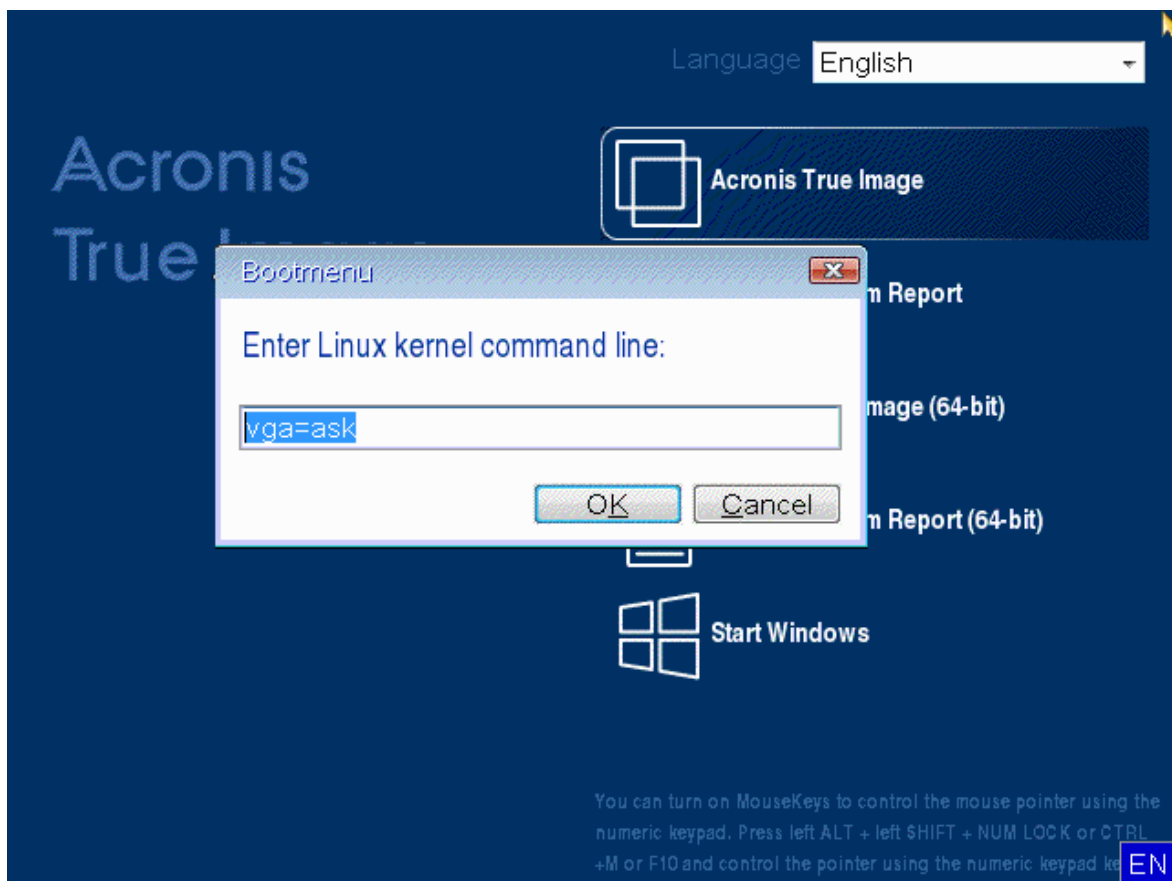
7. Click **Proceed** on the Summary window to start recovery.
8. After the recovery finishes, exit the standalone Acronis True Image.

Now, you can be reasonably sure that your 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** item and press the F11 key.
2. When the command line appears, type **vga=ask** and click **OK**.



3. Select **Acronis True Image** 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 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 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.

Acronis Startup Recovery Manager

The Acronis Startup Recovery Manager lets you start Acronis True Image without loading the operating system. With this feature, you can use Acronis True Image by itself to recover damaged partitions, even if the operating system won't boot. Unlike booting from Acronis removable media, you will not need a separate media or network connection to start Acronis True Image.

Note

Acronis Startup Recovery Manager cannot be used on tablets running Windows.

To activate Acronis Startup Recovery Manager

1. Start Acronis True Image.
2. In the **Tools** section, click **All tools**, and then double-click **Activate Acronis Startup Recovery Manager**.
3. In the opened window, click **Activate**.

If a failure occurs, turn on the computer and press F11 when you see the "Press F11 for Acronis Startup Recovery Manager" message. This will start a standalone version of Acronis True Image that differs only slightly from the complete version.

To deactivate Acronis Startup Recovery Manager

1. Start Acronis True Image.
2. In the **Tools** section, click **All tools**, and then double-click **Activate Acronis Startup Recovery Manager**.
3. In the opened window, click **Deactivate**.

Additional information

Disk letters in standalone Acronis True Image might sometimes differ from the way Windows identifies drives. For example, the D: disk identified in the standalone Acronis True Image might correspond to the E: disk in Windows. The disk labels and information on partition sizes, file systems, drive capacities, their manufacturers, and model numbers can help in correctly identifying the disks and partitions.

You won't be able to use the previously activated Acronis Startup Recovery Manager if the Try&Decide is turned on. Rebooting the computer in the Try mode will allow you to use Acronis Startup Recovery Manager again.

The Acronis Startup Recovery Manager cannot be activated on a BitLocker-encrypted disk. Activation is possible only if at least one partition is not locked by BitLocker, has sufficient free space for loader files, and meets the disk type requirements (for example, GPT on UEFI systems). For more information, see [Startup Recovery Manager and BitLocker limitations](#) and [BitLocker Compatibility with Acronis True Image](#).

Does Acronis Startup Recovery Manager affect other loaders?

When Acronis Startup Recovery Manager is activated, it overwrites the master boot record (MBR) with its own boot code. If you have any third-party boot managers installed, you will need to reactivate them after the Startup Recovery Manager has been activated. For Linux loaders (e.g. LiLo and GRUB), you might consider installing them to a Linux root (or boot) partition boot record instead of MBR before activating Acronis Startup Recovery Manager.

UEFI boot mechanism is different from the BIOS one. Any OS loader or other boot program has its own boot variable that defines a path to the corresponding loader. All loaders are stored on a special partition called EFI System Partition. When you activate Acronis Startup Recovery Manager in UEFI-booted system, it changes the boot sequence by writing its own boot variable. This variable is added to the list of variables and does not change them. Since all loaders are independent and do not affect each other, there is no need to change anything before or after activating Acronis Startup Recovery Manager.

Try&Decide

Note

To install Try&Decide, you can select this component when installing Acronis True Image, or add it later as described in "Installing Acronis True Image" (p. 14).

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.

When Try&Decide can help

We recommend that you turn Try&Decide on before you try to:

- Change any system settings, when you are not sure how these changes may affect your computer.
 - Install system updates, drivers, etc.
 - Install unfamiliar applications.
 - Open email attachments from unknown senders.
 - Visit websites that might contain potentially troublesome content.
-

Note

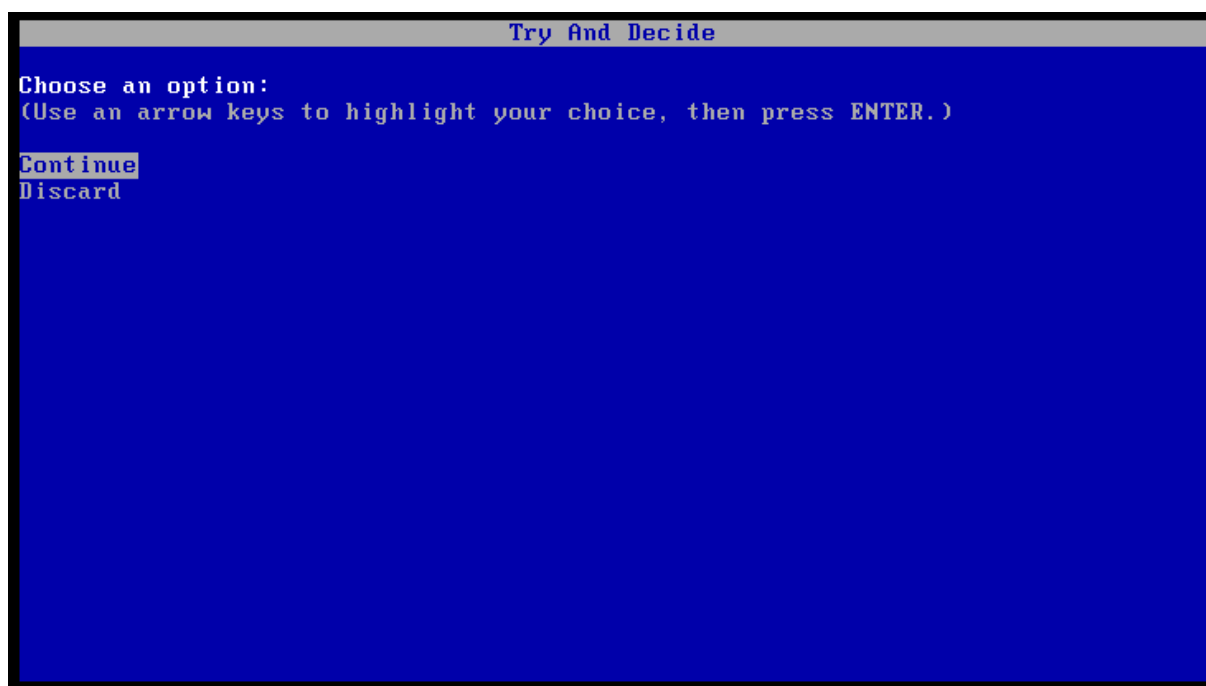
Remember that if you download email from a POP mail server, create new files or edit existing documents while in the Try mode, and then decide to discard your changes, those files, document changes, and mail will no longer exist. In this case, save the new files and edited documents, for example, to a USB flash drive and unplug it before discarding the changes.

How Try&Decide works after a computer restart

You can leave the Try&Decide turned on as long as you like, because this mode "survives" across reboots of your operating system.

When your computer reboots for whatever reason while working in the Try mode, before booting of the operating system starts, you will be shown a dialog offering you two choices – stop the mode and discard changes or continue working in the mode. This will allow you to discard the changes that have resulted in a system crash. On the other hand, if you reboot, for example, after installing an application, you can continue working in the Try mode after starting Windows.

Every "soft" reboot of your computer while in the Try mode results in adding up to 500 MB of Try&Decide's housekeeping data into the storage selected for storing virtual changes.

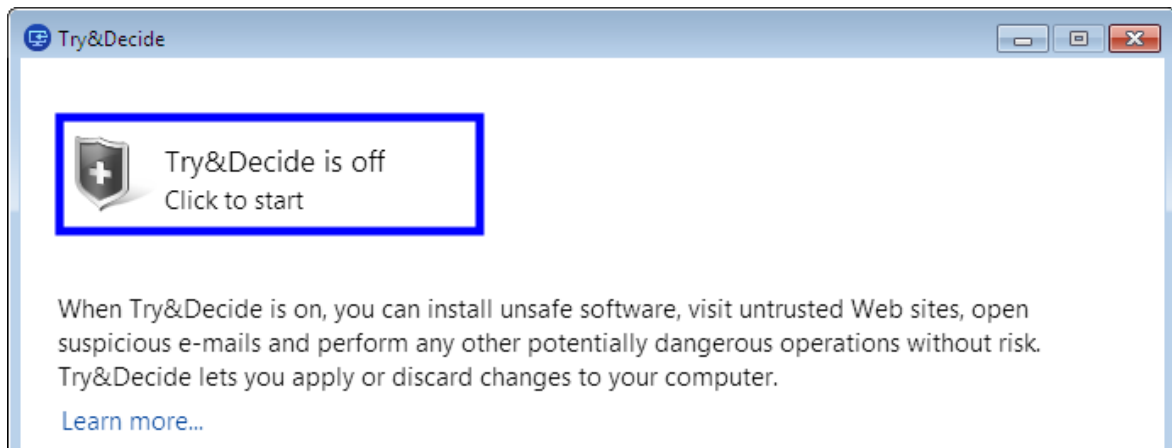


Limitations in using Try&Decide

- Try&Decide is not compatible with the Memory integrity feature of Windows (turned on by default in Windows 11). To avoid compatibility issues with Try&Decide, you can turn off Memory integrity in the Windows Security settings.
- If you use Windows 10 or Windows 11, in the Try mode the program may use free disk space quite intensively, even when your computer is idle. This is due to housekeeping activities such as indexing that run in the background.
- While working in the Try mode you will experience slowing down of the system performance. Furthermore, the process of applying changes may take a long time, especially if you leave the Try mode turned on days on end.
- Try&Decide cannot track changes in disk partitions, so you will be unable to use the Try mode for virtual operations with partitions such as resizing partitions or changing their layout. In addition, you must not use the Try&Decide and disk defragmentation or disk error checking utilities at the same time, because this can irreparably corrupt the file system, as well as make the system disk unbootable.
- When the Try mode is started, you won't be able to use the previously activated Acronis Startup Recovery Manager. Rebooting the computer in the Try mode will allow you to use Acronis Startup Recovery Manager again.
- Try&Decide and Nonstop Backup cannot work simultaneously. Starting the Try mode suspends Nonstop Backup. Nonstop Backup will resume after you stop the Try mode.
- When the Try mode is started, you won't be able to use the Hibernate power saving mode.
- Try&Decide cannot be used for protecting dynamic disks.
- Try&Decide cannot work when a partition in your system is encrypted with BitLocker.
- Try&Decide cannot protect Acronis Secure Zone or use it as a storage for the virtual changes.

Using Try&Decide

1. Start Acronis True Image.
2. In the **Tools** section, click **Try&Decide**.
3. Set up the Try&Decide options, if necessary. See [Try&Decide options and notifications](#) for details.
4. To start the Try mode, click the **Try&Decide** icon. The program starts tracking all changes made to the OS and files and temporarily stores all the changes on the selected disk.

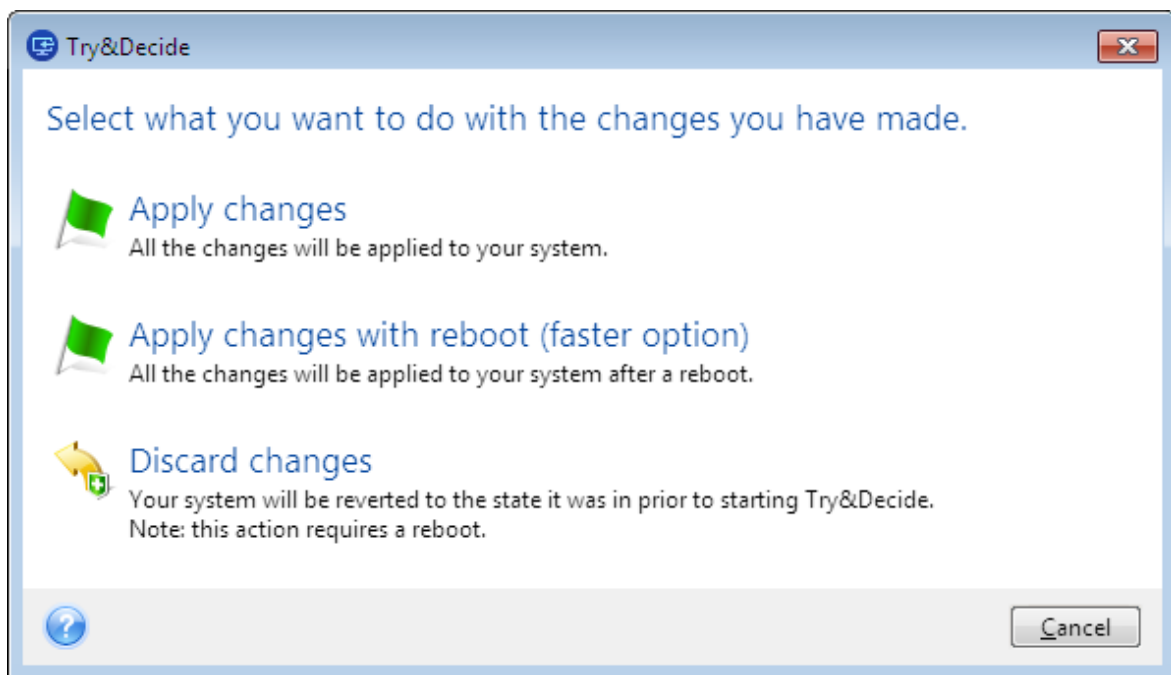


5. Perform all the changes you wanted to try.

Note

When the disk space in the location selected for storing virtual changes is minimal for applying the changes, the program asks you whether to apply or discard the changes. If you ignore the alert message, the program will automatically restart the system when the disk is full, and discard the changes.

6. To stop the Try mode, click the **Try&Decide** icon in the **Try&Decide** window.



7. Choose one of the following:

- Select **Apply changes** if you want to keep the changes made to the system.
- Select **Apply changes with reboot** if you want to speed up the applying process. When you click the button, Try&Decide restarts your computer and applies the changes during the reboot.
- Select **Discard changes** if you want to return your system to the state it was in prior to turning on the Try mode. When you select this option, a pop-up window is displayed with the following options: **Reboot to discard changes** and **Do not reboot**. If you select the **Do not reboot** option, the Try&Decide feature remains on, and the changes will not be discarded.

Note

If you have chosen **Discard Changes** and rebooted the computer with multiple operating systems installed, you won't be able to boot other operating systems except the one used for working in the Try mode. A second reboot will recover the original MBR and make other operating systems bootable.

Try&Decide options and notifications

You can change Try&Decide options in the Try&Decide window. To restore the default values of the settings, click Reset settings to default.

Protected partitions

To change this setting:

1. Click the partition letter next to the setting name. The Partition Selection window opens.
2. Select the partitions that you want to protect, and then click **OK**.

By default, Try&Decide protects the system partition (Disk C), though you may choose to protect any other partitions in your system.

Storage for virtual changes

To change this setting:

1. Click the partition letter next to the setting name. The Storage for Virtual Changes window opens.
2. Select the partition that you want to use as a storage for virtual changes, and then click **OK**.
By default, Try&Decide saves the information to a free space on Disk C.

Note

When choosing to protect more than one partition, you cannot select one of the partitions to be protected to store virtual changes. In addition, you cannot select an external hard disk drive.

Notifications

To change the default notification settings, click **Change alert settings**. The Settings window opens.

- On free disk space remaining - If the amount of free space in the storage for virtual changes becomes less than the specified value, the program displays a notification message.
- On time elapsed since Try&Decide started - The program will notify you if Try&Decide has been working for longer than the period of time that you specified.

Try&Decide: typical use cases

The Try&Decide feature can help you in various circumstances, for example:

Software evaluation

Sometimes it may be useful to turn on the Try mode before installing new software. For example, we recommend that you turn it on when you want to:

- Choose antivirus software.
There are known cases when installation of antivirus software cripples functionality of some applications or they may even refuse to launch after antivirus installation. You can test a trial version of the antivirus. If you encounter any problems, discard the changes in your system and try antivirus software from another vendor.
- Install a trial version of a program.
It is well known that the "Add or Remove Programs" component of the Windows Control Panel cannot give a complete guarantee of cleanly uninstalling applications. If you do not like the program that you installed, discard the changes in your system. In this case, you can be sure that Try&Decide removed the program without a trace.
- Install suspicious software.

If you do not trust the vendor of the software that you want to install, or when the source of the software is unknown, turn on the Try mode before installing this software. If anything goes wrong, discard the changes made in the Try mode.

File recovery

You have accidentally deleted some files and then emptied the Recycle Bin. Then you have remembered that the deleted files contained important data and now you are going to try to undelete them using the appropriate software. However, sometimes you may do something wrong while trying to recover deleted files, making things worse than before trying to recover them. So you can proceed as follows:

- Turn on the Try mode.
- Launch the file undelete utility.
- After the utility scans your disk in search of the deleted file or folder entries, it will present you the deleted entries it has found (if any) and offer you the opportunity to save whatever it can recover. There is always a chance that you might pick the wrong file and while recovering it the utility may overwrite the very file you are trying to recover. If not for the Try&Decide, this error would be fatal and the file would be lost irretrievably.
- But now you can just discard the changes made in the Try mode and make one more attempt to recover the files after turning on the Try mode again. Such attempts may be repeated until you are sure that you have done your best in trying to recover the files.

Web privacy

Suppose you do not want anybody to know, which Web sites you have visited or which pages you have opened - we all have the right to privacy. But the problem is that to make your Web surfing more comfortable and fast, the system stores this information and much more: cookies you have received, search engine queries you have made, URLs you have typed, etc. in special hidden files. And such information is not deleted completely when you clear your temporary internet files, delete cookies, clear history of the recently opened Web pages using the browser's tools. So snoopers may be able to view the information using special software.

Turn on the Try mode and surf the Web as you please. Afterwards, if you want to remove all traces of your activity, discard the changes made in the Try mode.

Acronis Secure Zone

The Acronis Secure Zone is a special secure partition that you can create on your computer for storing backups. The Acronis Secure Zone has a FAT32 file system.

When you create an Acronis Secure Zone, it is displayed in the **Other** section of File Explorer. You can navigate through the Acronis Secure Zone as an ordinary partition.

If Acronis Secure Zone is password-protected, any operation, except viewing version details, requires entering the password.

Acronis Secure Zone cleanup

If there is not enough space in the Acronis Secure Zone for a new backup, you can:

- Cancel the backup operation, increase the size of the Acronis Secure Zone, and then run the backup again.
- Cancel the backup operation, manually delete some backups in the Acronis Secure Zone, and then run the backup again.
- Confirm that you want to automatically delete the oldest backup of the same type (file-level or disk-level) with all subsequent incremental and differential versions. After that, if free space is still insufficient, Acronis True Image asks for confirmation and will delete the next full backup. This will repeat until there is enough free space for the new backup. If after deleting all the previous backups there is still not enough space, the backup will be canceled.

To prevent the zone overflow:

1. Select a scheduled backup.
2. Click **Options**.
3. On the **Advanced** tab, expand the **Error handling** section.
4. Select the **When not enough space in ASZ, delete the oldest backup** check box.
5. Click **OK**.

See [Error handling](#) for details.

You cannot use the Acronis Secure Zone as the storage for virtual system changes in the Try mode. The Try&Decide data will be automatically cleaned up after you stop a Try&Decide session.

Acronis True Image does not delete nonstop backup versions in the Acronis Secure Zone automatically. Such versions can only be deleted manually. For more information see [Acronis Nonstop Backup data storage](#).

Creating and managing Acronis Secure Zone

1. Click the **Start** button → **Acronis** (product folder) → **Acronis Secure Zone** .
The Manage Acronis Secure Zone wizard opens.
2. Perform one of the following:
If you want to create the Acronis Secure Zone, specify its [location](#) and [size](#).
If you want to modify the Acronis Secure Zone, select an action:
 - [Increase or decrease size](#)
 - [Remove](#)
 - [Change password](#)Then follow the wizard steps.
3. On the **Finish** step, click **Proceed**.

Note

This operation may require a computer restart.

Acronis Secure Zone location

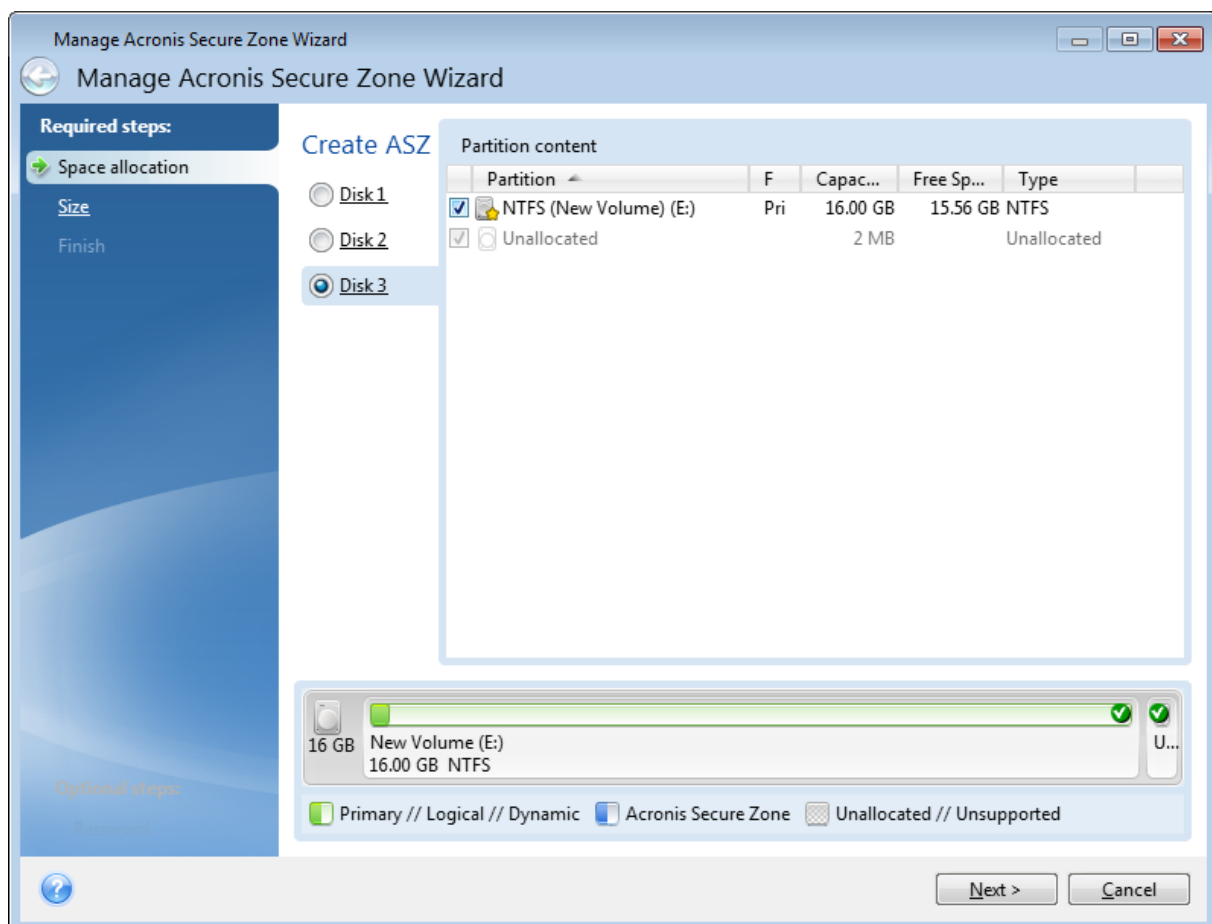
To specify a location for the Acronis Secure Zone

1. Select a hard disk drive to create the Acronis Secure Zone on.
2. Select one or more partitions from which unallocated and/or free space will be taken. The chosen partitions will be resized if necessary to give space to the Acronis Secure Zone.

Note

The Acronis Secure Zone cannot be created on dynamic disks and volumes.

3. Click **Next**.

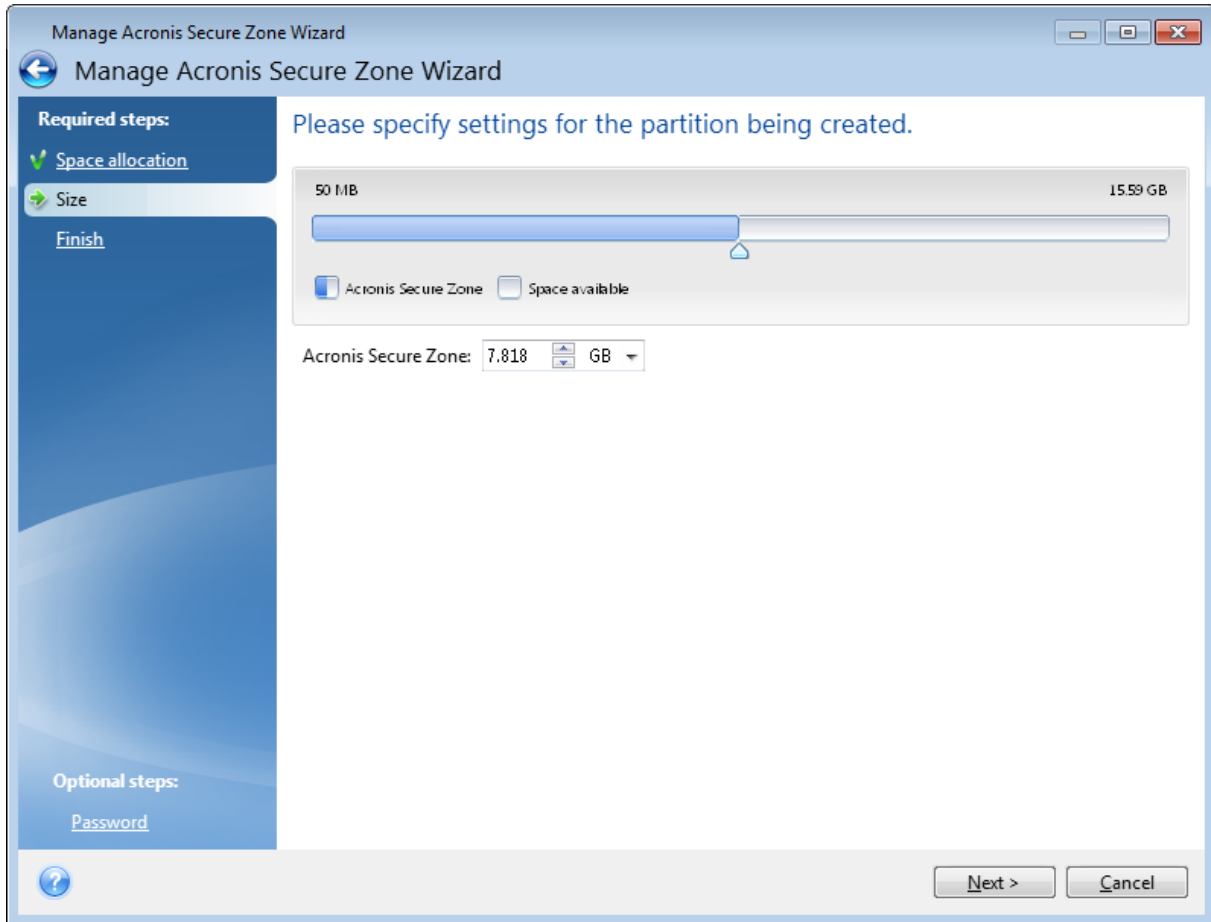


To increase or decrease the size of the Acronis Secure Zone

1. Select the partitions from which space will be used to increase the size of the Acronis Secure Zone, or that will receive free space after the size of the Acronis Secure Zone is reduced. You can also select partitions with unallocated space.
2. Click **Next**.

Size of Acronis Secure Zone

To specify the size of the Acronis Secure Zone, drag the slider to the appropriate position or type an exact value.



The minimum size is about 50 MB, depending on the geometry of the hard disk. The maximum size is equal to the disk's unallocated space plus the total free space on all partitions selected at the previous step.

When creating/enlarging the Acronis Secure Zone, the program will first use the unallocated space. If the unallocated space is not enough to achieve the desired size, the selected partitions will be decreased in size. Resizing of partitions may require the computer to be rebooted.

When reducing the size of the Acronis Secure Zone, if there is any unallocated space on the hard disk, it will be allocated to the selected partitions along with the space freed up from the Acronis Secure Zone. Thus, no unallocated space will remain on the disk.

Warning!

Reducing a system partition to the minimum size may prevent your operating system from booting-up.

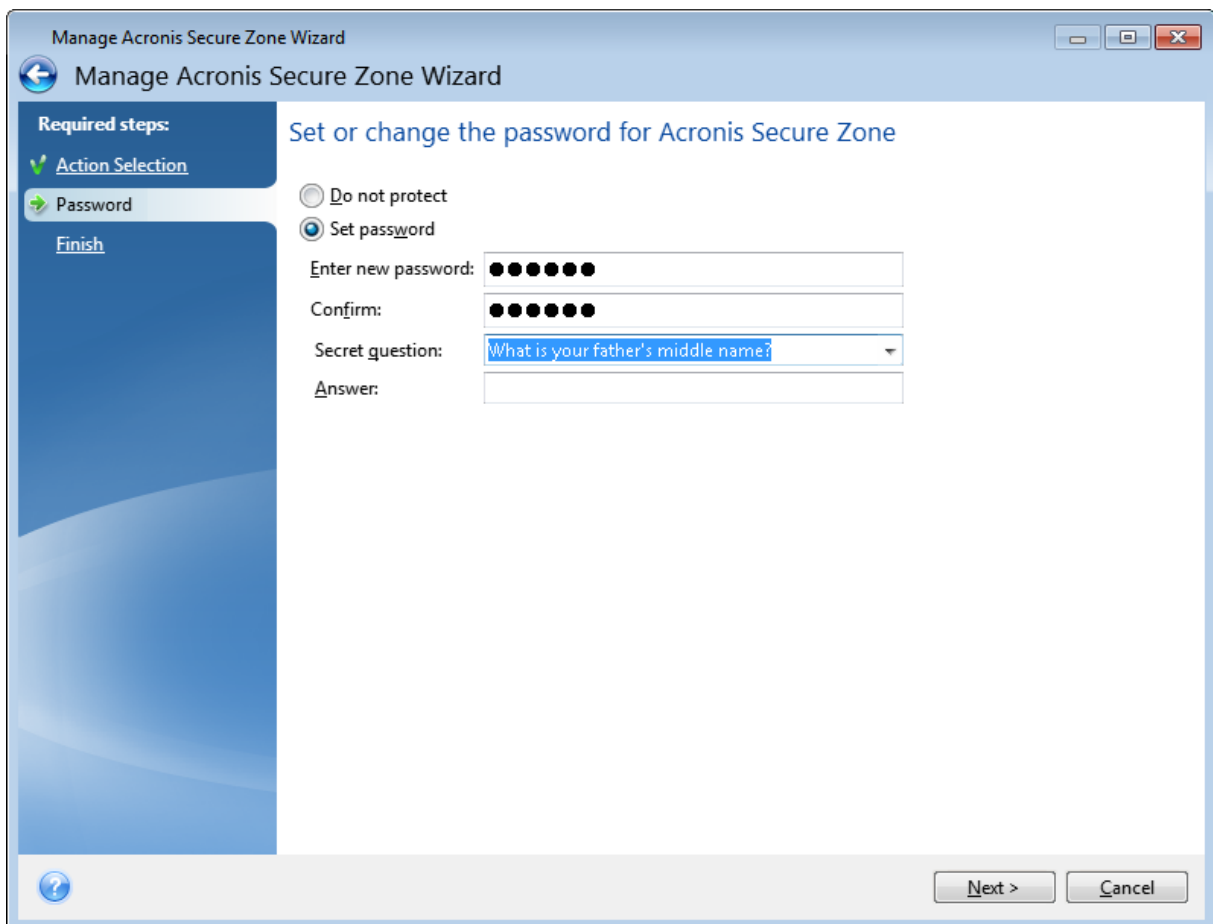
Acronis Secure Zone protection

You can set up password protection for the Acronis Secure Zone in order to prevent it from unauthorized access.

The program will ask for the password at any operation relating to the Acronis Secure Zone such as data backup and recovery, mounting images or validating backups in the Acronis Secure Zone, resizing and deleting the Acronis Secure Zone.

To set a password for the Acronis Secure Zone

1. Select **Set password**.
2. Type the password in the **Password** field.
3. Retype the previously entered password in the **Confirm** field.
4. [Optional step] You can also select a secret question that will be asked in case you forget the password. Select a secret question from the list and enter an answer to it.
5. Click **Next** to continue.



The screenshot shows the 'Manage Acronis Secure Zone Wizard' window. The title bar reads 'Manage Acronis Secure Zone Wizard'. The main window has a blue header with the title 'Manage Acronis Secure Zone Wizard'. On the left, there is a 'Required steps' sidebar with three items: 'Action Selection' (marked with a green checkmark), 'Password' (marked with a green arrow), and 'Finish' (marked with a blue question mark). The main area is titled 'Set or change the password for Acronis Secure Zone'. It contains two radio buttons: 'Do not protect' (unselected) and 'Set password' (selected). Below these are four input fields: 'Enter new password:' (filled with black dots), 'Confirm:' (filled with black dots), 'Secret question:' (a dropdown menu showing 'What is your father's middle name?'), and 'Answer:' (empty). At the bottom right, there are two buttons: 'Next >' and 'Cancel'.

Note

Acronis True Image repair or update will not affect the password. However, if the program is removed and then installed again while keeping the Acronis Secure Zone on the disk, the password to the Acronis Secure Zone will be reset.

Removing Acronis Secure Zone

Warning!

Acronis Secure Zone deletion will automatically destroy all backups stored in the zone.

Select the partitions to which you want to add the space freed up from Acronis Secure Zone. If you select several partitions, the space will be distributed proportionally to each partition's size.

Also, you can choose to remove the Acronis Secure Zone while uninstalling the program.

Adding a new hard disk

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

To add a new hard disk

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

Note

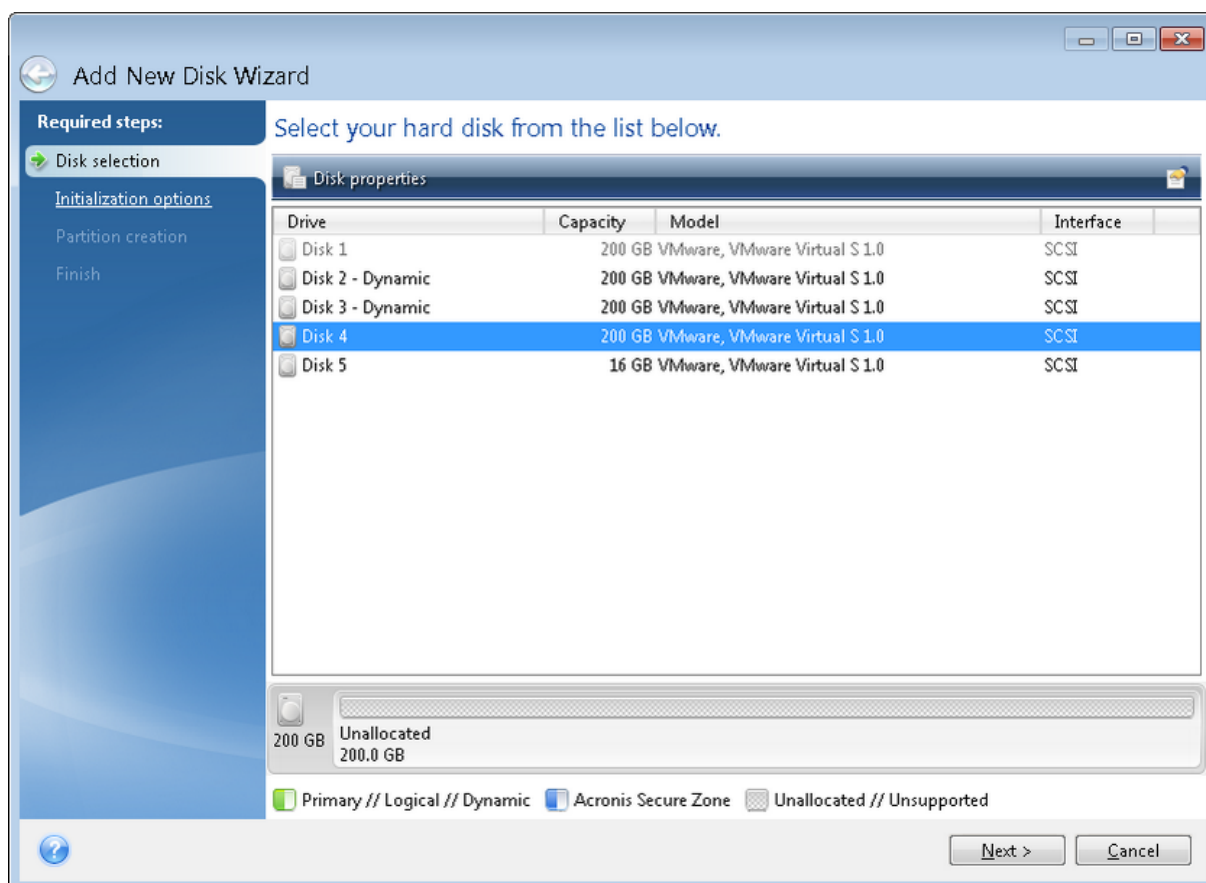
In the wizard, you select the disk layout (MBR or GPT) and can create one or more partitions (for example, NTFS/FAT32, or EXT4/Linux Swap) plus unallocated space. After you click **Proceed**, the tool creates the partitions and assigns sizes, names, and drive letters.

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.

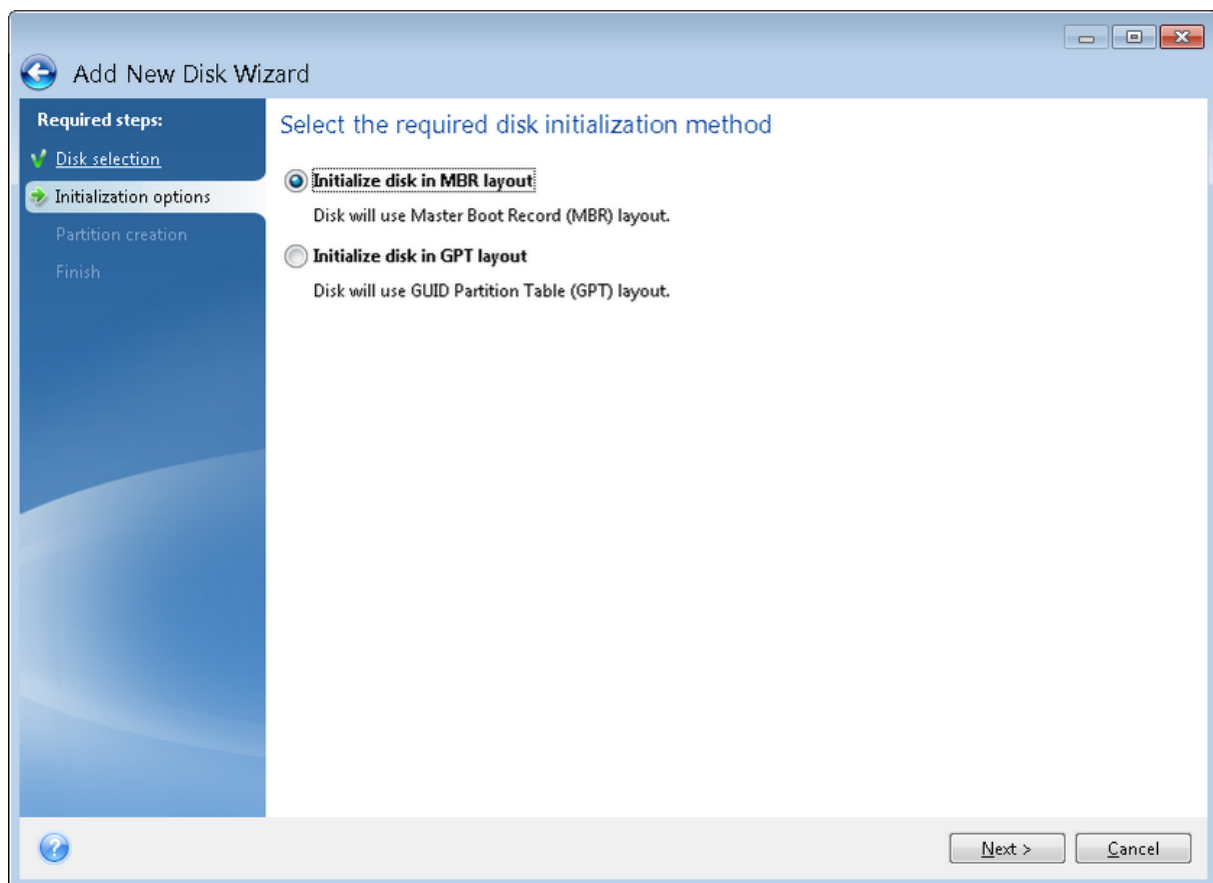
Note

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



Selecting initialization method

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



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

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

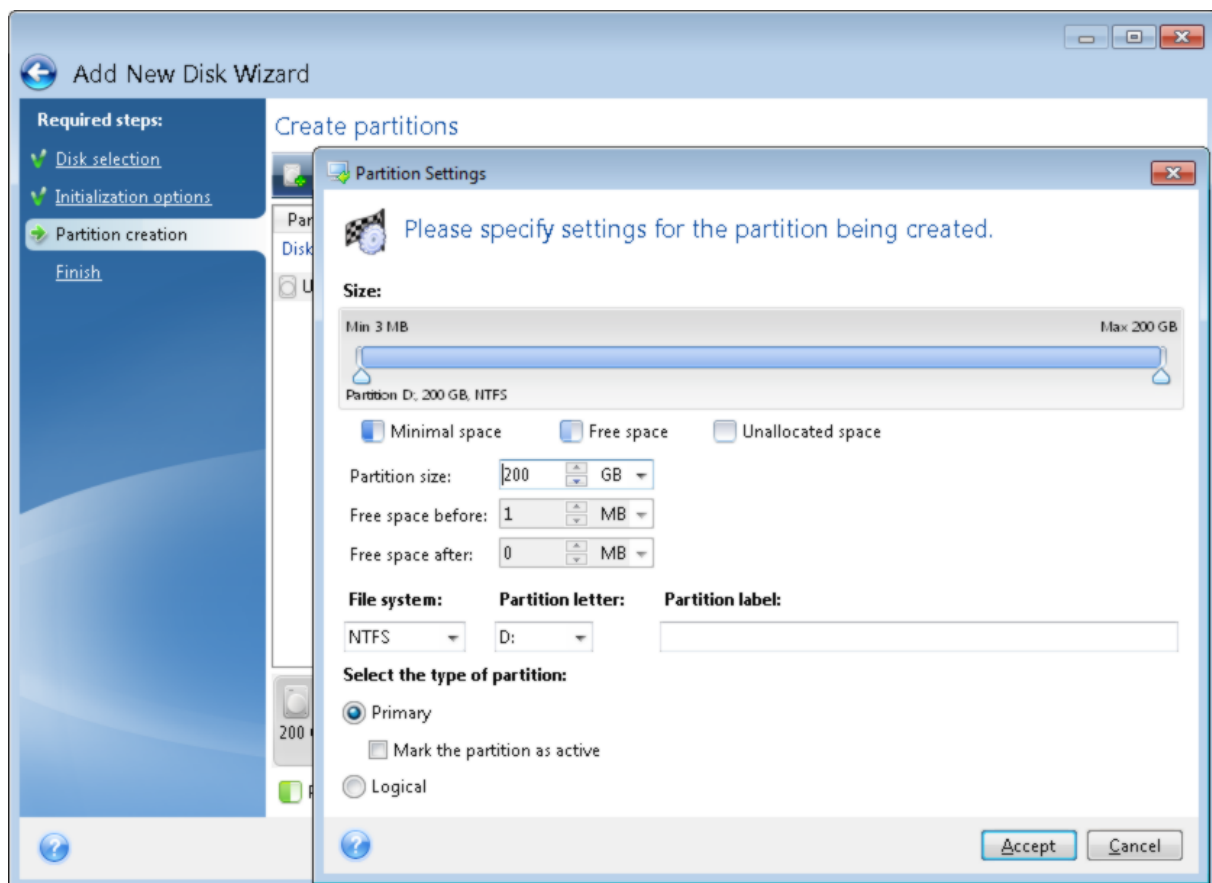
Creating new partitions

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

To create a new partition

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

See [Partition settings](#) for details.
3. Click **Accept**.



Partition settings

Size

To resize the partition, do one of the following

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

To relocate the partition, perform one of the following

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

Note

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

File System

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

- **NTFS** is a native file system for Windows NT, Windows 2000, Windows XP, and later operating systems. Choose it if you use these operating systems. Note, that Windows 95/98/Me and DOS cannot access NTFS partitions.
- **FAT 32** is an improved 32-bit version of the FAT file system that supports volumes up to 2 TB.
- **FAT 16** is a DOS native file system. Most operating systems recognize it. However, if your disk drive is more than 4 GB, it is not possible to format it in FAT16.
- **Ext2** is a Linux native file system. It is fast enough, but it is not a journaling file system.
- **Ext3** – officially introduced with Red hat Linux version 7.2, Ext3 is a Linux journaling file system. It is forwards and backwards compatible with Linux Ext2. It has multiple journaling modes, as well as broad, cross platform compatibility in both 32-bit and 64-bit architectures.
- **Ext4** is a new Linux file system. It has improvements in comparison to ext3. It is fully backward compatible with ext2 and ext 3. However, ext3 has only partial forward compatibility with ext4.
- **ReiserFS** is a journaling file system for Linux. Generally it is more reliable and faster than Ext2. Choose it for your Linux data partition.
- **Linux Swap** is a swap partition for Linux. Choose it if you want to add more swap space using Linux.

Partition letter

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

Partition label

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

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

You can define the new partition as primary or logical.

- **Primary** - choose this parameter if you are planning to boot from this partition. Otherwise, it is better to create a new partition as a logical drive. You can have only four primary partitions per drive, or three primary partitions and one extended partition.

Note

If you have several primary partitions, only one will be active at a time, the other primary partitions will be hidden and won't be seen by the OS.

- **Mark the partition as active** - select this check box if you are planning to install an operating system on this partition.
- **Logical** - choose this parameter if you don't intend to install and start an operating system from the partition. A logical drive is part of a physical disk drive that has been partitioned and allocated as an independent unit, but functions as a separate drive.

Security and Privacy Tools

Acronis DriveCleanser

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

Why do I need it?

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

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

How to use Acronis DriveCleanser

To permanently destroy data on your disk

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

Warning!

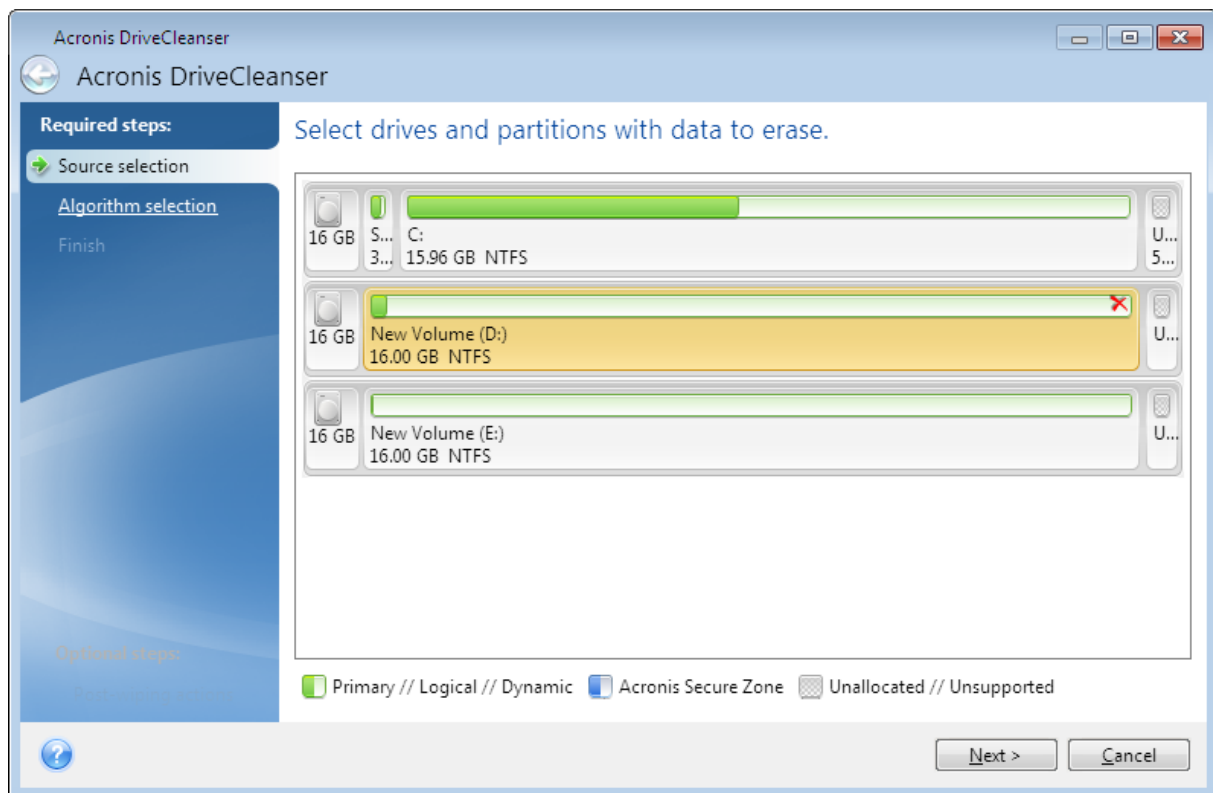
Be aware that, depending on the total size of selected partitions and the selected data destruction algorithm, the data destruction may take many hours.

Source selection

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

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

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



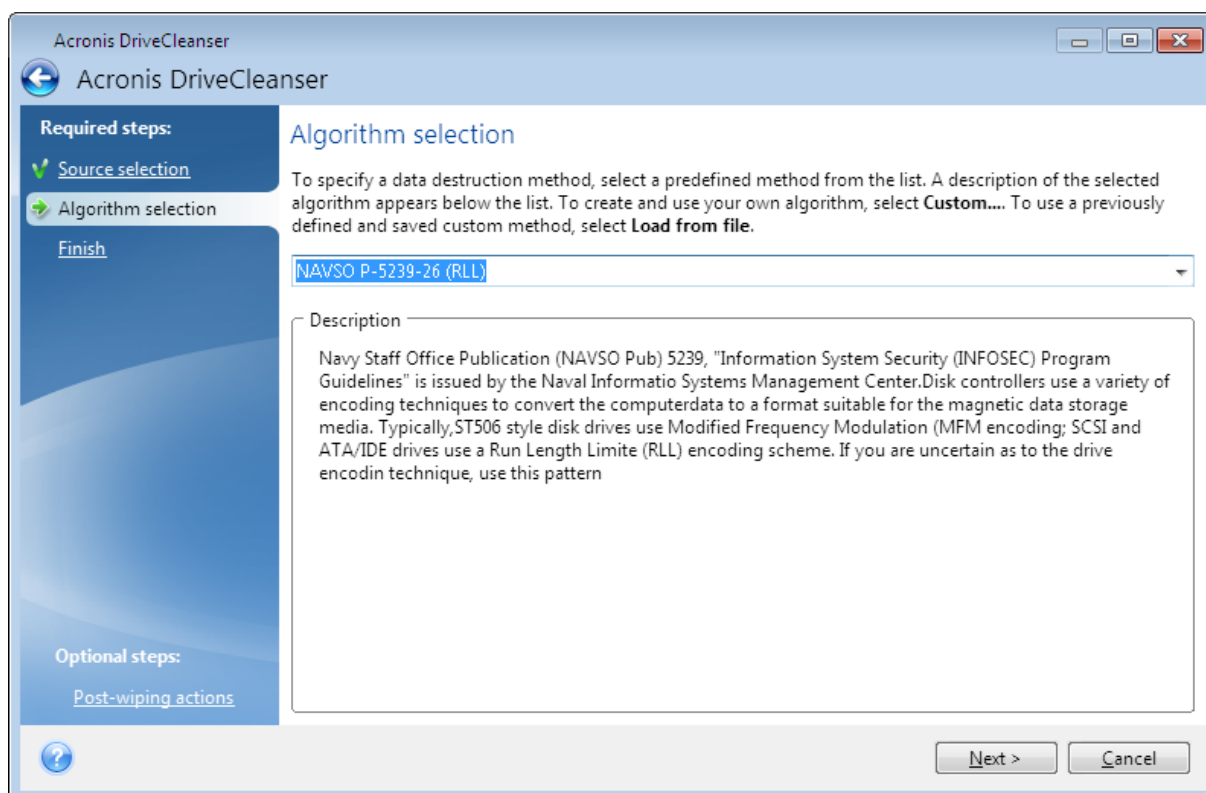
Note

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

Algorithm selection

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

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



Hard Disk Wiping methods

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

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

Information wiping methods

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

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

No.	Algorithm (writing method)	Passes	Record
2.	United States: NAVSO P-5239- 26 (RLL)	4	1 pass – 0x01 to all sectors, 2 – 0x27FFFFFF, 3 – random symbol sequences, 4 – verification.
3.	United States: NAVSO P-5239- 26 (MFM)	4	1 pass – 0x01 to all sectors, 2 – 0x7FFFFFFF, 3 – random symbol sequences, 4 – verification.
4.	German: VSITR	7	Passes 1 – 6 – alternate sequences of: 0x00 and 0xFF; pass 7 – 0xAA; i.e. 0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF, 0xAA.
5.	Russian: GOST P50739-95	1	Logical zeros (0x00 numbers) to each byte of each sector for the sixth to fourth security level systems. 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.

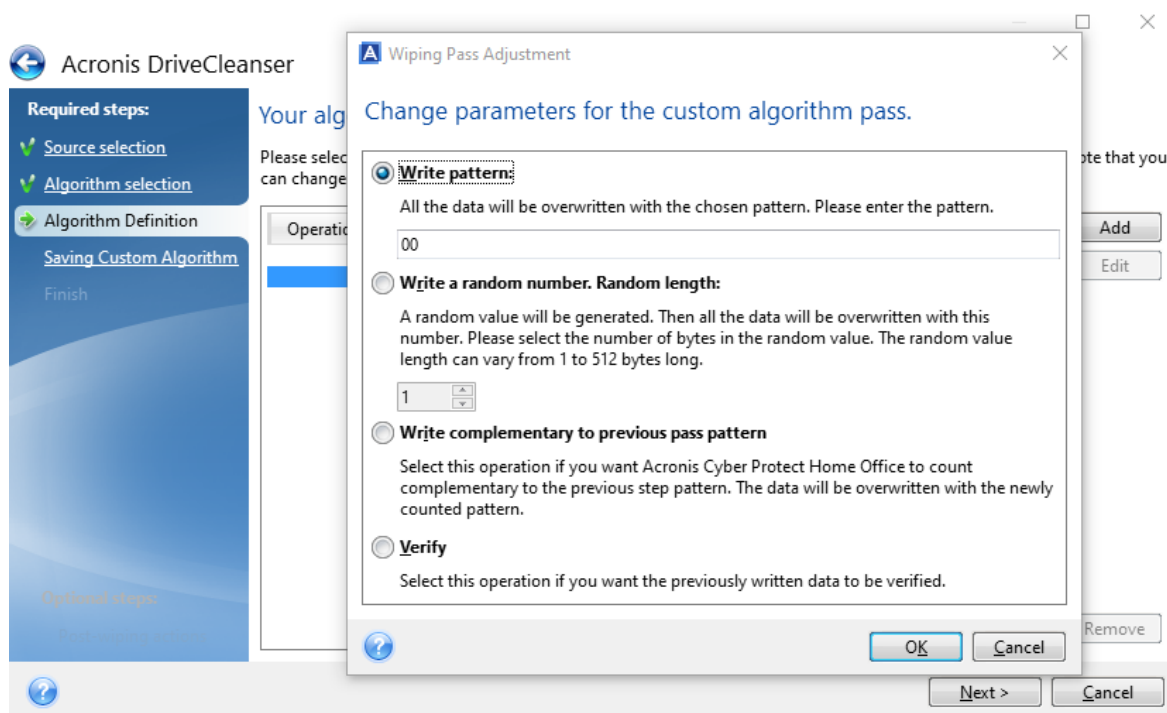
The table has the following legend:

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

- **Verify**

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

3. Click **OK**.

To edit an existing pass

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

The Wiping Pass Adjustment window opens.

Note

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

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

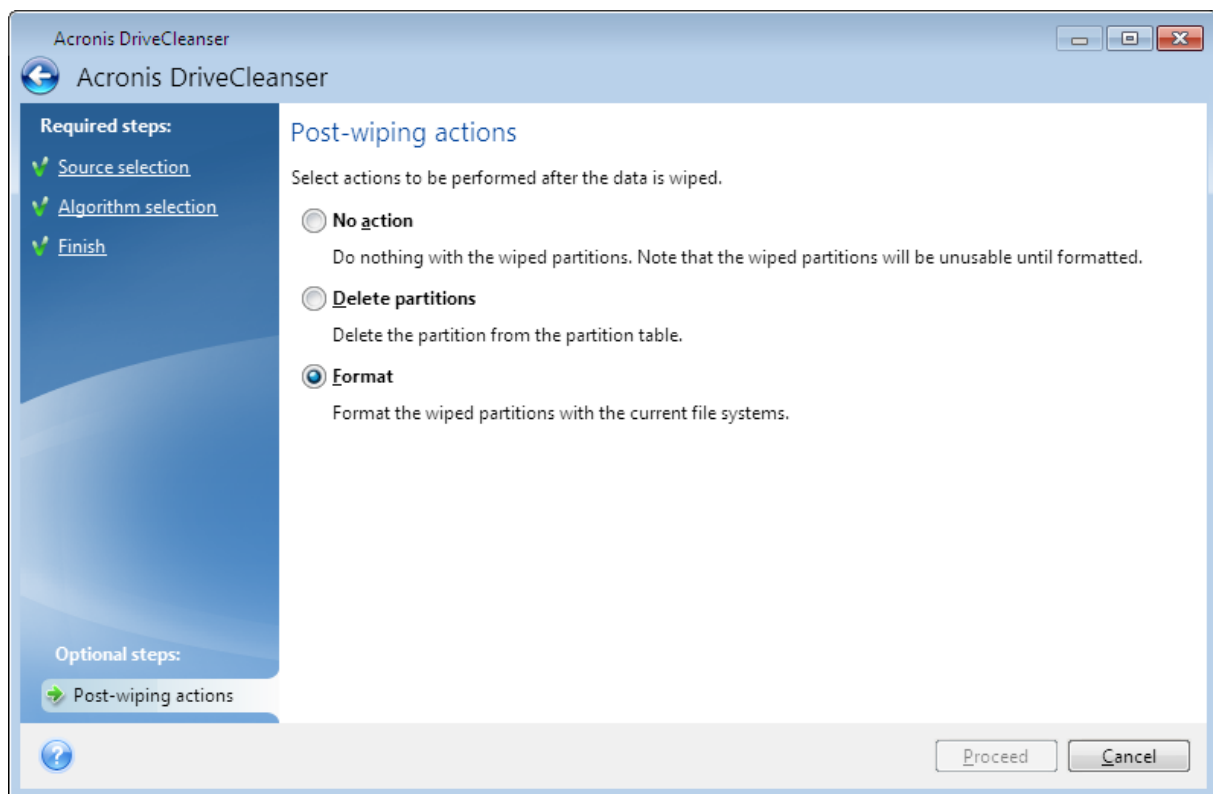
Saving algorithm to a file

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).



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.

It can carry out the following operations:

- Securely destroy data in the **Windows Recycle Bin**.
- Remove **temporary files** from appropriate Windows folders.
- Clean up **hard disk free space** of any traces of information previously stored on it.
- Remove traces of **file and computer searches** on connected disks and computers in the local area network.
- Clean the **recently used documents** list.
- Clean the **Windows Run** list.
- Clean the **opened/saved files** history.
- Clean the list of network places to which the user has connected using **network credentials**.
- Clean the **Windows prefetch directory**, where Windows stores information about programs you have executed and run recently.

Note

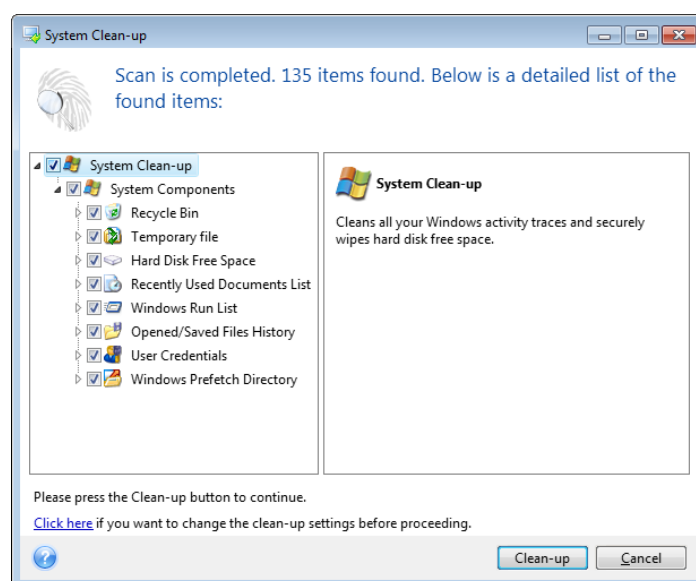
Windows 10 and later operating systems do not store information on file and computer searches. Furthermore, information on opened/saved files is stored differently in the registry, so the wizard shows this information in a different way.

Note

Windows stores passwords until the session ends, so cleaning the list of network user credentials will not take effect until you end the current Windows session by logging out or by rebooting the computer.

To start the System Clean-up wizard, click the **Start** button → **Acronis** (product folder) → **System Clean-up**.

After you start the wizard, it will search for any traces of user actions stored by Windows. When the search is finished, its results will be available at the top of the wizard window.



You can view the search results and manually select the items you wish to remove.

Click the **Click here** hyperlink text to change the clean-up settings before proceeding.

Click **Clean-up** to launch removing the found items.

Clean-up settings

In the clean-up settings window you can change the clean-up settings for every system component. Some of these settings apply to all components.

To change the clean-up settings for a component

- Expand the **System Components** item in the tree and select the component clean-up settings which you need to change. You can enable or disable scanning of the component by the Clean-up wizard. To do this, select or clear the **Enable** check box.

If required, you can also expand a component and customize the desired data destruction method, files to clean, clean-up registry search strings you have used for finding computers in the local network, etc. To do this, click the triangle near the component, select an option from the list and specify the settings.

- After you set the desired components' properties, click **OK** to save your settings. These settings will be used as default next time you launch the Clean-up wizard.

If you have already changed the clean-up settings before, you can always return to the program defaults by clicking the **Restore Defaults** button.

System components:

- Recycle Bin
- Temporary files
- Hard disk free space
- Find Computer list
- Find File list
- Recently Used Documents list
- Windows Run List
- Opened/saved files history
- User Credentials
- Windows Prefetch Directory

Default clean-up options

The default clean-up options are available by clicking the **Click to change this setting...** link on the **Data Destruction Method** option page.

To change the default clean-up options

1. Choose on the tree the component clean-up settings which you need to change.
2. After you change the options, click **OK** to save your settings.

If you have already changed the clean-up settings before, you can always return to the program defaults by clicking the **Restore Defaults** button.

General

By default, the summary dialog window is displayed after each clean-up procedure ends (the **Show summary** check box is selected). If you do not need this window to be displayed, uncheck the box.

Clean-up options

System Clean-up utilizes a number of the most popular data destruction methods. Here, you can select the common data destruction method which will be used by default for all other components.

The data destruction methods are described in detail in [Hard Disk Wiping Methods](#) of this guide.

Specific clean-up options

You can customize the following clean-up options:

- Data destruction method
- Default options
- Files
- Drive free space
- Computers
- Commands
- Network places filter

Data destruction method

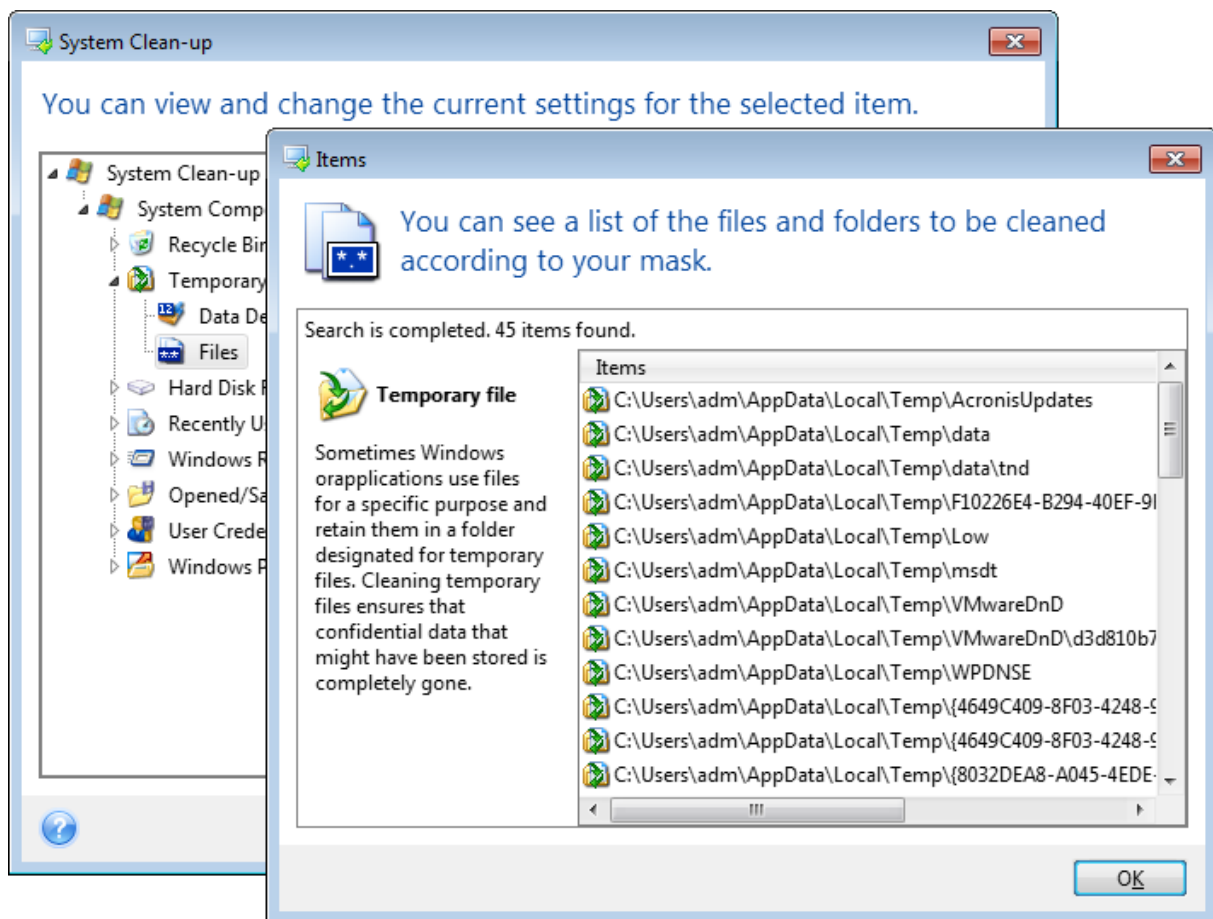
System Clean-up utilizes a number of the most popular data destruction methods. Here, you need to select the desired data destruction method.

- **Use common method** - if you leave this parameter selected, the program will use the default method (the initial setting is Fast method).
If you need another destruction method to be set as a default, click the corresponding link.
- **Use custom method for this component** - selecting this parameter allows you to choose one of the preset data destruction methods from the drop-down list.

The data destruction methods are described in detail in [Hard Disk Wiping Methods](#) of this guide.

Files

The Files setting defines the names of files to clean with System Clean-up wizard and can be used with a search string.



Under the Windows operating system, a search string can represent a full or partial filename. A search string can contain any alphanumeric symbols, including commas and Windows wildcard symbols, and can have values similar to the following:

- *.* – to clean all files with any file names and extensions.
- *.doc – to clean all files with a specific extension – Microsoft document files in this case .
- read*. – to clean all files with any extensions, and names beginning with "read".
- read?.* – to clean all files having five-letter names and any extensions, names beginning with "read"; the fifth letter is random.

The last search string, for example, will result in the removal of read1.txt, ready.doc files, but readiness.txt will remain with its longer name (excluding the extension)

You can enter several different search strings separated by semicolons; for example:

.bak;.tmp;*.~~~ (without spaces between the search strings)

All files with names corresponding to at least one of the search strings will be cleaned.

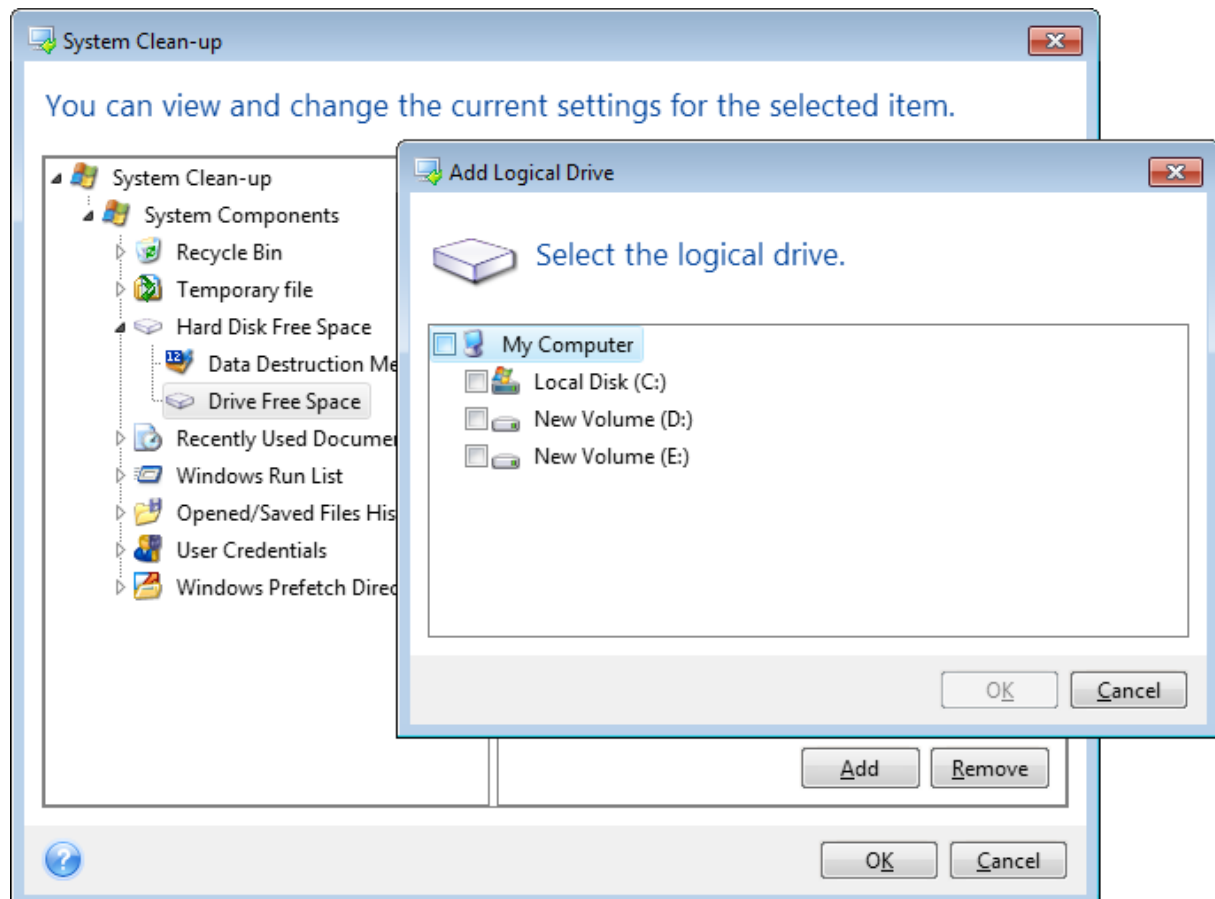
Upon entering the Files setting value, you can browse the files matching the search strings. To do this, click **Show Files**. You will see a window with the names of the found files. These files will be cleaned.

Drive free space

Here you can manually specify physical and/or logical drives to clean up free space on. By default, System Clean-up cleans up free space on all available drives.

If you want to change the settings of this parameter, you can use the **Remove** button to delete from the list the drives you don't need to clean free space on.

If you wish to add these drives to the list again, use the **Add** button.



Computers

The **Computers** setting is used for cleaning up the registry search strings you have used for finding computers in the local network. These strings keep information on what has interested you in the network. These items should also be deleted to maintain confidentiality.

The **Computers** setting is similar to the **Files** setting. It is a string that can contain any number of full or partial computer names separated by semicolons. The deletion of computer search strings is based on a comparison with the **Computers** setting value according to Windows rules.

If you simply need to delete all local network computer search strings (suitable in most cases), just leave the default value of this setting. To restore the default settings:

- Select the **Find Computer List** component
- Make sure the **Enable** check box is selected
- Select the **Computers** setting; make sure its text box is clear.

As a result, all computer search strings will be deleted from the registry.

After entering the **Computers** setting value, you can browse the search strings found by the System Clean-up Wizard in the registry. To do so, click **Show Computers**. You will see the window with full and partial computer names searched for in the network. These items will be deleted.

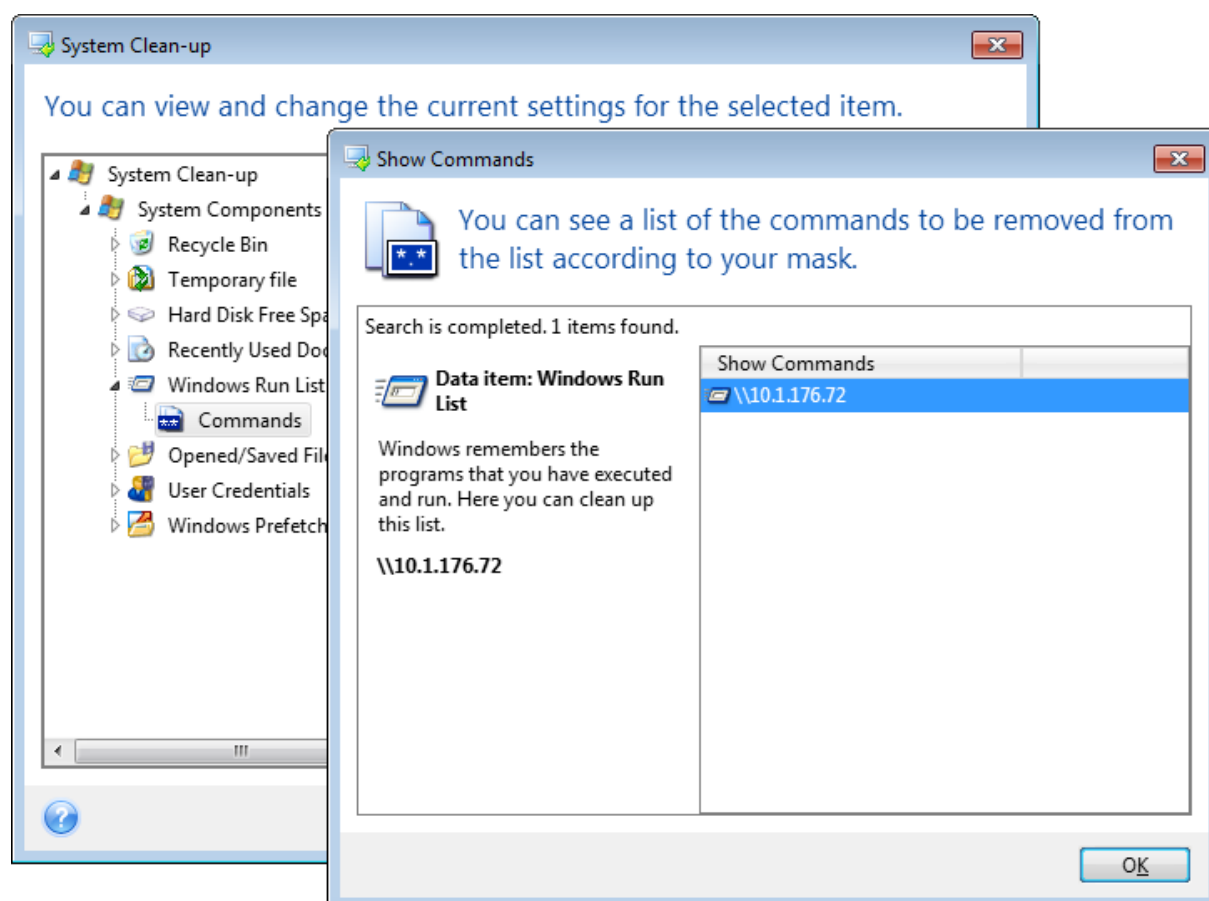
Setting commands

Here you can select the commands to remove during **Windows Run List** clean-up.

This template can contain any command names or their parts separated by semicolons, e.g.:

help; cmd; reg

This will result in removing commands with names corresponding to or containing any of the names or parts of names you entered.



Network places filter

Here you can enter (separated by semicolons) any hostnames or IP addresses of network places, servers, FTP servers, network shares, etc. to which you have made connection by supplying network

credentials (a user name and password). While entering hostnames and IP addresses you can use * and ? wildcards.

Click **Show network places** to view the list of network places that you visited using the credentials you want to delete.

Preview

When the scanning is finished, its results will be available in the upper part of the wizard window. By default, all system components are scanned for clean-up. If you want to customize which of the system components should be scanned and which should not, change the default clean-up settings.

You can view the search results and manually select/unselect the items you wish to clean up/keep. In order to help you make the right choice, all the components are provided with brief descriptions. Just click the component name, and its description displays in the right side of the window.

To select/unselect a component

- Expand the **System Components** item in the System Clean-up tree and make sure that the component you wish to clean up is selected. If you do not want to clean up a component, simply clear its check box.
- If required, you can dig deeper by expanding a component and selecting/unselecting its contents.

Having specified the components for clean-up, click the **Clean-up** button to continue.

Note

Windows 10 and later operating systems do not store information on file and computer searches. Furthermore, information on opened/saved files is stored in the registry differently, so the wizard shows this information in a different way.

Clean-up progress

The operation status window reports about the state of the current operation.

The progress bar indicates the level of completion of the selected operation.

In some cases, the operation may take a long time to be completed. If this is the case, select the **Shutdown the computer after completion** check box. When the operation finishes, Acronis True Image will turn the computer off.

Mounting a backup image

Note

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

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

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

Note

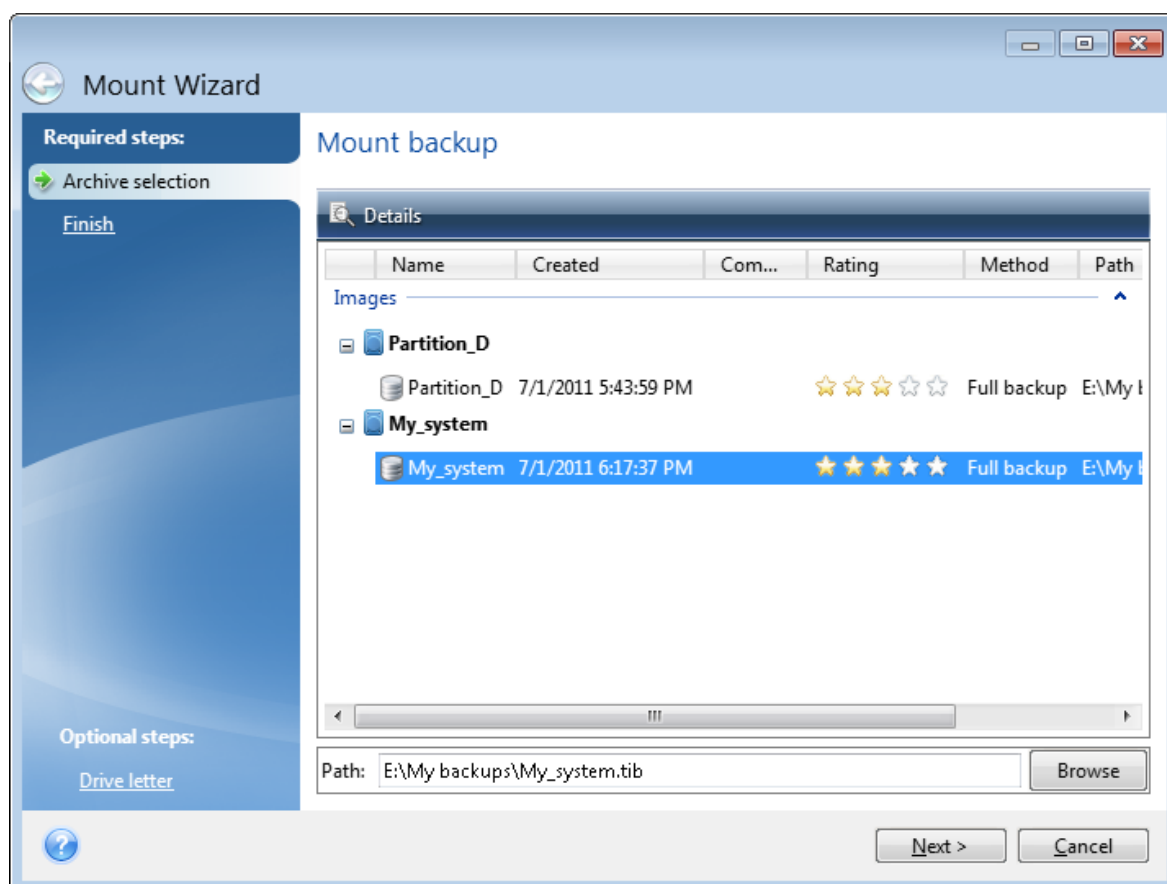
The operations described in this section are supported only for the FAT and NTFS file systems.

Note

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

How to mount an image

1. In File Explorer, right-click the image file that you want to mount, and then click **Mount**.
The Mount wizard opens.
2. Select the backup for mounting by its creation date/time. Thus, you can explore the data state at a certain moment.



3. [optional step] On the **Drive letter** step, select a letter to be assigned to the virtual disk from the **Mount letter** drop-down list. If you do not want to mount a partition, select **Do not mount** in the list or clear the partition's check box.

4. Click **Proceed**.
5. After the image is connected, the program will run File Explorer, showing its contents.

Unmounting an image

We recommend that you unmount the virtual disk after all necessary operations are finished, as maintaining virtual disks takes considerable system resources.

To unmount an image

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

Working with .vhd(x) files

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

How to use .vhd(x) files

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

Limitations and additional information

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

Converting Acronis backup

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

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

1. Start Acronis True Image.
2. Go to the **Backup** section.
3. In the backup list, click the down arrow icon next to the backup that you want to convert, and then click **Convert to VHD**.
If the backup is password-protected, Acronis True Image will ask for it. Note that the resulting .vhd(x) file will lose password protection.
4. Select the backup version that you want to convert.
Converting an incremental backup requires all the previous incremental backups and the original full backup. Converting a differential backup requires the original full backup. The result of conversion is always a full backup.
5. Specify the path to the file to be created.
The file can be directed to any local storage supported by Acronis True Image (except the Acronis Secure Zone and CD/DVD). In addition, it can be directed to an SMB share.
6. [Optional step] While the backup is being converted, you can select the **Start virtual machine after completion** check box. If it is selected, Acronis True Image will restart your computer and run Hyper-V virtual machine by using the created .vhd(x) file.

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

Importing and exporting backup settings

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

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

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

- list of items for backup
- backup options

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

The settings of Nonstop Backup are as follows:

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

Note

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

To export the backup settings

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

To import the backup settings

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

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

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

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.

What problem does it solve?

A system disk image can be restored easily on the hardware where it was created or to identical hardware. However, if you try to do it on a dissimilar hardware, the recovered system will fail to boot. This is because the new hardware is incompatible with critical drivers included in the image. The utility finds and installs drivers for devices that are critical for the operating system start-up, such as storage controllers, motherboard, or chipset.

How do I use it?

Before you start recovery to dissimilar hardware, ensure that you have:

- [Backup of your system disk or Entire PC backup](#)
- [Acronis bootable media](#)
- [Acronis Universal Boot media](#)

Note

If you have Acronis True Image and Acronis Universal Boot Media Builder installed on your computer, you can place both Acronis True Image and Acronis Universal Boot on the same media. See [Creating Acronis Universal Boot media](#) for details.

To recover your system to dissimilar hardware:

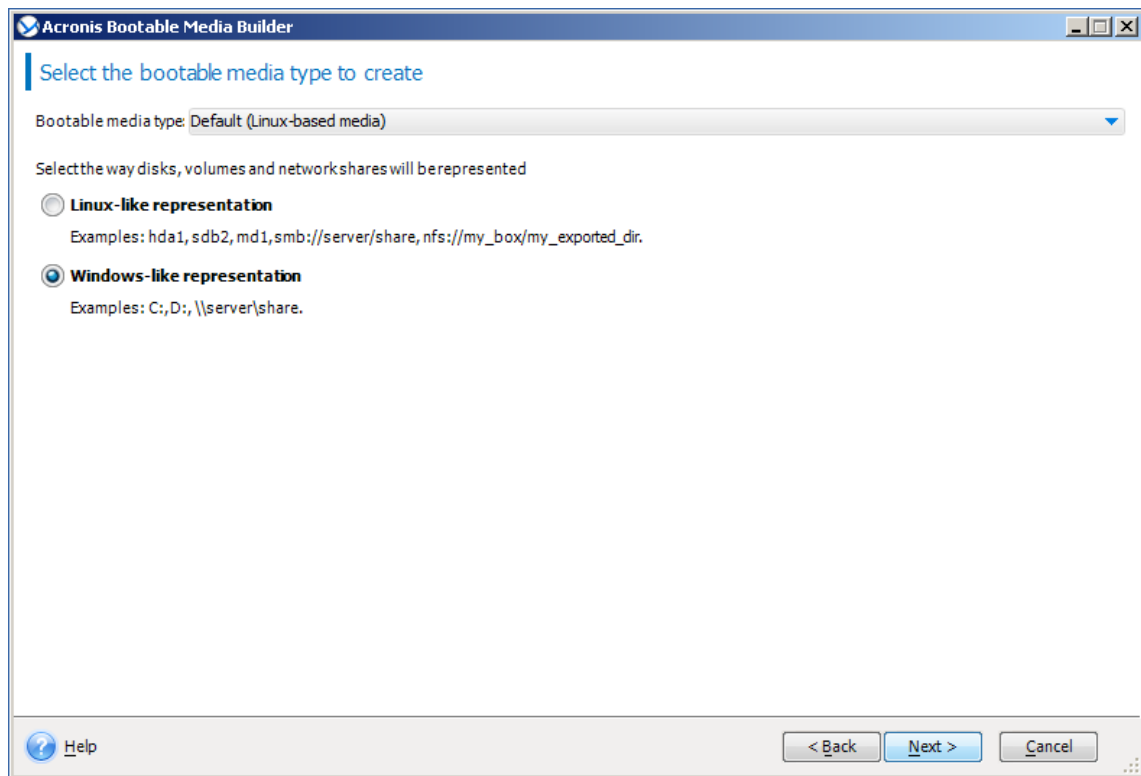
1. Start your target computer by using Acronis bootable media, and then recover your system from your system backup or Entire PC backup. See [Recovering your system to a new disk under bootable media](#) for details.
2. Start your target computer by using Acronis Universal Boot media, and then follow the on-screen instructions to make your system bootable. See [Using Acronis Universal Restore](#) for details.

Creating Acronis Universal Boot media

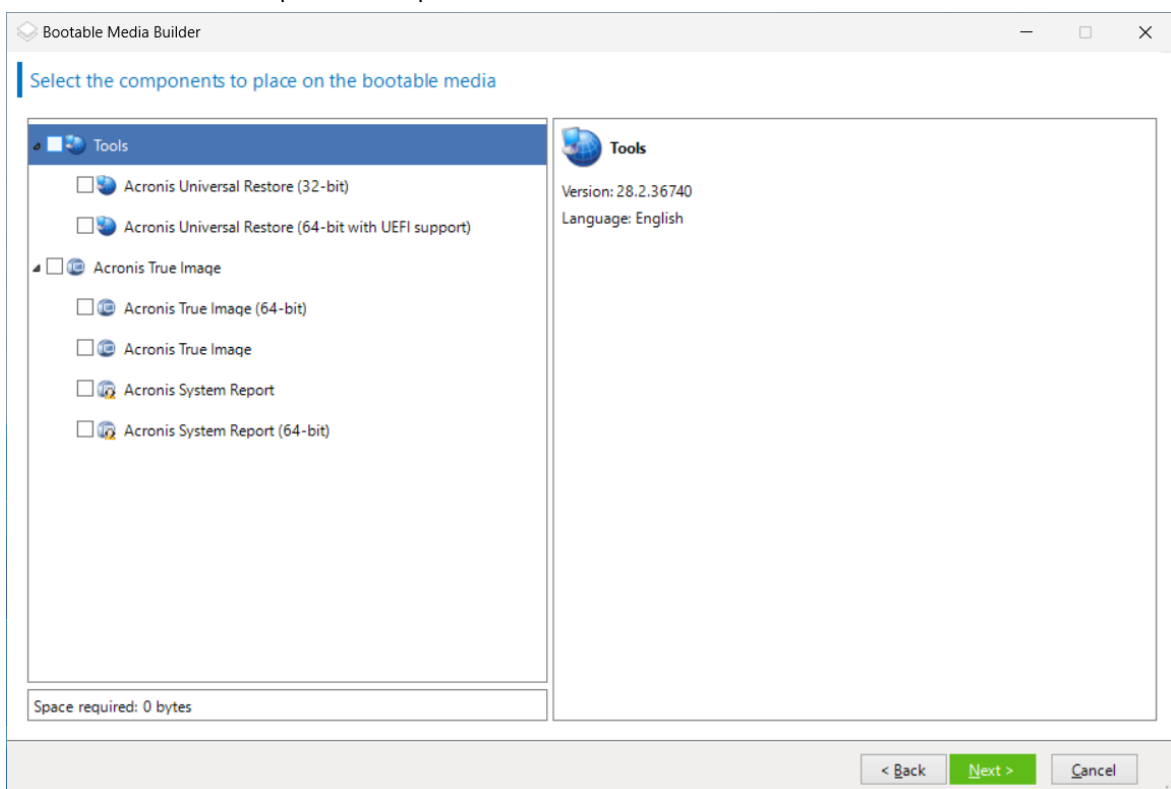
Acronis Universal Boot media is used to make your computer bootable after recovery to dissimilar hardware. See [Acronis Universal Restore](#) for details.

To create Acronis Universal Boot media

1. Start Acronis True Image.
2. In the **Tools** section, click **Acronis Universal Restore**.
3. Click **Download** to obtain Acronis Universal Boot Media Builder.
4. Run the downloaded file and install the media builder.
5. Plug in the USB flash drive or insert blank DVD that you want to make bootable.
6. To start Acronis Universal Boot Media Builder, perform one of the following:
 - In the **Tools** section, click **Acronis Universal Restore**.
 - Click the **Start** button, open the list of installed programs, and then click **Run Universal Boot Media Builder**.
7. Ensure that:
 - Linux-based media is selected as a bootable media type.
 - Windows-like representation is selected as a way the disks and volumes are represented.



8. [Optional] Specify Linux kernel parameters. See [Bootable media startup parameters](#) for details.
9. Select the Acronis components to place on the media.



You can select 32-bit and/or 64-bit components. The 32-bit components can work on 64-bit hardware. However, you need 64-bit components to boot a 64-bit computer that uses Unified Extensible Firmware Interface (UEFI).

To use the media on different types of hardware, select both types of components. When booting a machine from the resulting media, you will be able to select 32-bit or 64-bit components on the boot menu.

If Acronis True Image is installed on your computer, you can place it on the media as well. In this case, you will have a single bootable media containing both components required for recovery to dissimilar hardware.

10. Select a destination for the media:

- **CD**
- **DVD**
- **USB flash drive**
- **ISO image file**

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

When the .iso file is created, you can burn it onto a CD or DVD. For example, in Windows 10 and later, you can do this using a built-in burning tool. In File Explorer, double-click the created ISO image file, and then click **Burn**.

11. Specify the mass storage drivers to be used by Acronis Universal Boot.

You do not have to add the drivers now. You can do this later when you apply Acronis Universal Boot to a computer.

12. Click **Proceed**.

When the media is created, unplug it from your computer. This is your Acronis Universal Boot media.

Using Acronis Universal Restore

Preparation

Note

If you do not see Acronis Universal Restore in the **Tools** tab, the component may not be installed or may be unavailable in your edition. Open **Acronis Universal Restore** in **Tools** and use the **Download** link to get the installer for your operating system.

Note

The downloaded installer and created bootable media may use the operating system language. Installing Universal Restore does not change the language of the main application.

Prepare drivers

Before applying Universal Restore to a Windows operating system, make sure that you have the drivers for the new HDD controller and the chipset. These drivers are critical to start the operating system. Use the CD or DVD supplied by the hardware vendor or download the drivers from the vendor's website. The driver files should have the *.inf, *.sys or *.oem extensions. If you download the drivers in the *.exe, *.cab or *.zip format, extract them using a third-party application.

Check access to the drivers in bootable environment

Make sure you have access to the device with drivers when working under bootable media. Use WinPE-based media if the device is available in Windows but Linux-based media does not detect it.

Universal Restore settings

Automatic driver search

Specify where the program will search for the Hardware Abstraction Layer (HAL), HDD controller driver and network adapter driver(s):

- If the drivers are on a vendor's disc or other removable media, turn on the **Search removable media**.
- If the drivers are located in a networked folder or on the bootable media, specify the path to the folder by clicking **Add folder**.

In addition, Universal Restore will search the Windows default driver storage folder (usually WINDOWS/inf).

Mass storage drivers to install anyway

You need this setting if:

- The hardware has a specific mass storage controller such as RAID (especially NVIDIA RAID) or a fibre channel adapter.
- If the automatic drivers search does not help to boot the system.

Specify the appropriate drivers by clicking **Add driver**. The drivers defined here will be installed, with appropriate warnings, even if the program finds a better driver.

Universal Restore process

After you have specified the required settings, click **OK**.

When the process is complete, you will be able to configure the network connection and specify drivers for the video adapter, USB and other devices.

Troubleshooting

If Acronis True Image 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 installer again. It will detect Acronis True Image 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. You can read the corresponding solutions in the [Acronis Support Portal](#).

- [Signing in at program start fails](#)
- [Error "You've exceeded the maximum number of activations for this serial number"](#)
- [Error "This serial number is already registered to another account"](#)
- [Error "Plug in external drive"](#)
- [A backup to Acronis Cloud fails with error "Write error" or "Error occurred while writing the file" or "FES request failed"](#)
- [Blue Screen of Death \(BSOD\) after recovery to new hardware and error "Stop 0x0000007B" due to missing drivers](#)

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

Acronis System Report

When you contact the Acronis Support team, they will usually need information about your system in order to resolve your problem. Sometimes getting the information is an inconvenient process and may take a long time.

The **Generate System Report** tool 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 is performing any other operation.
- If you use Windows 11, click **All apps > Acronis > Acronis System Report**.
- If you use Windows 10, in the **Start** menu, click **Acronis > Acronis System Report**.

After the report is generated

- To save the generated System Report, click **Save** and in the opened window specify a location for the created file.

- To exit to the main program window without saving the report, click **Cancel**.

You can place the tool on your bootable media as a separate component to generate a System Report when your computer cannot boot. After you boot from the media, you can generate the report without running Acronis True Image. 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 installation folder. To do so, enter:

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

3. To create the System Report file, enter:

```
SystemReport
```

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

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

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

To generate a System Report under bootable media

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

Note

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

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

The program will archive the report into a zip file.

Acronis Smart Error Reporting

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

When you have an internet connection

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

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

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

When you do not have an internet connection

1. In the error message window, click **More details** and write down the event code. The code may look like this:
0x000101F6 - example of an ordinary event code.
0x00970007+0x00970016+0x00970002 - example of a composite event code. A code of this kind may appear when an error occurred in a low-level program module and then propagated to higher-level modules, resulting in errors in those modules as well.
2. When you establish internet connection or if you can use another computer where internet connection is available, enter the event code at [Acronis Smart Error Reporting](#).

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

Sending feedback to Acronis

We frequently improve our products and services by making them more functional, reliable, and fast. Via the feedback form, you can point out inconveniences and defects that we should resolve to make Acronis True Image even better. Please spend a couple of minutes to tell us what you think about our product, suggest a new feature, or report a problem. We do read and analyze all feedback.

Note

We do not reply to all feedback messages. If you need assistance with Acronis True Image, contact the Support team.

To send feedback to Acronis

1. On the sidebar, click **Help**, and then click **Send feedback**. The feedback form opens.

 Send Feedback to the Acronis team 

Share your thoughts about Acronis True Image or report a problem.

Reason

Enter your feedback here

 Attach file...

joh.doe@company.com

Name

☒ Attach system report [What is this?](#)

We cannot reply to all messages sent via this form, but we do read and analyze your feedback.

Send

2. Choose a feedback reason from the list.
3. Type your message.
4. Provide your name and email.
5. [Optional step] You can also attach a file and Acronis System Report. See [Acronis System Report](#) for details.

We recommend that you attach the System Report when you faced a serious error, for example, when Acronis True Image stopped responding.
6. Click **Send**.

How to collect crash dumps

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

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

If Acronis True Image causes a Windows crash

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

If Acronis True Image hangs

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

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

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

Log files

Acronis True Image creates log files for backup, recovery, clone, and other operations. These logs can help in troubleshooting. You can open them with Notepad. The most recent log usually contains the full error message of the failed operation.

The log files are located in:

C:\ProgramData\Acronis\TrueImageHome\Logs

The folders in this location contain the following logs:

- **ti_demon** – ti_demon_GUID_[date-time].log: backup, clone, and recovery operations
- **backup_worker** – backup_worker_[date-time].log: service-level backup operations
- **ti_console** – ti_console.0.log: operations in the product interface
- **ti_media_builder** – ti_media_builder.0.log: Media Builder operations
- **ti_tools** – ti_tools.0.log: tools and utilities operations

Additional logs:

- afcdpsrv.log, NSB_[date-time].log – Nonstop Backup
- installer-[GUID].log – MSI installation log

Log retention rules

Acronis True Image automatically manages the retention of its log files. The retention rules are defined in the product configuration files. Older log files are either compressed or deleted once the limits are exceeded.

Log type	Config file	Max size (per file)	Max files
ti_console	TruelImage.config	10 MB	10
backup_worker	inherited (TruelImage.config / TruelImageHomeService.config)	1 MB	10
ti_demon	TruelImageHomeService.config	1 MB	10
ti_monitor	TruelImageMonitor.config	1 MB	10
pcs	TruelImage.config	1 MB	10
arw-client-rest, ti-rpc-client, ti-licensing, ti-notifications, ti-analytics	TruelImage.config	1 MB	3

The parameters `maxsize` (in bytes) and `maxfiles` are defined in the respective configuration files. For example, a setting of `maxsize="1048576"` means a maximum of 1 MB per file, and `maxfiles="10"` means up to 10 files are kept. Older logs are either compressed or removed automatically.

Firewall settings

Acronis True Image requires certain ports to be open for proper operation. The table below lists the ports, their direction, and purpose.

Port	Direction	Purpose
58101 (TCP)	Inbound	Tray Notification Center communication
8099 (TCP)	Outbound	Policy application
8890 (TCP)	Outbound	Quarantine communication
30630 (TCP)	Inbound	Alert Manager Service
9772 (TCP)	Outbound	Malware detection, quarantine management, database updates
58091 (TCP)	Inbound	Online Dashboard and cloud registration

Port	Direction	Purpose
9999 (TCP)	Outbound	Authorization and routing
6110 (TCP)	Inbound	Anti-malware protection
6888 (TCP, builds prior to Acronis Cyber Protect Home Office 2024 Update 1)	Outbound	Legacy update communication
Cloud and additional connectivity		
443, 80 (TCP)	Outbound	Cloud and license communication
44445, 55556 (TCP)	Outbound	Cloud login, activation, service communication
58085, 58081 (TCP)	Inbound	Local mobile backup
20, 21 (TCP and UDP)	Outbound	Used when backing up to an FTP server

Note

Dynamic ports in the range 49152–65535 are also used by the operating system for tasks such as on-demand scans, vulnerability assessment, and database updates. These ports are managed by Windows automatically.

For the most up-to-date list of required ports and troubleshooting steps, see the Knowledge Base article: [Firewall settings for Acronis products](#).

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.

Acronis Drive

A virtual drive that contains both local and cloud archives. The drive is accessible in File Explorer under Favorites and provides access to the archived files, in read-only mode.

Acronis Notary

A technology that allows user to check if a notarized file was modified since the time it was backed up. Notary calculates a hash code based on hash codes of the files selected for notarization, and then sends the hash code to a Blockchain-based database. The Blockchain technology guarantees that the hash code will not be changed. Therefore, the file authenticity can easily be verified by comparing the hash in the database and the hash of the file that you want to check.

Acronis Secure Zone

A secure partition for storing backups on a hard disk. Advantages: enables recovery of a disk to the same disk where the disk's backup resides offers a cost-effective and handy method for protecting data from software malfunction, virus attack, operator error eliminates the need for a separate media or network connection to back up or recover the data Limitations: 1) The Acronis Secure Zone cannot be created on a dynamic disk. 2) The Acronis Secure Zone is not available as a location for backups in the recovery environment when you start from bootable media, through Startup Recovery Manager or BartPE.

Acronis Startup Recovery Manager

A protection tool that allows to start standalone version of at boot time when F11 is pressed. Startup Recovery Manager eliminates the need for bootable media. Startup Recovery Manager is especially useful for mobile users. If a failure occurs, the user reboots the machine, hits F11 on prompt "Press F11 for Startup Recovery Manager..." and performs data recovery in the same way as with ordinary bootable media. Limitations: cannot be organized on a dynamic disk; requires manual configuration of boot loaders, such as LILO and GRUB; requires re-activation of third-party loaders.

Archive

A file created as a result of an archiving operation. The file includes a set of compressed files that a user selects for archiving. Archives can be stored in Cloud or local storage, such as an external hard drive or

NAS, and they are accessible in read-only mode on a virtual Acronis Drive.

Archiving operation

An operation that compresses files that you select and moves them to Cloud or local storage, such as an external hard drive or NAS. The main purpose of the operation is to free up space on a hard drive by moving old or large files to different storage. After completion, the files are deleted from their original locations and accessible in read-only mode on a virtual Acronis Drive.

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 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. 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

Data synchronization

Data synchronization is a process of keeping data identical in two or more synchronized folders. These folders may be located on the same computer or on different computers connected via a local network or via the Internet. When you create, copy, modify or

delete a file or a subfolder in your sync folder, the same action is automatically done in the other sync folders. And vice versa - when something changes in the other sync folders, the same change is done in your folder.

Differential backup

A backup method used for saving data changes that occurred since the last full backup version within a backup. A backup process that creates a differential backup version.

Differential backup version

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

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.

I

Incremental backup

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

Incremental backup version

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

M

Mobile backup

A backup that contains files from a mobile device, such as a smartphone or tablet.

N

Nonstop backup

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

Nonstop protection

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

Notarization

A process of "remembering" a file state and defining this state as authentic. During notarization, Acronis Notary calculates a hash code based on hash codes of the files selected for notarization, and then sends the hash code to a Blockchain-based database.

Notarized backup

A backup that contains files notarized with Acronis Notary.

Notarized file

A file that was notarized with Acronis Notary. A file becomes notarized after adding it to a notarized backup and sending its hash code to a Blockchain-based database.

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.

Version of synced file

A state of a file which is located in a sync folder after each modification of this file. File versions may be stored on Acronis Cloud.

Index

1

1. Entire PC backup “Two full versions” 82

2

2. File backup “Daily incremental version + weekly full version” 82

3

3. Disk backup “Full version every 2 months + differential version twice a month” 83

32-bit or 64-bit components 92

A

About recovery of dynamic/GPT disks and volumes 139

Accessing your archived files 185

Acronis account 32

Acronis ASign 109

Acronis bootable media startup parameters 206

Acronis Cloud Backup Download 202

Acronis Cloud during trial 40

Acronis DriveCleanser 232

Acronis Media Builder 203

Acronis Mobile 71

Acronis Nonstop Backup 56

Acronis Nonstop Backup data storage 57

Acronis patented technologies 9

Acronis Secure Zone 222

Acronis Secure Zone cleanup 223

Acronis Secure Zone location 224

Acronis Secure Zone protection 226

Acronis Smart Error Reporting 255

Acronis Startup Recovery Manager 215

Acronis System Report 253

Acronis Universal Restore 125, 248

Activating a subscription 42

Activating Acronis True Image 15

Active protection 167

Adding a new device to Online Dashboard 159

Adding a new hard disk 227

Adding an existing backup to the list 105

Adding drivers to an existing .wim image 207

Additional information 216

Advanced settings 75

Algorithm definition 235

Algorithm selection 233

Anti-ransomware protection 167

Antivirus scans 172

Application settings 15

Archiving data 181

Archiving your data 183

Arranging boot order in BIOS or UEFI BIOS 142

Authentication settings 55

Auto-renewal of subscription 44

Automatic driver search 252

Automatic patch installation 176

Available licenses 38

B

- Backing up all data on your PC 23
- Backing up BitLocker-encrypted drives 61
- Backing up data 65
- Backing up data remotely 160
- Backing up disks and partitions 65
- Backing up disks and partitions using bootable media 68
- Backing up files and folders 68
- Backing up Microsoft 365 data 72-73
- Backing up mobile devices 70
- Backing up your computer 20
- Backing up your files 27
- Backup activity and statistics 100
- Backup file naming 59
- Backup operations 97
- Backup options 74
- Backup protection 87
- Backup schemes 77
- Backup size metrics (.tib archives, legacy) 101
- Backup size metrics (.tibx archives, current format) 102
- Backup splitting 90
- Backup to various places 104
- Backup validation option 90
- Backups created before Acronis True Image 2020 10
- Basic concepts 47
- Before you start 29
- BIOS-booted system, GPT, no Windows 136, 195

- BIOS-booted system, GPT, UEFI supported 135, 195

- BIOS-booted system, MBR, no Windows 134, 194

- BIOS-booted system, MBR, UEFI not supported 134, 193

- BIOS-booted system, MBR, UEFI supported 134, 193

- Built-in store 18

C

- Causes of possible discrepancies in sizes 102

- Changed Block Tracker (CBT) 52

- Changing billing information 46

- Check access to the drivers in bootable environment 252

- Clean-up options 240

- Clean-up progress 244

- Clean-up settings 239

- Cleaning up backups manually 112

- Cleaning up backups, backup versions, and replicas 111

- Cleaning up space on Acronis Cloud 163

- Cleanup rules for backup replicas 111

- Cleanup rules for backups 111

- Clone Disk wizard 188

- Cloning a disk 29

- Cloning BitLocker-encrypted drives 62

- Cloning your hard drive 28

- Cloud archiving vs. Online backup 182

- Compatibility with Microsoft BitLocker encryption feature 61

- Compression level 94

Computer restart 154
Computer shutdown 94
Computers 242
Configuring Active Protection 169
Configuring Antivirus scans 173
Configuring Protection exclusions 178
Converting Acronis backup 247
Copyright statement 9
Creating Acronis bootable media 22, 204
Creating Acronis Universal Boot media 249
Creating an .iso file from a .wim file 208
Creating an Acronis Survival Kit 24
Creating and managing Acronis Secure Zone 223
Creating custom algorithms 235
Creating new partitions 229
Custom schemes 80

D

Daily backup parameters 76
Data archiving options 184
Data center 184
Data destruction method 240
Deactivating a subscription 42
Deciding where to store your backups 53
Default clean-up options 239
Deleting an entire backup 163
Deleting backups and replicas 110
Deleting the versions of a backup replica to cloud 164
Deleting the versions of a backup to cloud 164
Differential method 51

Disk cloning and migration 187
Disk cloning utility 187
Disk recovery from Cloud 143
Disk recovery mode 152
Downloading Protection updates 179
Drive free space 242

E

Edit user command for backup 89
Edit user command for recovery 153
Email notification 84, 157
Email notifications 161
Encryption 184
Error handling 92
Error handling for Cloud backups and replicas 93
Example of recovery to a UEFI system 140
Examples of custom schemes 82
Excluding items from backup 85
Excluding items from cloning 191

F

FAQ about backup, recovery and cloning 63
File-level security settings for backup 93
File recovery 222
File recovery options 154
File System 230
Files 240
Firewall settings 258
Free disk space threshold 84, 156
FTP connection 54
Full method 50

Full, incremental and differential backups 50

G

General 240

General limitations 40

Getting started 20

Getting started with Acronis Cloud 35

H

Hard Disk Wiping methods 234

How Acronis True Image uses the Blockchain technology 107

How do I use it? 249

How it works 56, 143

How to clear the backup log 101

How to collect crash dumps 257

How to enable UEFI in BIOS? 129

How to get access to a password-protected backup 88

How to migrate an original system to a larger hard drive? 129

How to mount an image 245

How to use .vhd(x) files 246

How to use Acronis DriveCleanser 232

How to use the default exclusion settings 85

How Try&Decide works after a computer restart 217

How we ensure security of your data 36

I

Identity protection 171

Image creation mode 87

Importing and exporting backup settings 247

Incremental method 50

Installing Acronis True Image 14

Integrated anti-malware and privacy features 39

Integration with Windows 60

Introduction 10

L

Laptop power settings 96

Licensing 38

Limitations and additional information 246

Limitations in using Try&Decide 218

Limitations on operations with dynamic disks 13

Local destination of mobile backups 72

Log files 257

Log retention rules 258

M

Making sure that your bootable media can be used when needed 209

Management features 40

Managing custom backup schemes 81

Managing detected issues 177

Managing files in Quarantine 178

Managing your subscription licenses manually 16

Manual partitioning 189

Manual patch installation 176

Manual verification of a file's authenticity 109

Mass storage drivers to install anyway 252

Migrating to an SSD or NVMe drive using the backup and recovery method 200

Migrating your system from an HDD to an SSD
or NVMe drive 199

Migration method 133, 193

Minimum system requirements 11

Monthly backup parameters 76

Mounting a backup image 244

N

Naming convention for backup files created
before Acronis True Image 2020 (.tib) 59

Naming convention for backup files created in
Acronis True Image 59

Network places filter 243

Nonstop Backup - Frequently asked
questions 58

Nonstop Backup limitations 56

Notarized backup 105

Notifications 221

Notifications for backup operation 83

Notifications for recovery operation 156

O

One-time cleanup 165

Online backup protection 88

Online Dashboard and Acronis Cloud 159

Operation priority 95, 156

Operations with backups 97

Other common activation problems 44

Other requirements 11

Overview 61

Overwrite file options 155

P

Partition label 231

Partition layouts 130

Partition letter 231

Partition properties 127

Partition settings 230

Partition style after recovery 140

Partition type (these settings are available only
for MBR disks) 231

Patch management 175

Performance of backup operation 94

Performance of recovery operation 155

Post-wiping actions 237

Pre/Post commands for backup 89

Pre/Post commands for recovery 152

Preparation 251

Prepare drivers 251

Preparing a new disk for backup 54

Preparing for recovery 114

Preview 244

Protected partitions 220

Protecting your system 20

Protection 166

Protection of replicated data 162

Purchasing a subscription 41

Purchasing a subscription to the full version 41

Purchasing and activating a subscription 41

R

Real-time Protection 168

- Recommendations 62
- Recovering data 114
- Recovering data with Online Dashboard 161
- Recovering disks and partitions 114
- Recovering files and folders 148
- Recovering Microsoft 365 data 151
- Recovering partitions and disks 126
- Recovering your computer 30
- Recovering your system after a crash 114
- Recovering your system from Acronis Cloud 144
- Recovering your system to a new disk under bootable media 119
- Recovering your system to the same disk 115
- Recovery of basic volumes and disks 140
- Recovery of dynamic volumes 139
- Recovery options 152
- Reliable data protection
 - backup, cloning, and recovery features 38
- Removable media settings 91
- Removing Acronis Secure Zone 227
- Removing data from Acronis Cloud 163
- Replicating backups to Acronis Cloud 162
- Replication activation 162
- Resolving the most frequent issues 253
- Restoring BitLocker-encrypted drives 61
- Retention rules 57

S

- Saving algorithm to a file 237
- Scheduling 74
- Searching backup content 150

- Security and Privacy Tools 232
- Selecting a data center for backup 96
- Selecting a hard disk 227
- Selecting initialization method 228
- Selecting video mode when booting from the bootable media 213
- Sending feedback to Acronis 255
- Setting commands 243
- Sharing data 186
- Signing a file 109
- Single version scheme 78
- Size 230
- Size of Acronis Secure Zone 225
- Snapshot for backup 95
- Software evaluation 221
- Sorting backups in the list 103
- Source selection 232
- Specific clean-up options 240
- Splitting backups on the fly 105
- Storage for virtual changes 221
- Subscription information 36
- Supported file systems 12
- Supported internet connection types 12
- Supported operating systems 11
- Supported storage media 13
- System Clean-up 237
- System recovery with BitLocker 62
- System requirements and supported media 11

T

- Table 1. Destination disk is larger than 2 TB 130

Table 2. Destination disk is less than 2 TB 132

Target drive size 199

Technical Support 19

The Activity tab 100

The Backup tab 102

The difference between file backups and disk/partition images 48

The Protection dashboard 166

Too many activations 43

Too many activations issue 16

Tools 202

Transferring your subscription to a new computer 43

Transferring your subscription to another account 43

Trial version features and limitations 40

Troubleshooting 55, 253

Troubleshooting activation issues 43

Troubleshooting patch installation 177

Try&Decide 217

 typical use cases 221

Try&Decide options and notifications 220

Trying to determine the crash cause 114

Two-factor authentication (2FA) 33

U

UEFI-booted system, GPT, no Windows 139, 198

UEFI-booted system, GPT, UEFI supported 138, 198

UEFI-booted system, MBR, no Windows 137, 197

UEFI-booted system, MBR, UEFI not supported 136, 196

UEFI-booted system, MBR, UEFI supported 137, 196

Unified Extensible Firmware Interface (UEFI) 128

Uninstalling 18

Universal Restore process 252

Universal Restore settings 252

Unmounting an image 246

Updating the product to the latest version 45

Upgrading Acronis True Image 16

Upgrading your license 45

Upon event execution parameters 76

User interface language 20

Using Acronis Universal Restore 251

Using Blockchain technology 107

Using Try&Decide 219

Using WinPE- or WinRE-based bootable media 23

V

Validating backups 103

Validation option 153

Verifying file authenticity 108

Version chain scheme 79

Videoconference app protection 179

Viewing patch installation results 177

Vulnerability assessment 174

W

Web filtering 169

Web privacy 222

Weekly backup parameters 76

What if recovery has been interrupted 144

What is Acronis ASign? 109

What is Acronis True Image? 10

What is Blockchain? 107

What is data archiving? 181

What is excluded from archives? 182

What is Online Dashboard? 159

What is UEFI? 128

What items can be recovered? 151

What problem does it solve? 248

What to do if Acronis True Image does not
recognize your SSD or NVMe drive 199

What you can exclude and how 86

What you can view and analyze 101

When no information about the file content is
shown 102

When the recovery is complete 125

When Try&Decide can help 217

When you do not have an internet
connection 255

When you have an internet connection 255

Which migration method to choose 199

Why back up Microsoft 365 data? 72

Why do I need it? 28, 232

Why replicate? 162

Why UEFI? 129

Wi-Fi networks for backup to Acronis Cloud 97

Wizards 62

Working with .vhd(x) files 246