



Acronis® True Image™ 2015

Table of contents

1	Introduction	6
1.1	What is Acronis® True Image™ 2015?	6
1.2	New in this version	6
1.3	System requirements and supported media	7
1.3.1	Minimum system requirements	7
1.3.2	Supported operating systems	7
1.3.3	Supported file systems	8
1.3.4	Supported Internet connection types	8
1.3.5	Supported storage media	8
1.4	Installing Acronis True Image 2015	9
1.5	Activating Acronis True Image 2015	10
1.6	Trial version information	11
1.7	Upgrading Acronis True Image 2015	12
1.8	Technical Support	13
2	Getting started	14
2.1	Protecting your system	14
2.1.1	Step 1. Backing up your system disk	14
2.1.2	Step 2. Creating bootable rescue media	15
2.2	Backing up all data on your PC	16
2.3	Backing up your files	16
2.4	Cloning your hard drive	17
2.5	Recovering your computer	18
2.6	Recovering your files and folders	19
2.7	Getting started with Acronis Cloud	20
2.7.1	Subscription information	20
3	Basic concepts	22
3.1	Basic concepts	22
3.2	The difference between file backups and disk/partition images	23
3.3	Full, incremental and differential backups	24
3.4	FAQ about backup, recovery and cloning	26
3.5	Deciding where to store your backups	28
3.5.1	FTP connection	29
3.5.2	Authentication settings	29
3.6	Using Acronis Nonstop Backup	29
3.6.1	Acronis Nonstop Backup data storage	30
3.6.2	Nonstop Backup - Frequently asked questions	31
3.7	Backup file naming	32
3.8	Integration with Windows	32
3.9	Wizards	33

4	Backing up data	35
4.1	Backing up disks and partitions	35
4.2	Backing up files and folders	36
4.3	Backup options	37
4.3.1	Scheduling.....	39
4.3.2	Backup schemes	41
4.3.3	Notifications for backup operation	46
4.3.4	Excluding items from backup	47
4.3.5	Image creation mode.....	49
4.3.6	Backup protection	49
4.3.7	Pre/Post commands for backup.....	50
4.3.8	Backup splitting	50
4.3.9	Backup validation option	51
4.3.10	Backup reserve copy	51
4.3.11	Removable media settings	52
4.3.12	Backup comment	52
4.3.13	Error handling	52
4.3.14	File-level security settings for backup.....	53
4.3.15	Computer shutdown	54
4.3.16	Acronis Cloud cleanup	54
4.3.17	Encryption key	54
4.3.18	Performance of backup operation.....	55
4.4	Operations with backups	56
4.4.1	Backup operations menu.....	56
4.4.2	Backup list operations.....	57
4.4.3	Validating backups	57
4.4.4	Backup to various places	58
4.4.5	Adding an existing backup to the list	58
4.4.6	Backing up to Acronis Cloud from several computers	59
4.4.7	Removing data from Acronis Cloud	59
5	Recovering data	61
5.1	Recovering disks and partitions	61
5.1.1	Recovering your system after a crash.....	61
5.1.2	Recovering partitions and disks	68
5.1.3	About recovery of dynamic/GPT disks and volumes.....	72
5.1.4	Arranging boot order in BIOS	74
5.2	Recovering files and folders.....	75
5.3	Recovery from Acronis Cloud	76
5.3.1	Recovering data from online backups	77
5.3.2	Selecting a version to recover	77
5.3.3	Disk recovery from Cloud	78
5.4	Recovery options	81
5.4.1	Disk recovery mode	82
5.4.2	Pre/Post commands for recovery	82
5.4.3	Validation option	82
5.4.4	Computer restart.....	83
5.4.5	File recovery options.....	83
5.4.6	Overwrite file options	83
5.4.7	Performance of recovery operation	84
5.4.8	Notifications for recovery operation	84
5.5	Restoring computer to factory settings.....	85

6	Synchronizing data.....	88
6.1	About the Sync feature.....	88
6.2	How we ensure security of your data.....	88
6.3	What you can and cannot synchronize.....	88
6.4	Sync icons.....	89
6.5	Sync creation.....	90
6.5.1	Default sync.....	90
6.6	What is True Image for mobile devices?.....	91
6.6.1	How to install True Image app on your mobile device.....	92
6.6.2	Synchronizing a mobile device.....	92
6.7	Versions of synchronized files.....	92
6.7.1	Reverting to a previous file version.....	93
6.8	How to clean up your space on Acronis Cloud.....	93
6.9	How to recover a deleted file.....	94
6.10	How to unlink a device from your account.....	95
7	Disk cloning and migration.....	97
7.1	Disk cloning utility.....	97
7.1.1	Clone Disk wizard.....	97
7.1.2	Manual partitioning.....	100
7.1.3	Excluding items from cloning.....	101
7.2	Migrating your system from an HDD to an SSD.....	102
7.2.1	Preparing for migration.....	102
7.2.2	Migrating to SSD using the backup and recovery method.....	104
8	Tools and utilities.....	105
8.1	Creating bootable rescue media.....	105
8.1.1	Acronis Media Builder.....	106
8.1.2	Making sure that your rescue media can be used when needed.....	110
8.1.3	Creating factory bootable media.....	115
8.2	Acronis Startup Recovery Manager.....	115
8.3	Working with Acronis Secure Zone.....	116
8.3.1	Acronis Secure Zone.....	117
8.3.2	Creating and managing Acronis Secure Zone.....	117
8.3.3	Acronis Secure Zone location.....	118
8.3.4	Size of Acronis Secure Zone.....	119
8.3.5	Acronis Secure Zone protection.....	119
8.3.6	Removing Acronis Secure Zone.....	120
8.4	Adding a new hard disk.....	120
8.4.1	Selecting a hard disk.....	121
8.4.2	Selecting initialization method.....	122
8.4.3	Creating new partitions.....	122
8.5	Security and Privacy Tools.....	124
8.5.1	Acronis DriveCleanser.....	124
8.5.2	System Clean-up.....	128
8.5.3	Hard Disk Wiping methods.....	134
8.6	Mounting an image.....	135
8.7	Unmounting an image.....	136

9	Troubleshooting	137
9.1	Acronis System Report.....	137
9.2	Acronis Smart Error Reporting.....	138
9.3	How to collect crash dumps	139
9.4	Creating a custom rescue CD	139
9.5	Acronis Customer Experience Program	140
10	Glossary of Terms	142

1 Introduction

In this section

What is Acronis® True Image™ 2015?	6
New in this version.....	6
System requirements and supported media	7
Installing Acronis True Image 2015.....	9
Activating Acronis True Image 2015	10
Trial version information.....	11
Upgrading Acronis True Image 2015.....	12
Technical Support	13

1.1 What is Acronis® True Image™ 2015?

Acronis True Image 2015 is an integrated software suite that ensures the security of all of the information on your PC. It can back up your documents, photos, email, and selected partitions, and even the entire disk drive, including operating system, applications, settings, and all of your data.

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.

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

Key features:

- Disk backup to a local storage and to Acronis Cloud
- File backup to a local storage and to Acronis Cloud
- Rescue bootable media
- Hard disk cloning
- File synchronization
- Security and privacy tools

1.2 New in this version

- **Completely new design**—The design and usability of Acronis True Image 2015 were completely reworked to improve and simplify the user experience. Moreover, the new interface allows you to work with True Image on touch screens.
- **Disk recovery from Acronis Cloud via Wi-Fi**—When you recover a disk from Acronis Cloud and you cannot use an Ethernet cable, you can connect and download your data by using a Wi-Fi connection. Acronis True Image 2015 supports several wireless security protocols, including WPA-Personal, WPA2-Personal, and WPA2-Enterprise. You can even wirelessly migrate your operating system with all the installed programs to a bare-metal computer.
- **Automatic deduplication of online backup source data**—Before you start an online backup, True Image analyzes the data that you selected. If there are two or more identical data blocks, only one of them will be uploaded to Acronis Cloud. During recovery, True Image will duplicate the block and insert it to all places where it was originally detected. This algorithm decreases the amount of uploaded data by 10 percent on average and saves your free space on Acronis Cloud.

- **The Standard product version includes the Premium version functionality**—When you buy Acronis True Image 2015, you obtain the full feature set, including dynamic disk support and Acronis WinPE ISO builder.
- **New simplified Acronis Media Builder**—The new wizard allows you to create both Acronis bootable media and WinPE-based media in a few simple steps.
- **Entire PC backup**—With the new Entire PC backup type, you can protect all data stored on your computer at once. In case of disaster, you will be able to recover Windows and applications, in addition to all your documents, photos, and other files.
- **Rarely used tools were removed**—To lighten the product and to make it more reliable, the following tools were removed:
 - Acronis Extended Capacity Manager
 - Trim SSD
 - Backup file conversion from the .tib format to .vhd, and vice versa
 - Disk Editor
 - Boot Sequence Manager
 - File Shredder
 - Import and export of backup settings
 - Try&Decide
 - Mail backup

1.3 System requirements and supported media

1.3.1 Minimum system requirements

Acronis True Image 2015 requires the following hardware:

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

1.3.2 Supported operating systems

Acronis True Image 2015 has been tested on the following operating systems:

- Windows XP SP3
- Windows XP Professional x64 Edition SP2
- Windows Vista SP2 (all editions)
- Windows 7 SP1 (all editions)
- Windows 8 (all editions)
- Windows 8.1 (all editions)
- Windows Home Server 2011

Acronis True Image 2015 also lets you create a bootable CD-R/DVD-R that can back up and recover a disk/partition on a computer running any Intel- or AMD- based PC operating system, including Linux®. (Note that the Intel-based Apple Macintosh is not supported.)

1.3.3 Supported file systems

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

If a file system is not supported or is corrupted, Acronis True Image 2015 can copy data using a sector-by-sector approach.

** The Ext2/Ext3/Ext4, ReiserFS, and Linux SWAP file systems are supported only for disk or partition backup/recovery operations. You cannot use Acronis True Image 2015 for file-level operations with these file systems (file backup, recovery, search, as well as image mounting and file recovering from images). You also cannot perform backups to disks or partitions with these file systems.*

ReiserFS partitions and disks cannot be backed up to Acronis Cloud.

1.3.4 Supported Internet connection types

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

	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	+	- **	-	-	-

* - You can activate the product by using an activation code. Refer to the **Activation from another computer** section in Activating Acronis True Image 2015 (p. 10) for details.

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

1.3.5 Supported storage media

- Hard disk drives*

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

* Limitations on operations with dynamic and GPT disks:

- Creation of Acronis Secure Zone on dynamic disks is not supported.
- Recovery of a dynamic volume as a dynamic volume with manual resizing is not supported.
- "Clone disk" operation is not supported for dynamic disks.

** An FTP server must allow passive mode file transfers. For data to be recovered directly from an FTP server, the backup must consist of files no greater than 2GB each.

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

1.4 Installing Acronis True Image 2015

Installing Acronis True Image 2015

To install Acronis True Image 2015:

1. Run the setup file. Before starting the setup process, Acronis True Image 2015 will check for a newer build on the website. If there is one, the newer version will be offered for installation.
2. Read:
 - The terms of the license agreement.
 - The participation terms of the Acronis Customer Experience Program.
3. If you accept the terms of both documents, click **Install**.
4. When the installation is complete, click **Start application**.
5. In the opened window, enter your serial number, and then click **Activate**.

Recovering from an Acronis True Image 2015 error

If Acronis True Image 2015 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 2015 installer again. It will detect Acronis True Image 2015 on your computer and will ask you if you want to repair or remove it.

Removing Acronis True Image 2015

Select **Start -> Settings -> Control panel -> Add or remove programs -> Acronis True Image 2015 -> Remove**. Then follow the instructions on the screen.

If you use Windows Vista, select **Start -> Control panel -> Programs and Features -> Acronis True Image 2015 -> Remove**. Then follow the instructions on the screen. You may have to reboot your computer afterwards to complete the task.

If you use Windows 7, select **Start -> Control Panel -> Uninstall a program -> Acronis True Image 2015 -> Uninstall**. Then follow the instructions on the screen. You may have to reboot your computer afterwards to complete the task.

If you use Windows 8, click the Settings icon, then select **Control Panel -> Uninstall a program -> Acronis True Image 2015 -> Uninstall**.

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

Upgrading from old versions of True Image

If you already have True Image installed, the new version will simply update it; there is no need to remove the old version and reinstall the software.

Please keep in mind that the backups created by the later program version may be incompatible with the previous program versions. Therefore if you roll back Acronis True Image 2015 to an older 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 product upgrade.

1.5 Activating Acronis True Image 2015

To use Acronis True Image 2015, 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.

You can activate Acronis True Image 2015 either on your computer or from another computer, if your computer is not connected to the Internet.

Activation on a computer connected to the Internet

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

To activate the product manually from the main screen:

1. Start Acronis True Image 2015.
2. On the main program screen, click **Activate now** on the information bar.

If the computer where you install Acronis True Image 2015 does not have Internet connection or if the program cannot connect to Acronis Activation Server, you may select one of the following actions:

- **Try again** - select this option to try to connect to the Acronis Activation Server again.
- **Retry automatically later** - Acronis True Image 2015 will try to connect to the Acronis Activation Server every hour without the user interaction.
- **Activate from another computer** - you can activate the program manually from another machine that is connected to the Internet (see below).

Activation from another computer

If your computer is not connected to the Internet, you may activate Acronis True Image 2015 by using another computer which has connection to the Internet.

To activate the product from another computer:

1. Install and start Acronis True Image 2015.
2. On the main program screen, click **Activate now** on the information bar.
3. In the opened window, select **Activate from another computer**.
4. In the Acronis True Image 2015 Activation window, perform 3 simple steps:

1. Save your installation code to a file by clicking the **Save to file** button, and specify a removable media as the file location (for example, a USB flash drive). You may also simply write down this code on a piece of paper.
 2. On another computer which has the Internet connection, go to <http://www.acronis.com/activation/>. The instructions on the screen will help you to get your activation code by using the installation code. Save the obtained activation code to a file on a removable media, or write it down on paper.
 3. On your computer, click the **Load from file** button and specify a path to the file with the activation code; or, simply type it into the box from the piece of paper.
5. Click **Activate**.

"Too many activations" issue

Possible reasons for the issue:

- **You exceed the maximum number of computers with installed Acronis True Image 2015.**
For example, you have a serial number for one computer and you install True Image on the second computer.
Solutions:
 - Enter a new serial number. If you do not have it, you can buy it in the Acronis built-in store.
 - 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 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 True Image sees your computer as a new one.
Solution:
To reactivate True Image on your computer, choose from the list the same computer by its old name.

1.6 Trial version information

General limitations

The trial version of Acronis True Image 2015 works only during the trial period of 30 days. It has the following limitations:

- Disk cloning is disabled.
- Only recovery is available when booting from an Acronis Bootable Media.

Synchronization

Data synchronization is available without any limitations, but when the trial period expires:

- Your computer is excluded from all syncs. After installing the full version of Acronis True Image 2015 you will be able to connect to the syncs again.
- All the versions of synced files will be permanently deleted from Acronis Cloud.

Acronis Cloud

You have unlimited storage space during the trial period. You can use this space to store your online backups and versions of synced files. After the trial period is over, Acronis Cloud works in

recovery-only mode for 30 days. After this period you won't be able to use the Acronis Cloud service and all your data on the Cloud will be deleted.

Upgrading to the full version

You can buy the full version at the Acronis website or using in-app purchase functionality. See details in *Upgrading Acronis True Image 2015* (p. 12).

1.7 Upgrading Acronis True Image 2015

Trial version upgrade

To upgrade to the full version of the product:

1. Start Acronis True Image 2015.
2. On the sidebar, click **License**, 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.

Updating Acronis True Image 2015

To update True Image:

1. Start Acronis True Image 2015.
2. On the sidebar, click **Help**, and then click **About True Image**.
If there is a new version available, you will see the appropriate message next to the current build number.
3. Click **Download and install**.

Before you start downloading, please 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, turn on or turn off the **Automatically check for updates at startup** switcher.

Built-in store

Acronis True Image 2015 adds in-app purchase functionality.

Using in-app purchase you can:

- Buy the full product, when your trial version expires.
- Buy the Family Pack upgrade for up to 3 computers.
- Buy, renew, and upgrade a subscription to the Acronis Cloud service.
- Purchase additional Acronis Cloud space.

Installing Acronis hotfixes

Acronis hotfix is a small update for Acronis products. It makes changes to one or more application files or registry keys but does not change an application version. A hotfix targets only a specific Acronis True Image 2015 build, and cannot be applied to any other build.

To install an Acronis hotfix, follow the steps described in **Updating Acronis True Image 2015** above. A list of available hotfixes for the current build will be displayed in a table, where you can select those you want to install.

Upgrading from old versions of True Image

If you already have True Image installed, the new version will simply update it; there is no need to remove the old version and reinstall the software.

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

1.8 Technical Support

Maintenance and Support Program

If you need assistance with your Acronis product, please go to <http://www.acronis.com/support/>

Product Updates

You can download the latest updates for all your registered Acronis software products from our website at any time after logging into your **Account** (<http://www.acronis.com/my>) and registering the product. See **Registering Acronis Products at the Website** (<http://kb.acronis.com/content/4834>) and **Acronis Website User Guide** (<http://kb.acronis.com/content/8128>).

2 Getting started

In this section

Protecting your system	14
Backing up all data on your PC.....	16
Backing up your files	16
Cloning your hard drive.....	17
Recovering your computer	18
Recovering your files and folders.....	19
Getting started with Acronis Cloud.....	20

2.1 Protecting your system

To protect your system:

1. Create a backup of your system disk (p. 14).
2. Create bootable media (p. 15).

It is recommended to test the rescue media as described in Making sure that your rescue media can be used when needed (p. 110).

2.1.1 Step 1. Backing up your system disk

When should I back up my system disk?

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

Examples of these events include:

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

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

How do I create a backup of my system?

1. Start Acronis True Image 2015.
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 you first need to click the plus sign at the bottom of the list.

3. Click the **Backup source** icon, click **Disks and partitions**, and then select your system partition (usually C:) and the System Reserved partition (if any).

Instead of selecting specific partitions, you can choose the Entire PC backup. Refer to Backing up all data on your PC (p. 16) for details.

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

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

For advanced users: the best way to create a backup of your system disk is to do it under bootable media, and not under Windows.

Refer to Backing up disks and partitions (p. 35) for details.

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.

Refer to Deciding where to store your backups (p. 28) for details.

How many backup versions do I need?

In most cases, you need 2-3 backup versions of your system disk, with a maximum of 4-6 (see above for information about when to create backups).

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.

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.

2.1.2 Step 2. Creating bootable rescue media

What is bootable media?

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

How do I create bootable media?

1. Insert a CD-R/RW or plug in a USB drive.
2. Start Acronis True Image 2015.
3. On the sidebar, click **Tools**, and then click **Rescue Media Builder**.
4. On the first step, select **Acronis bootable rescue media**.
5. Select the device to use to create the bootable media.
6. Click **Proceed**.

How do I use bootable media?

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

1. Connect the bootable media to your computer (insert the CD or plug in the USB drive).

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

Refer to Arranging boot order in BIOS (p. 74) for details.

3. Boot your computer from the rescue media and select **Acronis True Image 2015**.

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

Refer to Acronis Media Builder for details.

Refer to Recovering your system (p. 62) for more details about computer recovery.

2.2 Backing up all data on your PC

What is an Entire PC backup?

An Entire PC backup is the easiest way to back up the full contents of your computer. We recommend that you choose this option when you are not sure which data that you need to protect. If you want to back up your system partition only, refer to Backing up disks and partitions (p. 35) for details.

When you select Entire PC as a backup type, 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. True Image recovers all data from the backup to the original location. Note that you cannot select specific disks or partitions to recover and you cannot change the default destination. If you need to avoid these limitations, we recommend that you back up your data with an ordinary disk-level backup method. Refer to Backing up disks and partitions (p. 35) 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.

How do I create an Entire PC backup?

To back up the entire contents of your computer:

1. Start Acronis True Image 2015.
2. On the sidebar, click **Backup**.
3. Click the **Backup source** icon, and then select **Entire PC**.
4. Click the **Backup destination** icon, and then select a destination for the backup.
5. Click **Start backup**.

2.3 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. Refer to Subscription information (p. 20) for details.

To back up files and folders:

1. Start Acronis True Image 2015.
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 Acronis account, and then click **OK**.
 - **Your external drive**—When an external drive is plugged into your computer, you can select it from the list.
 - **Browse**—Select a destination from the folder tree.
6. Click **Start backup**.

Refer to Backing up files and folders (p. 36) for details.

2.4 Cloning your hard drive

Why do I need it?

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

Before you start

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

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

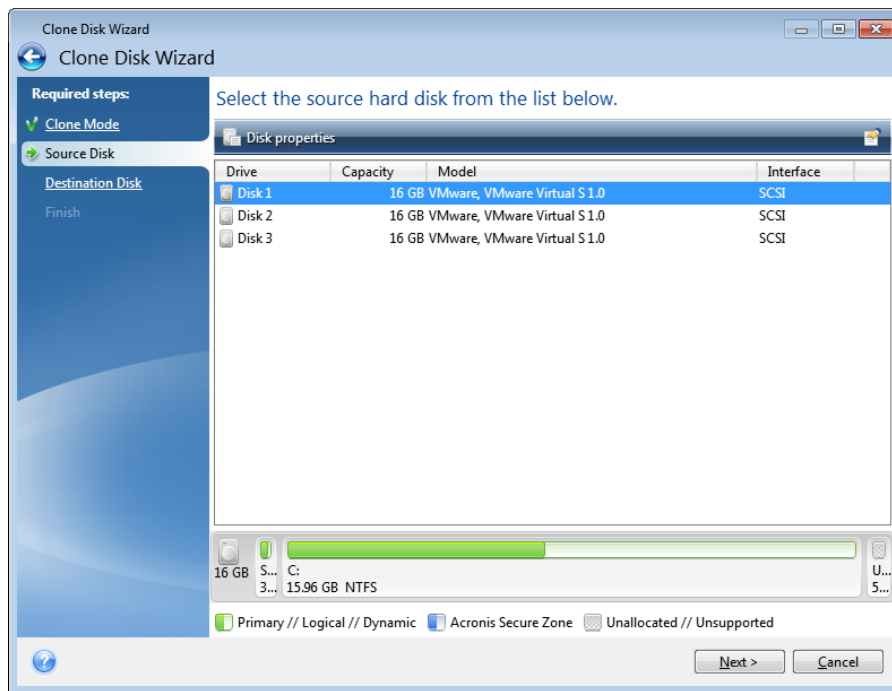
Using the Clone disk utility

To clone a disk:

1. On the sidebar, click **Tools**, and then click **Clone disk**.
2. On the **Clone Mode** step, we recommend that you choose the **Automatic** transfer mode. In this case, the partitions will be proportionally resized to fit your new hard drive. The **Manual** mode provides more flexibility. Refer to Clone Disk wizard (p. 97) for more details about the manual mode.

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

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



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

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

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

By default, Acronis True Image 2015 shuts down the computer after the clone process finishes. This enables you to change the position of master/subordinate jumpers and remove one of the hard drives.

2.5 Recovering your computer

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

- Trying to determine the crash cause (p. 61)
- Preparing for recovery (p. 61)
- Recovering your system to the same disk (p. 62)

Let's consider two different cases:

1. Windows works incorrectly, but you can start Acronis True Image 2015.
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 2015.
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. Depending on the backup type, click **Recover PC** or **Recover disks**.

5. In the opened window, select the backup version (the data state from a specific date and time).
6. Select the system partition and the System Reserved partition (if any) to be recovered.
7. Click **Recover now**.

To complete the operation, Acronis True Image 2015 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 2015.
Refer to Step 2 Creating bootable rescue media (p. 15) and Arranging boot order in BIOS (p. 74) for details.
2. On the Welcome screen, select **My disks** below **Recover**.
3. Select the system disk backup to be used for recovery. Right-click the backup and choose **Recover**.
When the backup is not displayed, click **Browse** and manually specify the path to the backup. In the same window, you can connect to Acronis Cloud and select an online backup. Refer to Recovering your system from Acronis Cloud (p. 79) 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 2015, remove the rescue media (if any), and boot from the recovered system partition. After making sure that you have recovered Windows to the state you need, restore the original boot order.

2.6 Recovering your files and folders

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

To recover files and folders:

1. Start Acronis True Image 2015.
2. On the sidebar, click **Backup**.
3. From the backup list, select the backup which contains the files or folders that you want to recover.
The backup can be located on local, network storage, or Acronis Cloud. When you recover data from Acronis Cloud, you first need to sign in to your Acronis account.
4. On the right panel, click **Recover files**.
5. Select the backup version (the data state from a specific date and time).
6. Select the files and folders that you want to recover, and then click **Next**.
7. Select a destination on your computer for the recovered files/folders. You can recover data to its original location or choose a new one, if necessary. To choose a new location, click the **Browse** button.
8. To start the recovery process, click the **Recover now** button.

2.7 Getting started with Acronis Cloud

Acronis Cloud might be unavailable in your region. For more information, click here:
<http://kb.acronis.com/content/4541>

Remote storage

On the one hand, 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. Refer to *What is True Image for mobile devices* (p. 91) for details.

To start using Acronis Cloud, you need a subscription to the service. Refer to *Subscription information* (p. 20) for details.

Web application

On the other hand, Acronis Cloud is a web application that allows you to recover and manage the data you store on Acronis Cloud. To work with the application, you can use any computer connected to the Internet.

To access the application, go to <https://www.acronis.com/my/online-backup/>, log in to your account, and then click **Recover my data now**.

2.7.1 Subscription information

Performing backups to Acronis Cloud requires subscription to the Acronis Cloud service. To subscribe, start Acronis True Image 2015 and sign in using your Acronis account.

If you use the trial version of the product, an unlimited storage space and 30-day free subscription will be assigned to your account automatically. See details in *Trial version information* (p. 11).

If you use the full version of the product, go to <https://www.acronis.com/my/online-backup/> and select a suitable subscription plan. To change your tariff, renew the subscription, or unsubscribe, go to the same subscription webpage.

How to create an Acronis account

If you do not have an Acronis account yet, perform the following steps:

1. On the sidebar, click **Account**, and then click **Create account**.
2. In the opened registration form, provide your email address, a password for your new account and confirm the password by retyping it once more in the appropriate field.

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.

3. Click **Create account**.

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

3 Basic concepts

In this section

Basic concepts.....	22
The difference between file backups and disk/partition images	23
Full, incremental and differential backups	24
FAQ about backup, recovery and cloning	26
Deciding where to store your backups	28
Using Acronis Nonstop Backup	29
Backup file naming	32
Integration with Windows	32
Wizards.....	33

3.1 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). Refer to Protecting your system (p. 14) 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 2015 does both by creating disk (or partition) images and file-level backups respectively.

Backup versions

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

Backup versions represent full, incremental and differential backups - see Full, incremental and differential backups (p. 24).

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

Disk cloning

This operation 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

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

Acronis Nonstop Backup uses a special hidden storage for data and metadata. The backed up data is compressed and split into files of about 1 GB. These files also have a proprietary format and the data they contain can be recovered only with the help of 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, 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, please do it by using the tools provided by Acronis True Image 2015.

Acronis True Image 2015 stores information on the backups in a metadata information database. Therefore, deleting unneeded backup files in Windows Explorer will not delete information about these backups from the database. This will result in errors when the program tries to perform operations on the backups that no longer exist.

3.2 The difference between file backups and disk/partition images

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

Disk/partition backups are different from file and folder backups. Acronis True Image 2015 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:
 1. Boot code.
 2. File system meta data, including service files, file allocation table (FAT), and partition boot record.

3. File system data, including operating system (system files, registry, drivers), user data and software applications.
3. System Reserved partition, if any.
4. EFI system partition, if any (applicable to GPT disk backups only).

What is excluded from disk backups?

To reduce image size and speed up image creation, by default Acronis True Image 2015 only stores the hard disk sectors that contain data.

Acronis True Image 2015 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 2015 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, True Image excludes the following data:

- The Temp folder (usually located in C:\Windows\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 files
- .tmp files
- .~ files

3.3 Full, incremental and differential backups

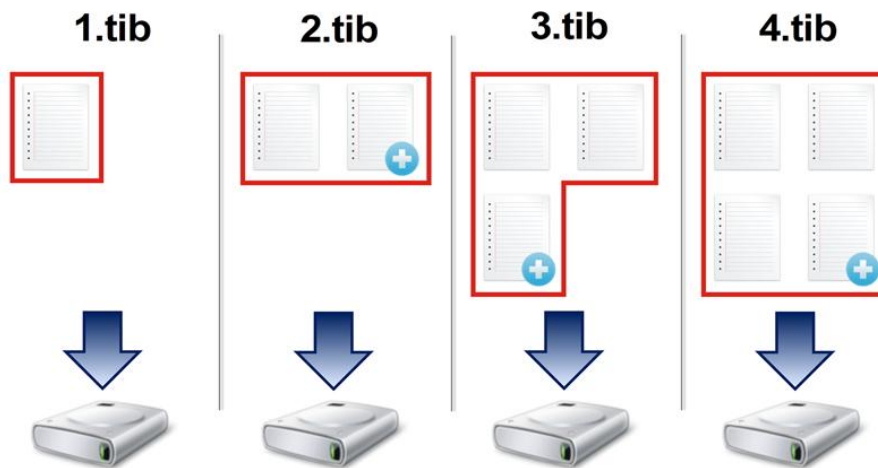
Acronis True Image 2015 offers three backup methods:

Full method

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

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

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



Additional information

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

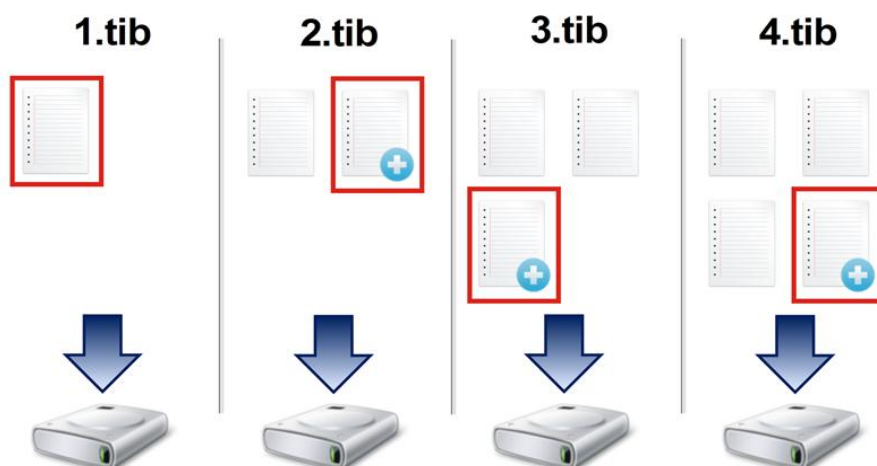
Incremental method

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

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

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

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



Additional information

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

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

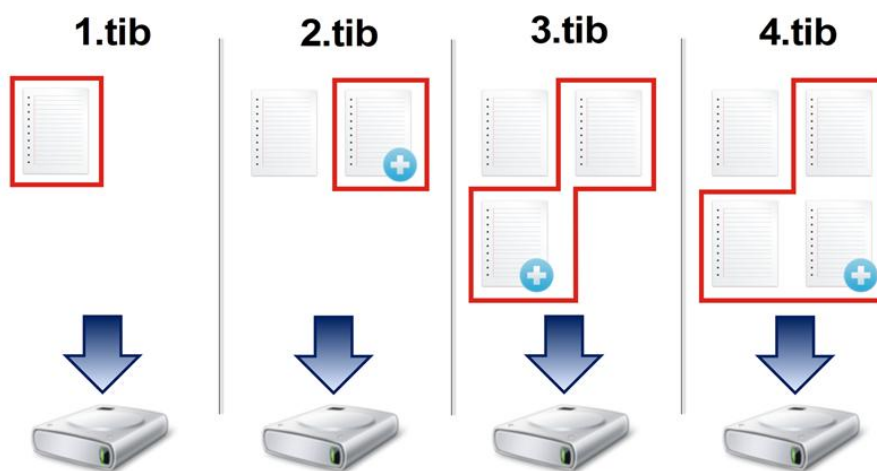
Differential method

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

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

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

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



Additional information

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

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

To choose a desired backup method, you usually need to configure a custom backup scheme. For more information see Custom schemes (p. 43).

3.4 FAQ about backup, recovery and cloning

- **I have a 150GB system partition, but the occupied space on that partition is only 80GB. What will Acronis True Image 2015 include in a backup?** - By default, Acronis True Image 2015 copies only the hard disk sectors that contain data, so it will include only 80GB in a backup. You can also choose the sector-by-sector mode. Note that such a backup mode is required only in special cases. For more information see Image creation mode (p. 49). While creating a sector-by-sector

backup, the program copies both used and unused hard disk sectors and the backup file will usually be significantly larger.

- **Will my system disk backup include drivers, documents, pictures, etc.?** - Yes, such a backup will contain the drivers, as well as the contents of the My documents folder and its subfolders, if you kept the default location of the My documents folder. If you have just a single hard disk in your PC, such a backup will contain all of the operating system, applications and data.
- **I have an old hard disk drive which is almost full in my notebook. I purchased a new bigger HDD. How can I transfer Windows, programs and data to the new disk?** - You can either clone the old hard disk on the new one or back up the old hard disk and then recover the backup to a new one. The optimum method usually depends on your old hard disk partitions layout.
- **I want to migrate my old system hard disk to an SSD. Can this be done with Acronis True Image 2015?** - Yes, Acronis True Image 2015 provides such a function. For procedure details, see Migrating your system from an HDD to an SSD (p. 102)
- **What is the best way to migrate the system to a new disk: cloning or backup and recovery?** - The backup and recovery method provides more flexibility. In any case, we strongly recommend to make a backup of your old hard disk even if you decide to use cloning. It could be your data saver if something goes wrong with your original hard disk during cloning. For example, there were cases when users chose the wrong disk as the target and thus wiped their system disk. In addition, you can make more than one backup to create redundancy and increase security.
- **What should I back up: a partition or the whole disk?** - In most cases, it is better to back up the whole disk. However, there may be some cases when a partition backup is advisable. For example, your notebook has a single hard disk with two partitions: system (disk letter C) and the data (disk letter D). The system partition stores your working documents in the My documents folder with subfolders. The data partition stores your videos, pictures, and music files. Such files are already compressed and backing them up using Acronis True Image 2015 would not give you significant reduction of the backup file size. In this case, it may be better to use a local sync for the data partition files and a separate backup for the system partition. However, we also recommend creating at least one whole disk backup if your backup storage has enough space.
- **Could you tell me how to clone: in Windows or after booting from the rescue media?** Even when you start cloning in Windows, the computer will reboot into the Linux environment the same as when booting from the rescue media. Because of this, it is better to clone under rescue media. For example, there may be a case when your hard disk drives are detected in Windows and not detected in Linux. If this is the case, the cloning operation will fail after reboot. When booting from the rescue media, you can make sure that Acronis True Image 2015 detects both the source and target disks before starting the cloning operation.
- **Can I clone or back up and recover a dual boot machine?** Yes, this is possible in most cases. If your systems are installed in separate partitions of the same physical hard disk drive, cloning or recovery usually proceeds without any problems. If the systems are on different physical hard disk drives, there may be some problems with bootability after recovery.
- **Does Acronis True Image 2015 support RAID?** - Acronis True Image 2015 supports hardware RAID arrays of all popular types. Support of software RAID configurations on dynamic disks is also provided. Acronis Bootable Rescue Media supports most of the popular hardware RAID controllers. If the standard Acronis rescue media does not "see" the RAID as a single volume, the media does not have the appropriate drivers. In this case you can try to create WinPE-based rescue media. This media may provide the necessary drivers.

3.5 Deciding where to store your backups

Acronis True Image 2015 supports quite a few of storage devices. For more information, refer to Supported storage media.

The table below shows possible backup destinations for your data.

	HDD (internal or external)	SSD	USB flash drive	Acronis Cloud	File server, NAS or NDAS	Netwo rk share	SMB/ NFS share	FTP server	DVD or Blue-ray disc	Memor y card
MBR partitions or entire disks (HDD, SSD)	+	+	+	+	+	+	+	+	+	+
GPT/dynamic volumes or disks	+	+	+	+	+	+	+	+	+	+
Files and folders	+	+	+	+	+	+	+	+	+	+
Email	-	-	-	-	-	-	-	-	-	-

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**

Please check whether Acronis True Image 2015 detects the selected backup storage, both in Windows and when booted from the rescue media.

To gain access to an NDAS-enabled storage device, in many cases you will need to specify the NDAS device ID (20 characters) and the write key (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.

The certain NAS devices can be detected by Acronis True Image 2015 if Bonjour software is installed.

4. **Network share**

See also: Authentication settings (p. 29).

5. **FTP server**

See also: FTP connection (p. 29).

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.

3.5.1 FTP connection

Acronis True Image 2015 allows you to store your backups on FTP servers.

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

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

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

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

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

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

Because of this, Acronis True Image 2015 splits a backup into files with a size of 2GB when backing up directly to an FTP server. If you back up to a hard disk with the aim of transferring the backup to an FTP later, you may split the backup into files of 2GB each by setting the desired file size in the backup options.

An FTP server must allow passive mode file transfers.

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

3.5.2 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 click a networked computer name. To open it manually, click **Specify credentials for this location**.

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

3.6 Using 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.

You can create only one nonstop backup.

You cannot use Acronis Nonstop Backup for protecting data stored on external hard drives.

How it works

Once you start Acronis Nonstop Backup, the program will perform an initial full backup of the data selected for protection. Acronis Nonstop Backup will then save changes in the protected files (including open ones) every five minutes, so that you will be able to recover your system to an exact point in time.

Usually the different states of the protected data will be backed up at 5-minute intervals for 24 hours.

The older backups will be consolidated in such a way that Acronis True Image 2015 will keep daily backups for the last 30 days and weekly backups until all Nonstop Backup data destination space is used.

Note, that if Acronis Nonstop Backup protects a non-system partition and no changes have occurred for 5 minutes since the last backup, the next scheduled backup will be skipped. Acronis Nonstop Backup will wait for a significant data change and will create a new incremental backup only when such change has been detected. In those cases, the actual time interval will exceed 5 minutes. In addition, if, for instance, you are working in Word and do not use the "Save" operation for an hour, changes in the Word document will not be backed up every five minutes, because Acronis True Image 2015 checks file changes on the disk and not in the memory.

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.

You may think that at these backup rates the storage will fill in no time. Do not worry as Acronis True Image 2015 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 2015 backs up only its changed parts in addition to the initially backed up file.

3.6.1 Acronis Nonstop Backup data storage

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

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

You can also use an NAS as the storage, but with one limitation - it must be accessible with the SMB protocol. It does not matter whether an NAS share you want to use for the storage is mapped as a local disk or not. If the share requires login, you will need to provide the correct user name and password. For more information see Authentication settings (p. 29). Acronis True Image 2015 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. Please note 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 2015 checks whether the selected destination has enough free space. It 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.

3.6.2 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. An Acronis Support Knowledge Base article at <http://kb.acronis.com/content/14708> describes the procedure for restarting the Acronis Nonstop Backup service.

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.

3.7 Backup file naming

By default, the program creates for each task a separate folder with task's name and then stores in the folder all backups for that task (For example, D:\My Backups\System)

A backup file name has the following attributes:

- Backup name.
- Backup method (full, inc, diff: full, incremental, differential).
- Number of backup chain (in the form of b#).
- Number of backup version (in the form of s#).
- Number of volume (in the form of v#).
For example this attribute changes when you split a backup into several files. Refer to Backup splitting (p. 50) for details.
- Macros, if applicable (can be in any part of a name, for example, in the beginning or in the end).

Thus a backup name may look the following way (note that "24.05.2012" in the following example is an optional macros):

1. **my_documents_full_b1_s1_v1.24.05.2012.tib**
2. **my_documents_full_b2_s1_v1.24.05.2012.tib**
3. **my_documents_inc_b2_s2_v1.24.05.2012.tib**
4. **my_documents_inc_b2_s3_v1.26.05.2012.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_v1-1.tib**.

3.8 Integration with Windows

During installation Acronis True Image 2015 provides closer integration with Windows. Such merging allows you to get the most out of your computer.

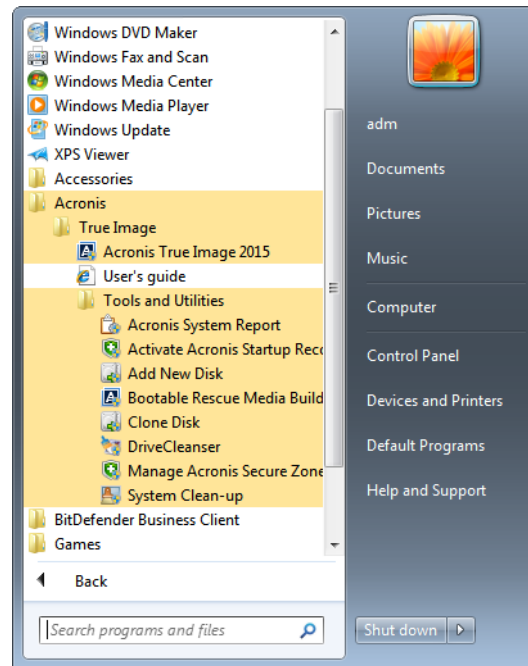
Acronis True Image 2015 integrates the following components:

- Acronis items on the Windows **Start** menu.
- Acronis True Image 2015 button on the taskbar.
- The **Acronis Recovery** tab in the **Properties** window of a file.
- Shortcut menu commands.

See details about the optional components in Integration settings.

Windows Start menu

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



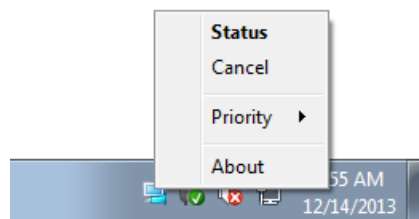
Acronis True Image 2015 button on the taskbar

The Acronis True Image 2015 button on the Windows taskbar shows the progress and result of Acronis True Image 2015 operations.



Taskbar notification area icons

During most of the operations, special indicator icons appear in the Windows taskbar notification area. This icon doesn't depend on the main program window being open.

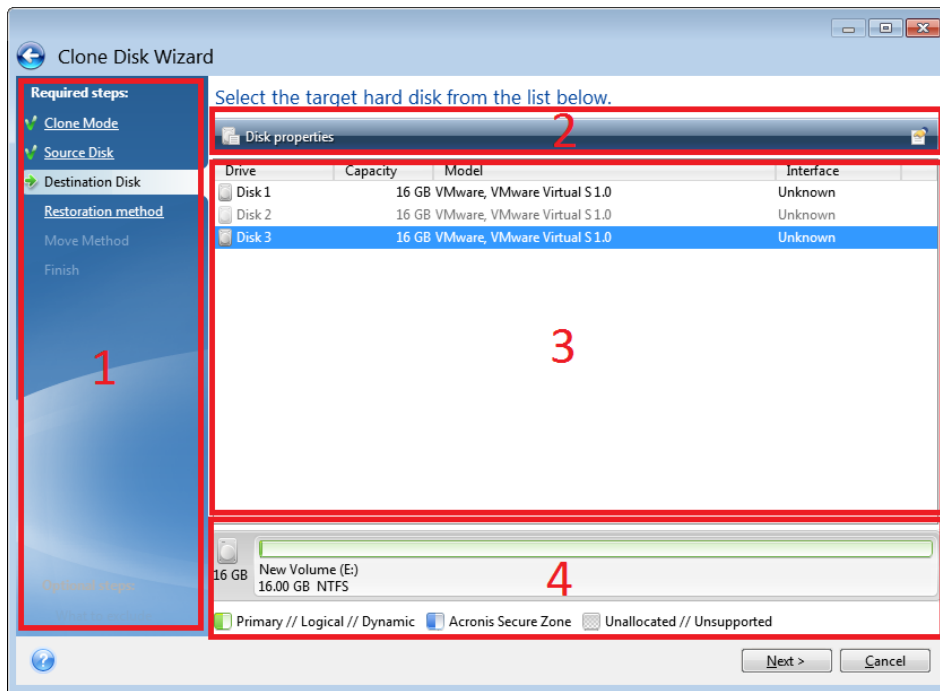


- To view a tooltip indicating the operation's progress or state, point to the icon.
- To view status, change priority or cancel a current operation, right-click the icon, and then click the corresponding command.

3.9 Wizards

When you use the available Acronis True Image 2015 tools and utilities, the program will in many cases employ wizards to guide you through the operations.

For example, see the screen shot below.



A wizard window usually consists of the following areas:

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

4 Backing up data

In this section

Backing up disks and partitions.....	35
Backing up files and folders	36
Backup options.....	37
Operations with backups	56

4.1 Backing up disks and partitions

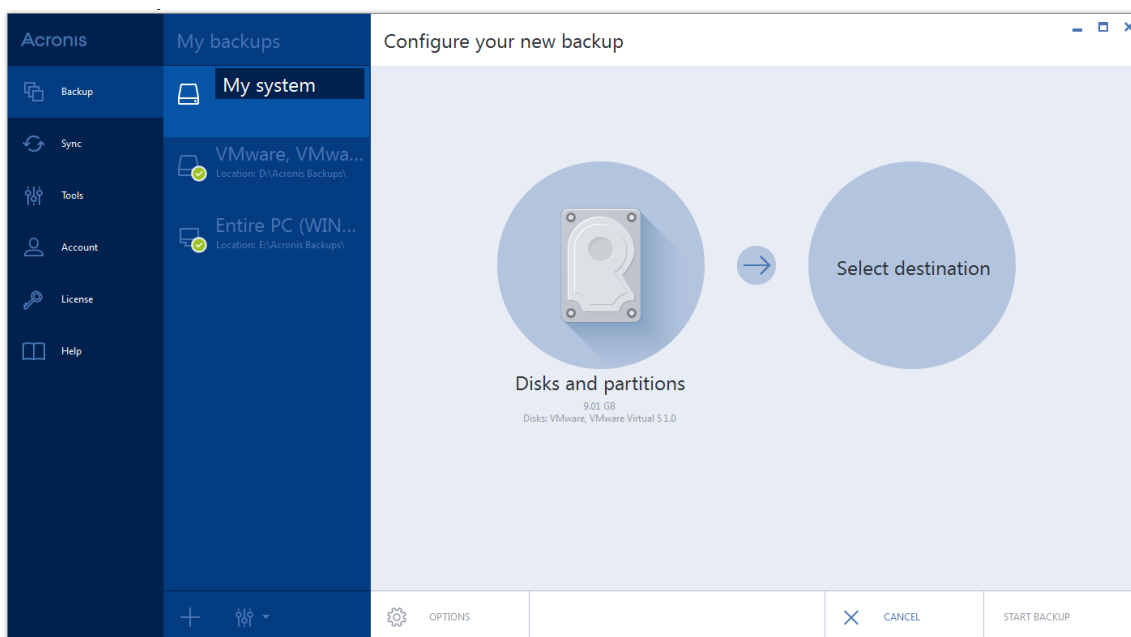
As opposed to file backups, disk and partition backups contain all the data stored on the disk or partition. This backup type is usually used to create an exact copy of a system partition of the whole system disk. Such backup allows you to recover your computer when Windows works incorrectly or cannot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

To back up partitions or disks:

1. Start Acronis True Image 2015.
2. On the sidebar, click **Backup**.
3. To add a new backup, click the plus sign at the bottom of the backup list, and then type a name for the backup.
4. Click the **Backup source** icon, and then select **Disks and partitions**.
5. In the opened window, select the check boxes next to the partitions and disks that you want to back up, and then click **OK**.

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

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



6. Click the **Backup destination** icon, and then select a destination for backup:
 - **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. Refer to Subscription information (p. 20) for details.

- **Your external drive**—When an external drive is plugged into your computer, you can select it from the list.
- **Browse**—Select a destination from the folder tree.

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

7. [optional step] Click **Options** to set the options for the backup, including Schedule (p. 39), Scheme (p. 41), and Password protection (p. 49). For more information see Backup options (p. 37).
8. Perform one of the following:
 - To run the backup immediately, click **Start backup**.
 - To run the backup later or on a schedule, click the arrow to the right of the **Start backup** button, and then click **Later**.

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.

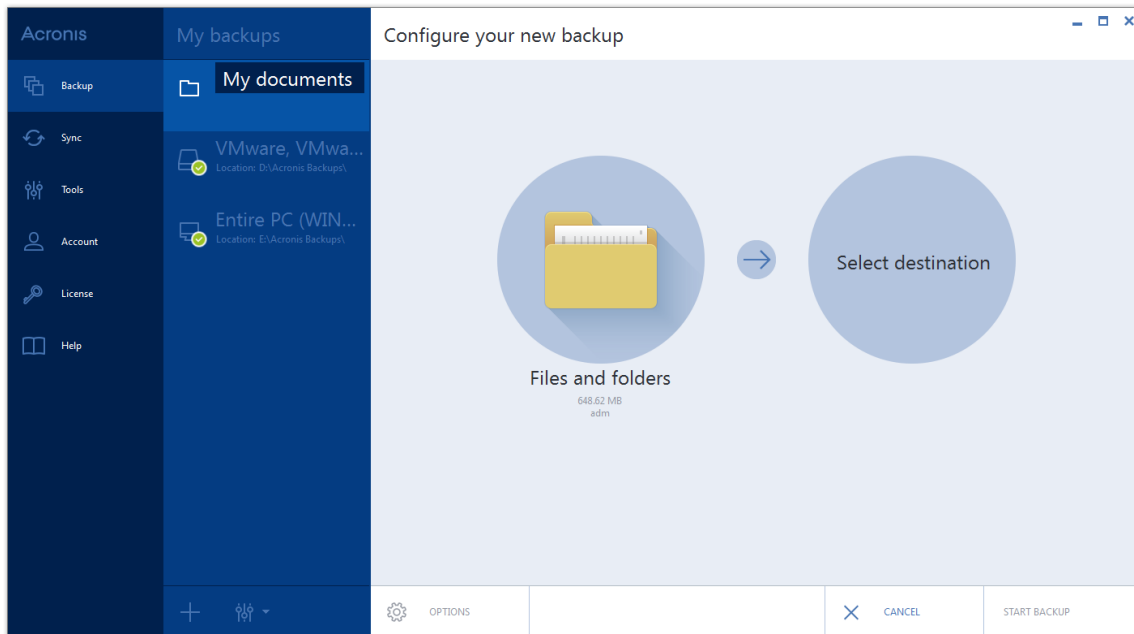
4.2 Backing up files and folders

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 2015.
2. On the sidebar, click **Backup**.
3. To add a new backup, click the plus sign at the bottom of the backup list, and then type a name for the backup.
4. Click the **Backup source** icon, and then select **Files and folders**.

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



6. Click the **Backup destination** icon, 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. Refer to Subscription information (p. 20) for details.
 - **Your external drive**—When an external drive is plugged into your computer, you can select it from the list.
 - **Browse**—Select a destination from the folder tree.
7. [optional step] Click **Options** to set the options for the backup, including Schedule (p. 39), Scheme (p. 41), and Password protection (p. 49). For more information see Backup options (p. 37).
8. Perform one of the following:
 - To run the backup immediately, click **Start backup**.
 - To run the backup later or on a schedule, click the down arrow to the right of the **Start backup** button, and then click **Later**.

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.

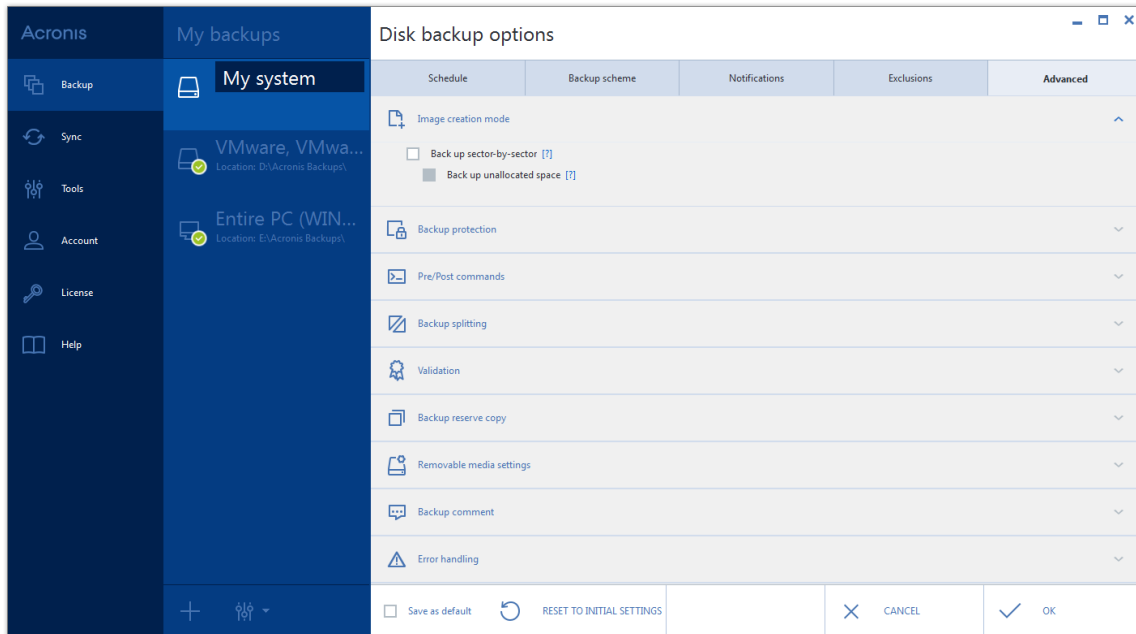
4.3 Backup options

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

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

After you have installed the application, all options are set to the initial values. You can change them for your current backup operation only or for all backups that will be created in future. Select the

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



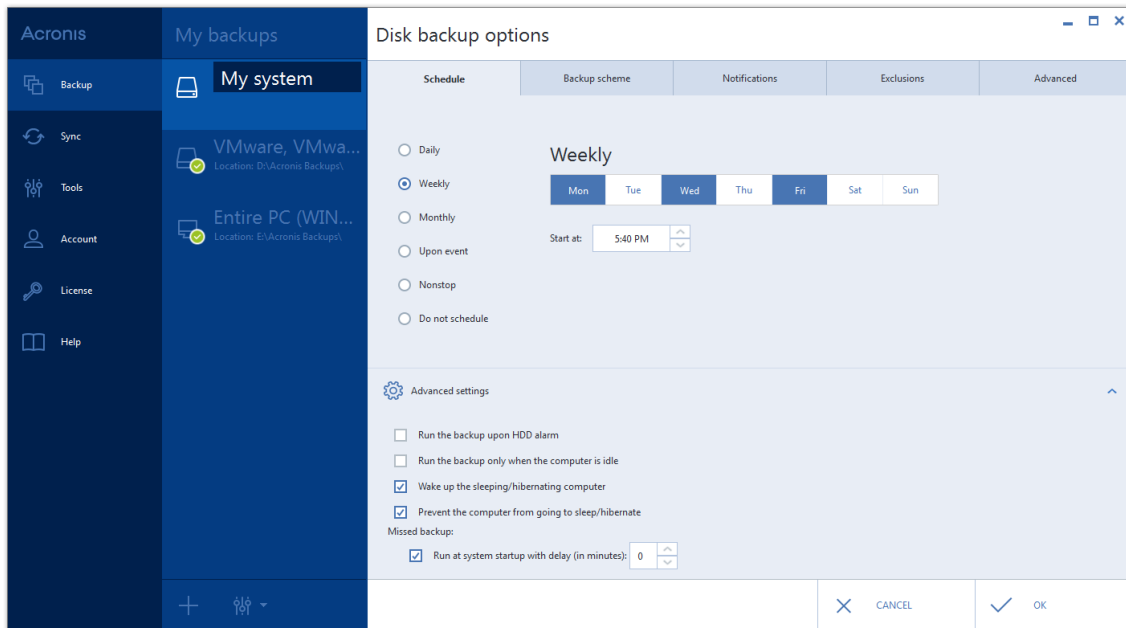
If you want to reset all the modified options to the values that were set after the product installation initially, click the **Reset to initial settings** button. Note that this will reset the settings for the current backup only. To reset the settings for all further backups, click **Reset to initial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

In this section

Scheduling	39
Backup schemes	41
Notifications for backup operation	46
Excluding items from backup	47
Image creation mode	49
Backup protection	49
Pre/Post commands for backup	50
Backup splitting	50
Backup validation option	51
Backup reserve copy	51
Removable media settings	52
Backup comment	52
Error handling	52
File-level security settings for backup	53
Computer shutdown	54
Acronis Cloud cleanup	54
Encryption key	54
Performance of backup operation	55

4.3.1 Scheduling

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



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

- **Nonstop** (p. 29)—The backup will run every five minutes.
- **Daily** (p. 40)—The operation will be executed once a day or more frequently.
- **Weekly** (p. 40)—The operation will be executed once a week or several times a week on the selected days.
- **Monthly** (p. 40)—The operation will be executed once a month or several times a month on the selected dates.
- **Upon event** (p. 41)—The operation will be executed upon an event.
- **Do not schedule**—The scheduler will be turned off for the current operation. In this case the backup or validation will run only when you click **Back up now** or **Validate** respectively in the main window.

Advanced settings

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

- To postpone a scheduled operation until the next time the computer is not in use (a screen saver is displayed or computer is locked), select the **Run the backup only when the computer is idle** check box. If you schedule validation, the check box will change to **Run the validation only when the computer is idle**.
- If you want to wake up the sleeping/hibernating computer to perform the scheduled operation, select the **Wake up the sleeping/hibernating computer** check box.
- If the computer is switched off when the scheduled time comes, the operation won't be performed. You can force the missed operation to run at the next system startup. To do so, select the **Run at system startup** check box.

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

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

4.3.1.1 Daily execution parameters

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

- **Start time or periodicity**
 - If you select **At**, set the operation's start time. Enter hours and minutes manually, or set the desired start time using the up and down buttons. You can specify several start times by clicking **Add**.
 - If you select **Every**, choose daily operation periodicity from the dropdown list (for example, every 2 hours).

Description of the **Advanced settings** see in Scheduling (p. 39).

4.3.1.2 Weekly execution parameters

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

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

Description of the **Advanced settings** see in Scheduling (p. 39).

4.3.1.3 Monthly execution parameters

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

- **Periodicity or dates**
 - If you select **Every**, choose a numeral and the day of the week from the dropdown lists (example: First Monday - the operation will be performed on the first Monday of every month)
 - If you select **On**, choose the date(s) for operation execution (example: you may want the operation to be run on the 10th, 20th, and last day of the month)
- **Start time**

Set the operation's start time. Enter hours and minutes manually, or set the desired start time using the up and down buttons.

Description of the **Advanced settings** see in Scheduling (p. 39).

4.3.1.4 Upon event execution parameters

You can set up the following parameters for the Upon event operation execution:

- **Event**
 - **User logon** – the operation will be executed each time the current user logs on to the OS.
 - **User logoff** – the operation will be executed each time the current user logs off the OS.
 - **System startup** – the operation will be executed at every OS startup.
Additionally, you can set a time delay to start backup after the system startup. For example, to start backup 20 minutes after system startup, type *20* in the appropriate box.
 - **System shutdown or restart** – the operation will be executed at every computer shutdown or reboot.

The last two options are unavailable for e-mail backups.

- **Additional condition**
 - If you want to run an operation only at the first occurrence of the event on the current day, select the **Once a day only** check box.

Description of the **Advanced settings** see in Scheduling (p. 39).

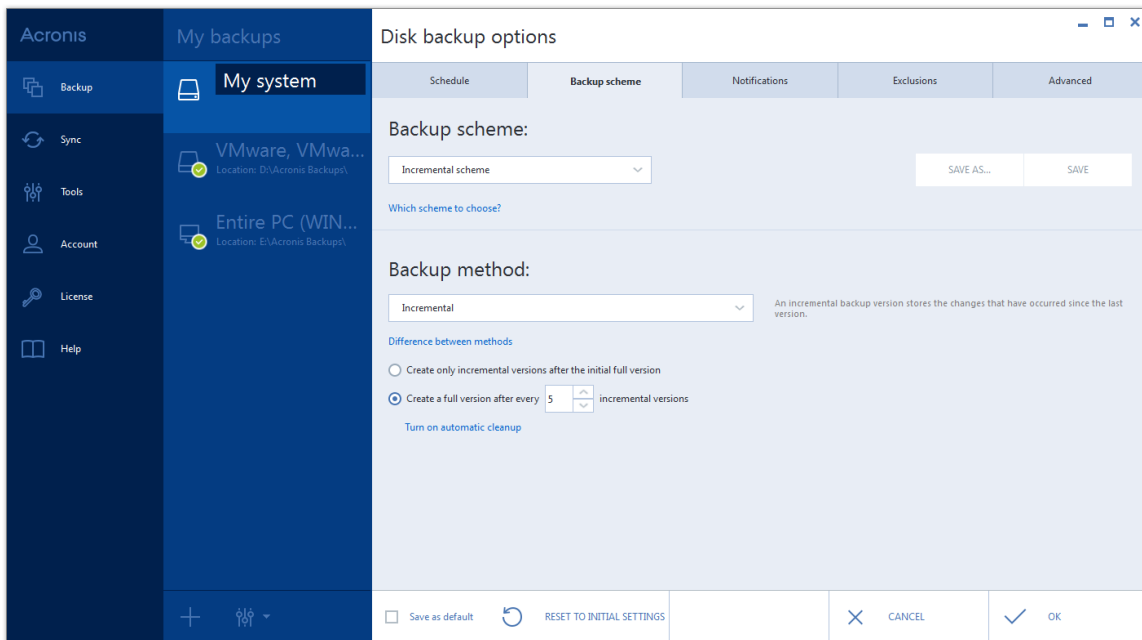
4.3.2 Backup schemes

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

Backup scheme defines the following parameters:

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

- Version cleanup rules



Acronis True Image 2015 allows you to choose from the following backup schemes:

- **Single version** (p. 42) - select this scheme if you want to use the smallest backup storage.
- **Version chain** (p. 42) - this may be the optimal scheme in many cases.
- **Incremental** - select to create a full version after every five incremental versions. This is the default scheme.
- **Differential** - select to create only differential backups after an initial full backup.
- **Custom** (p. 43) - select to set up a backup scheme manually.

You cannot change the backup scheme when backing up to optical media such as a DVD/BD. In this case, Acronis True Image 2015 by default uses a custom scheme with only full backups. This is because the program cannot consolidate backups stored on optical media.

4.3.2.1 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 backup manually.

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.

4.3.2.2 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.

4.3.2.3 Custom schemes

With Acronis True Image 2015 you also can create your own backup schemes. Schemes can be based on the pre-defined backup schemes. You can make changes in a selected pre-defined scheme to suit your needs and then save the changed scheme as a new one.

You cannot overwrite existing pre-defined backup schemes.

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

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

- **Full (p. 24)**
Select this method if you want to create only full backup versions.
- **Differential (p. 24)**
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 item 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 item to create several backup version chains. This is a more reliable but more space-consuming backup scheme.
- Incremental (p. 24)
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 item 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 item to create several backup version chains. This is a more reliable but more space-consuming backup scheme.

Automatic cleanup rules

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

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

The first backup version option

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

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

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

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

Managing custom backup schemes

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

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

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

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

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

The pre-defined backup schemes cannot be deleted.

Examples of custom schemes

1. 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. Refer to Backing up files and folders for details.
2. Click **Options**, open **Schedule** tab, then click **Daily** and 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 6 incremental versions day by day. Then, it will create 1 full version and 6 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. In the **File Backup** window, 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.

2. 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. Refer to Backing up disks and partitions (p. 35).
2. Select your system partition (usually C:) as the backup source.

3. Click **Options**, open **Schedule** tab, then click **Monthly** and specify, for example, the 1st and 15th days of the month. This will result in a backup version in about every 2 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 3 differential versions, each one in about two weeks. Then again a full version and 3 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**.

When the total backup size exceeds 100 GB, Acronis True Image 2015 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 3 differential backup versions.

9. In the **Disk Backup** window, 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.

4.3.3 Notifications for backup operation

Sometimes a backup or recovery procedure can last an hour or longer. Acronis True Image 2015 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 2015 finds out that the free space in the selected backup location is already less than the specified value, the program will not begin the actual backup process and will immediately inform you by displaying an appropriate message. The message offers you three choices - to ignore it and proceed with the backup, to browse for another location for the backup or to cancel the backup.

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

To set the free disk space threshold:

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

Acronis True Image 2015 can monitor free space on the following storage devices:

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

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

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

Email notification

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

To configure the email notifications:

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

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

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

Additional notification settings:

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

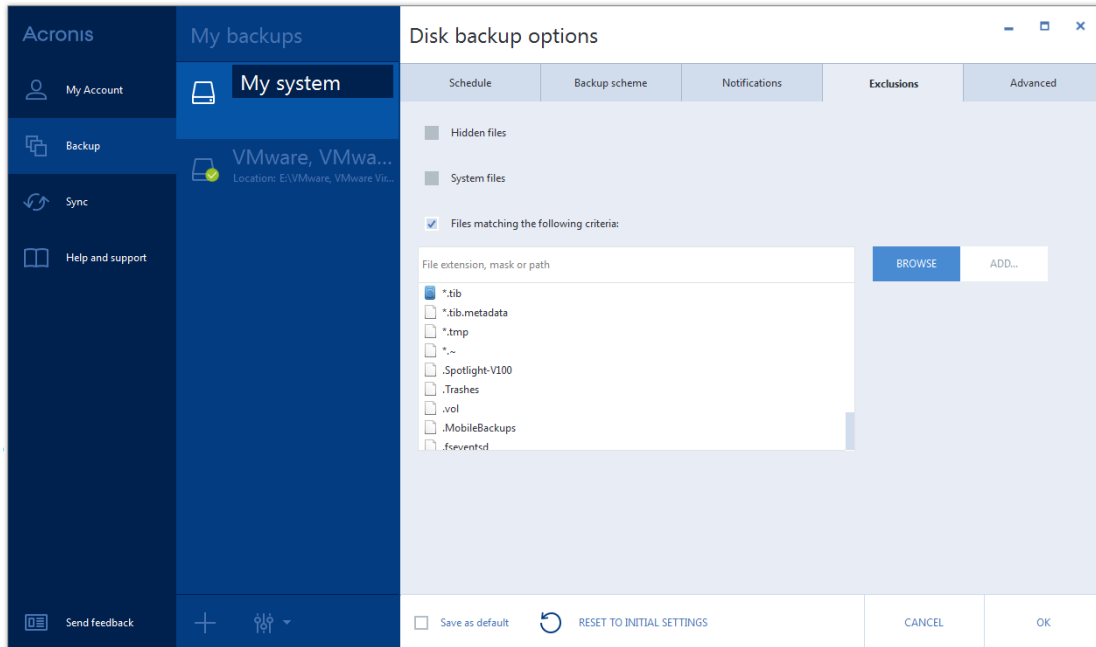
4.3.4 Excluding items from backup

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

1. You can exclude hidden and system files from a backup by selecting the corresponding check boxes.

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

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

How 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 **Browse**, select the folder you want to exclude on the directory tree, click **OK**, and then click **Add**.

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

4.3.5 Image creation mode

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

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

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

4.3.6 Backup protection

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

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

To protect a backup:

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

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

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

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

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

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

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

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

How to get access to a password-protected backup

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

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

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

4.3.7 Pre/Post commands for backup

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

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

To specify commands (batch files):

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

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

4.3.7.1 Edit user command for backup

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

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

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

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

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

4.3.8 Backup splitting

Acronis True Image 2015 cannot split already existing backups. Backups can be split only when being created.

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

The default setting - **Automatic**. With this setting, Acronis True Image 2015 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 2015 will ask you to insert a new disk when the previous one is full.

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

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

4.3.9 Backup validation option

You can specify the following settings:

- **Validate backup when it is created** - 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 backup regularly** - Select to schedule validation of your backups to ensure that they remain "healthy".

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.
- **Advanced settings:** the **Run the validation only when the computer is idle** check box is selected.

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 (p. 39).

4.3.10 Backup reserve copy

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

Please, be aware that CD/DVDs are not supported as locations for reserve copies.

To make a reserve copy:

1. Select the **Create a reserve copy of my backups** check box.
2. Specify a location for the backup copies.

You can protect the reserve copy with a password. All other backup options will be inherited from the source backup.

4.3.11 Removable media settings

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

Acronis True Image 2015 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 True Image on media**
True Image - includes support of USB, PC Card (formerly PCMCIA) and SCSI interfaces along with the storage devices connected via them, and therefore is strongly recommended.
- **Place Acronis System Report on media**
Acronis System Report - the component allows you to generate system report that is used for collecting information about your system in case of any program problem. Report generation will be available before you start Acronis True Image 2015 from the bootable media. The generated system report can be saved to a USB flash drive.
- **Place Acronis One-Click Restore on media**
Acronis One-Click Restore is a minimal addition to your bootable media, allowing one-click data recovery from an image backup stored on this media. This means that when booting from the media and after clicking **Recover**, all data will be silently recovered to its original place. No options or selections such as resizing partitions will be possible.

Acronis One-Click Restore can be added to the media only when creating a full backup of an entire hard disk.

- **Ask for first media while creating backups on removable media**
You can choose whether to display the Insert First Media prompt when backing up to removable media. With the default setting, backing up to removable media may not be possible if the user is away, because the program will wait for someone to press OK in the prompt box. Therefore, you should disable the prompt when scheduling a backup to removable media. Then, if the removable media is available (for example, CD-R/RW inserted) the backup can run unattended.

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

4.3.12 Backup comment

This option allows you to add comments to the backup. Backup comments may help you to find the necessary backup later.

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

4.3.13 Error handling

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

You can set the following error handling policy:

- **Do not show messages and dialogs while processing (silent mode)** - Enable this setting to ignore errors during backup operations. This is useful when you cannot control the backup process. You can view the detailed log of all operations after the backup process finishes.

- **Ignore bad sectors** - This option is available only for disk and partition backups. It lets you successfully complete a backup even if there are bad sectors on the hard disk.

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

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

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

- **When not enough space in ASZ, delete the oldest backup** (the preset is enabled) - We recommend that you select this check box when planning unattended scheduled backups to the Acronis Secure Zone. Otherwise, when the Acronis Secure Zone is full during a backup operation, True Image suspends the backup and requires your action. The dialog will open even when the **Do not show messages and dialogs while processing (silent mode)** setting is enabled.
- **Repeat attempt if a backup fails** - This option allows you to automatically repeat a backup attempt if the backup fails for some reason. You can specify number of attempts and time interval between attempts. Note that if the error interrupting the backup persists, then the backup will not be created.

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

4.3.14 File-level security settings for backup

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

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

These options relate only to file/folder backups.

4.3.15 Computer shutdown

If you know that the backup process you are configuring may take a long time, you may select the **Shut down the computer after the backup is complete** check box. In this case, you will not have to wait until the operation completion. The program will perform the backup and turn off your computer automatically.

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

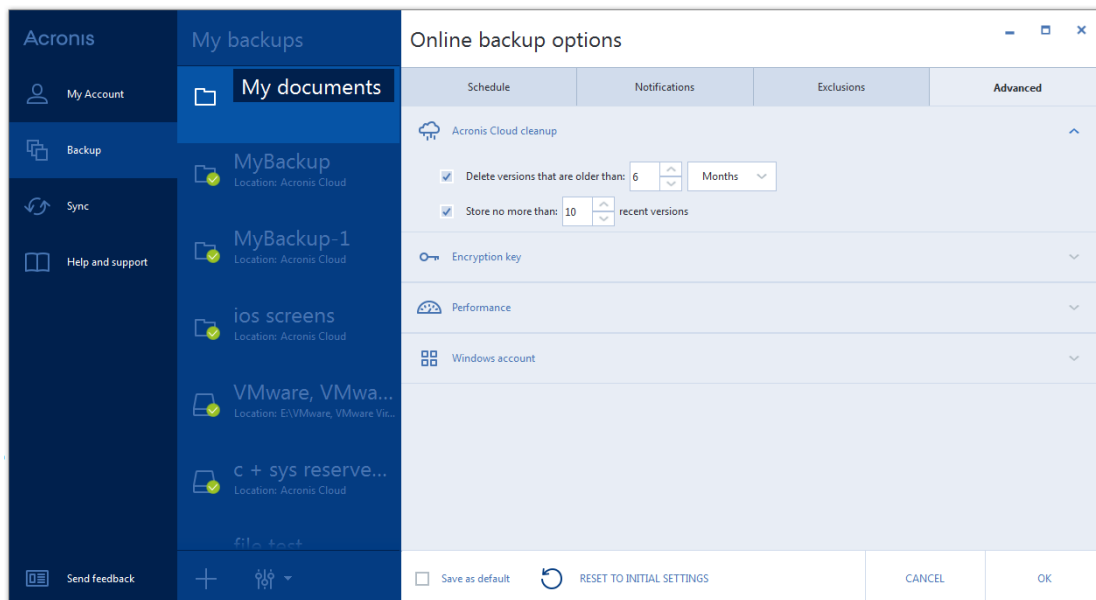
4.3.16 Acronis Cloud cleanup

This option is only available for online backup.

You can configure the cleanup settings for Acronis Cloud to optimize usage of its space.

To set the limits for the amount of versions on Acronis Cloud:


- Select the **Delete versions that are older than** check box and enter a value that limits the maximum age of the older versions. All other versions will be automatically deleted except the most recent versions.
- Select the **Store no more than ... recent versions** check box and enter a value that limits the maximum number of all versions in the storage.



4.3.17 Encryption key

This option is only available for online backup.

To protect your data on Acronis Cloud from unauthorized access, you can use encryption. In this case your data will be stored on Acronis Cloud in encrypted form. To encrypt and decrypt your data, the program needs the encryption key, that you should specify when you register your computer. An encryption key is a unique alphanumeric code, like a password. You can specify any set of characters you like. Note that the key is case-sensitive.

 **Warning!** An encryption key cannot be retrieved. Please memorize the key that you specify during your computer registration.

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

Note that you cannot set or change the encryption key for an already existing online backup.

4.3.18 Performance of backup operation

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

Compression level

You can choose the compression level for a backup:

- **None** - the data will be copied without any compression, which may significantly increase the backup file size.
- **Normal** - the recommended data compression level (set by default).
- **High** - higher backup file compression level, takes more time to create a backup.
- **Maximum** - maximum backup compression, but takes a long time to create a backup.

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

Operation priority

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

You can set up the operation priority:

- **Low** (enabled by default) - the backup or recovery process will run slower, but the performance of other programs will be increased.
- **Normal** - the backup or recovery process will have the equal priority with other processes.
- **High** - the backup or recovery process will run faster, but the performance of other programs will be reduced. Be aware that selecting this option may result in 100% CPU usage by Acronis True Image 2015.

Network connection speed limit

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

To reduce connection speed:

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

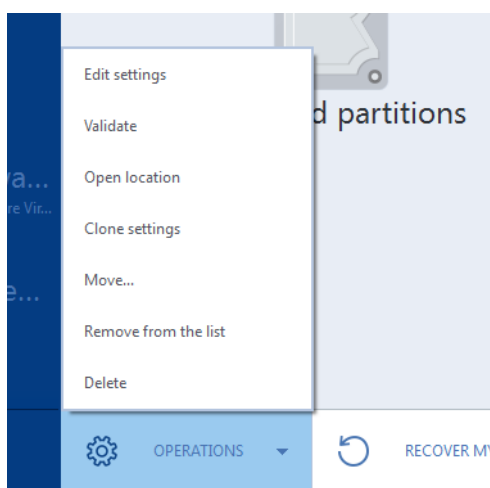
4.4 Operations with backups

In this section

Backup operations menu	56
Backup list operations.....	57
Validating backups	57
Backup to various places.....	58
Adding an existing backup to the list	58
Backing up to Acronis Cloud from several computers.....	59
Removing data from Acronis Cloud	59

4.4.1 Backup operations menu

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



The backup operations menu can contain the following items:

- **Edit settings** - allows editing of the current backup settings.
- **Reconfigure** (for backups manually added to the backup list) - allows configuring the settings of a backup created by a previous True Image version. This item may also appear for backups created on another computer and added to the backup list without importing their settings.
Without backup settings, you cannot refresh the backup by clicking **Back up now**. Also, you cannot edit and clone the backup settings.
- **Reconfigure** (for online backups) - allows you to bind a selected online backup to the current computer. To do this, click this item and reconfigure settings of the backup. Note that only one online backup can be active on one computer.
- **Validate** - starts backup validation.
- **Clean up** (available for nonstop backup only) - opens the **Cleanup** dialog box where you can delete the backup versions you no longer need. The backup chain will not be corrupted.
- **Open location** - opens the folder containing the backup files.
- **Clone settings** - Creates a new empty backup box with the settings of the initial backup and named **(1) [the initial backup name]**. Change the settings, save them, and then click **Back up now** on the cloned backup box.

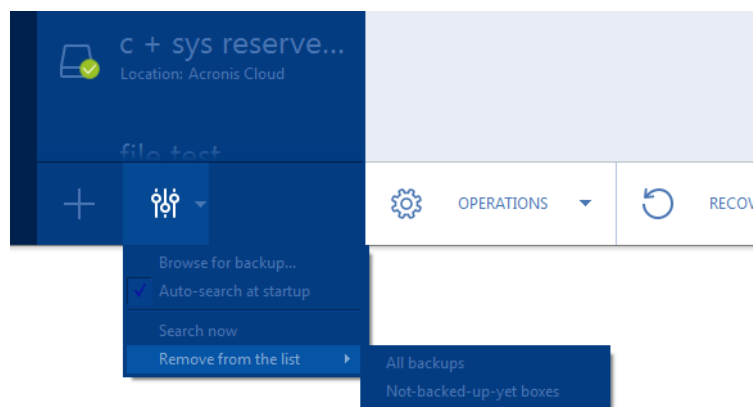
- **Move** - click to move all the backup files to another location. The subsequent backup versions will be saved to the new location.

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

- **Remove from the list** - removes the current backup from the backup list shown in the My backups area. This operation also turns off the scheduling of the removed backup (if a schedule was set), but it does not delete the backup files.
- **Delete** - depending on a backup type, this command completely deletes the backup from its location or allows you to choose whether you want to delete the backup completely or the backup box only. When you delete a backup box, the backup files remain in the location, and you will be able to add the backup to the list later. Note that when you delete a backup completely, the deletion cannot be undone.

4.4.2 Backup list operations

The menu contains commands that allow you to manage the backup list.



- **Browse for backup** - Click this item to browse for backups on your computer and add them to the backup list. This may be useful when you have backups created by a previous True Image version which are not shown in the backup list.
- **Auto-search at startup** - This setting allows the search for new backups at program startup to be turned on and off.
- **Search now** - This command allows you to search for True Image backups on your computer. All found backups are automatically added to the backup list.
- **Remove from the list:**
 - **All backups** - This command removes all backup boxes from the backup list. The removed backups can be returned to the list by using the Browse tool.
 - **Not-backed-up-yet boxes** - This command removes all "empty" backup boxes from the backup list. Be careful because, after removal, such backup boxes cannot be returned to the list.

4.4.3 Validating backups

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

Validating backups in Windows

To validate an entire backup:

1. Start Acronis True Image 2015, and then click **Backup** on the sidebar.
2. From the backup list, select the backup to validate, click **Operations**, and then click **Validate**.

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

To validate a specific backup version or an entire backup:

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

4.4.4 Backup to various places

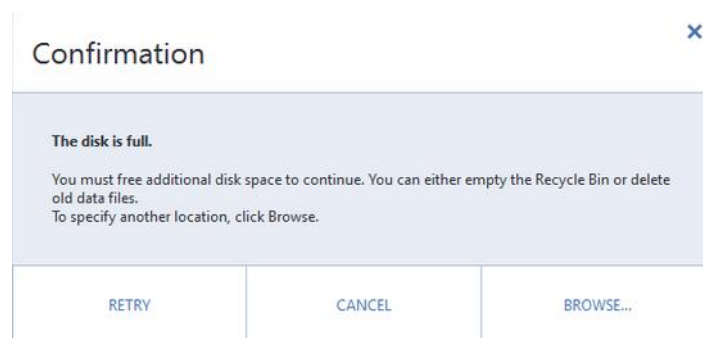
You can save versions of a backup to different destinations by changing the backup destination when editing the backup settings. For example, after you save the initial full backup to an external USB hard drive, you can change the backup destination to a USB stick by editing the backup settings. The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

You cannot continue backing up to an optical disc.

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

Splitting backups on-the-fly

When free space on the destination storage is insufficient to complete the current backup operation, the program displays a message warning you that the disk is full.



To complete the backup, perform one of the following:

- Free up some space on the disk and click **Retry**.
- Click **Browse**, and then select another storage device.

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

4.4.5 Adding an existing backup to the list

If you have backups that are not shown in the backup list in the **Backup** section (for example, backups created by a previous True Image version), you can add them to the list.

To add backups manually:

1. In the **Backup** section, click **Add backup**, and then click **Add existing backup**. Program opens a window where you can browse for backups on your computer.
2. Select the backup and click **Add**.

To add backups automatically:

- In the **Backup** section, click the **Backup list operations** icon, and then click one of the following:
 - To run the search, click **Search now**. Acronis True Image 2015 searches for backups on your computer and adds them to the list.
 - To search for backups every time the program starts, click **Auto-search at startup**.

4.4.6 Backing up to Acronis Cloud from several computers

When you want to back up data to Acronis Cloud under the same Acronis account, we recommend that you create a separate online backup on each computer. This allows you to avoid mixture of data from different computers within one online backup.

However, you may want to switch between your computers and back up data to the same online backup. When you sign in to your Acronis account, Acronis True Image 2015 tries to find out whether you already have online backups created on other computers. If this is the case, the program adds them to the backup list. To activate any of these backups on the current computer, click the **Start backup** button. After that, you can back up data of the current computer to the selected backup, but this backup will be stopped on the other computer. The backed up data from the previous computer is not deleted and remains available for recovery.

4.4.7 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 a variety of ways.

Deleting entire backup

The most "drastic" one is deleting the entire backup from a computer on Acronis Cloud. To remove the backup, click the gear icon on an online backup box and then click **Delete**.

Cleanup settings

The Online backup options provide for automatic cleanup of Acronis Cloud. You can specify deletion of files that have been kept longer than the specified number of months or days. In addition, you can set the maximum number of file versions to be kept on Acronis Cloud. You can accept the default settings for those options or set the values you need. For more information see Acronis Cloud cleanup (p. 54).

One-time cleanup

When your Acronis Cloud is full or is running out of space, we recommend that you use the cleanup tool in Acronis Cloud web application. This tool allows you to free up considerable amount of space on the cloud fast and easy.

To clean up Acronis Cloud:

1. Start Acronis True Image 2015 and click **Recover** on an online backup box. You will be taken to the Acronis Cloud web application.

2. On the **Storage status** tab, click the **Clean up space** link in the center of the screen.
3. In the opened window, configure the cleanup settings and click **Clean up now**.

Deleting specific files and folders

You can also manage Acronis Cloud by deleting individual files and folders.

1. Start Acronis True Image 2015 and click **Recover** on an online backup box. You will be taken to the Acronis Cloud web application.
2. Select files and folders you want to delete and click the **Delete** button.

5 Recovering data

In this section

Recovering disks and partitions	61
Recovering files and folders	75
Recovery from Acronis Cloud.....	76
Recovery options.....	81
Restoring computer to factory settings	85

5.1 Recovering disks and partitions

In this section

Recovering your system after a crash	61
Recovering partitions and disks	68
About recovery of dynamic/GPT disks and volumes	72
Arranging boot order in BIOS	74

5.1.1 Recovering your system after a crash

When your computer fails to boot, it is advisable to at first try to find the cause using the suggestions given in Trying to determine the crash cause (p. 61). If the crash is caused by corruption of the operating system, use a backup to recover your system. Make the preparations described in Preparing for recovery (p. 61) and then proceed with recovering your system.

5.1.1.1 Trying to determine the crash cause

A system crash can be due to two basic factors:

- **Hardware failure**

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

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

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

If the POST correctly detects your system hard disk drive, then the cause of the crash is probably a virus, malware or corruption of a system file required for booting. In this case, recover the system using a backup of your system disk or system partition. Refer to Recovering your system (p. 62) for details.

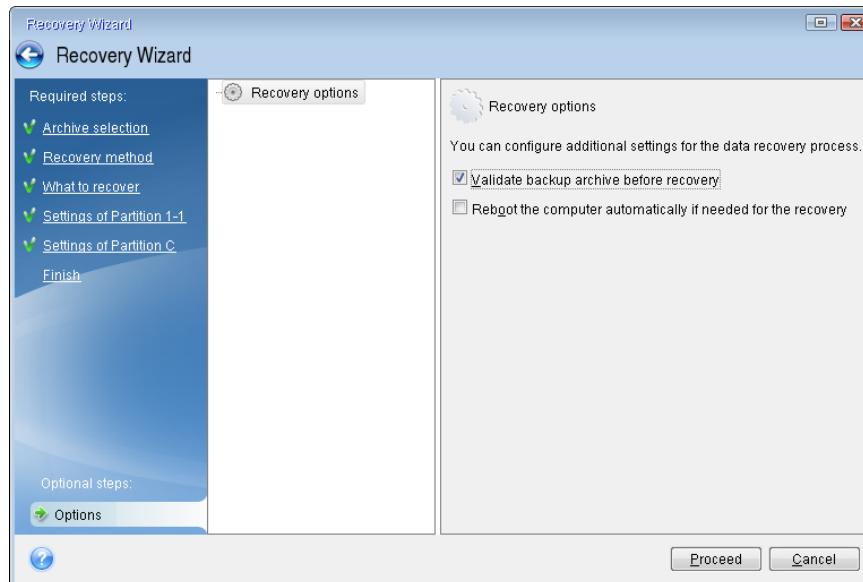
5.1.1.2 Preparing for recovery

We recommend that you perform the following actions before recovery:

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

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

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



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

When you use the Acronis True Image 2015 rescue media, it creates disk drive letters that might differ from the way Windows identifies drives. For example, the D: disk identified in the standalone Acronis True Image 2015 might correspond to the E: disk in Windows.

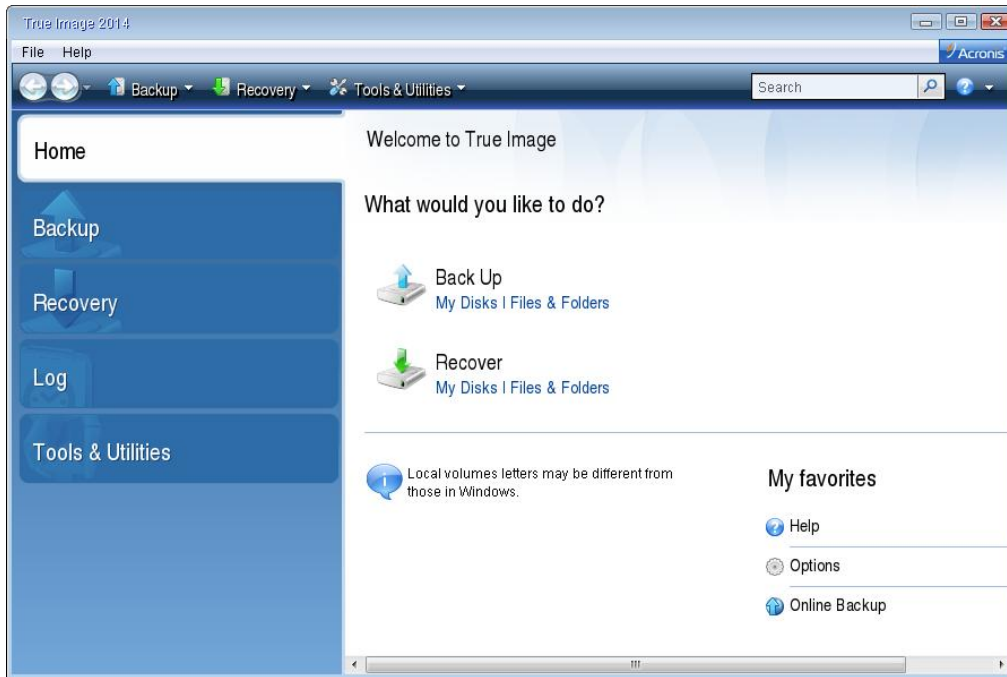
5.1.1.3 Recovering your system to the same disk

Before you start, we recommend that you complete the procedures described in Preparing for recovery (p. 61).

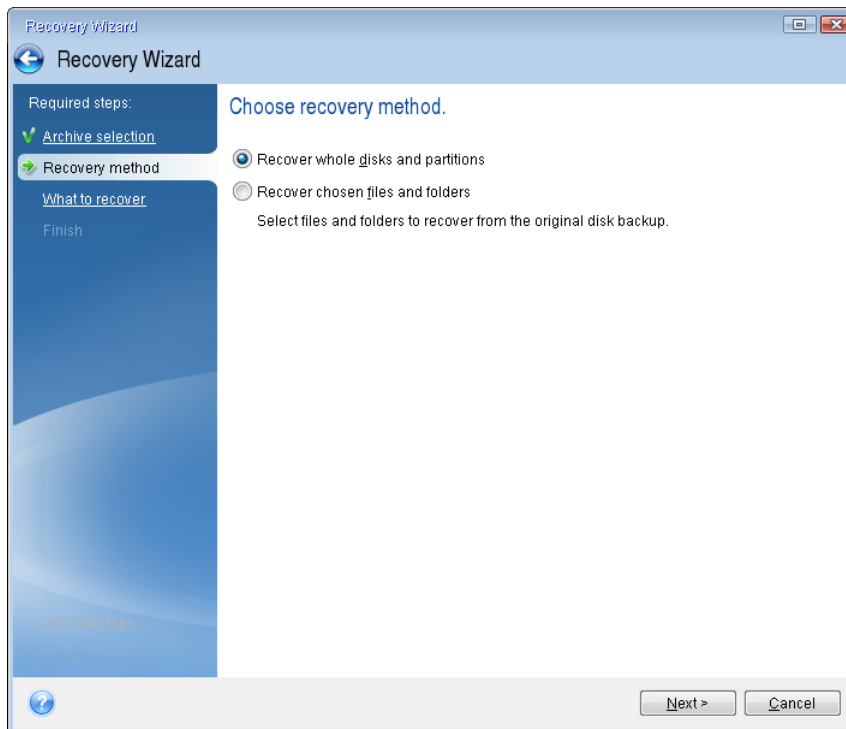
To recover your system:

1. Attach the external drive if it contains the backup to be used for recovery and make sure that the drive is powered on.
2. Arrange the boot order in BIOS so as to make your rescue media device (CD, DVD or USB stick) the first boot device. See Arranging boot order in BIOS (p. 74).
3. Boot from the rescue media and select **True Image**.

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

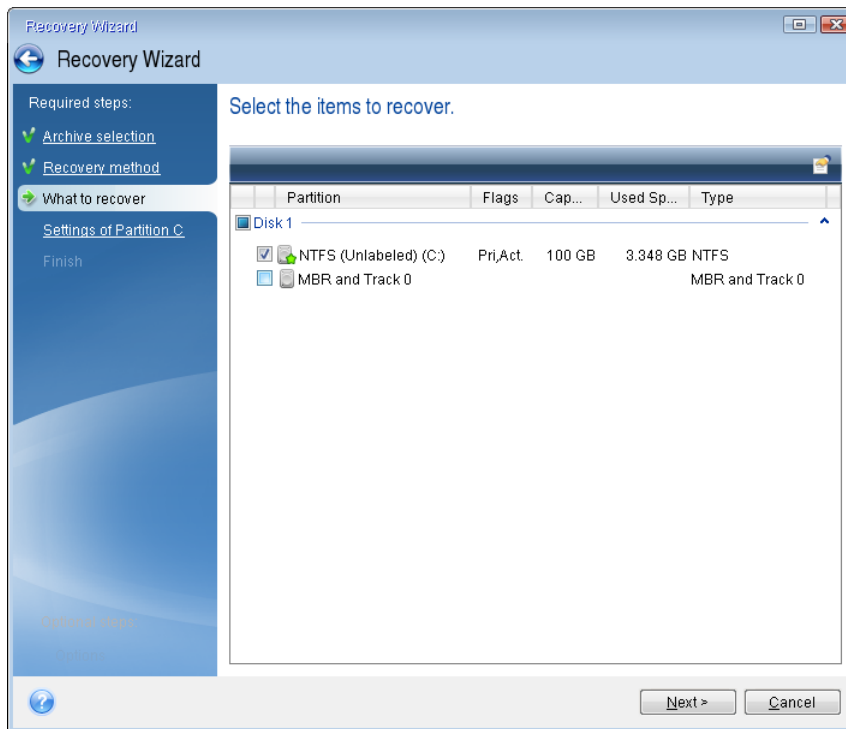


5. Select the system disk or partition backup to be used for recovery.
When the backup is not displayed, click **Browse** and specify path to the backup manually.
6. Select **Recover whole disks and partitions** at the **Recovery method** step.

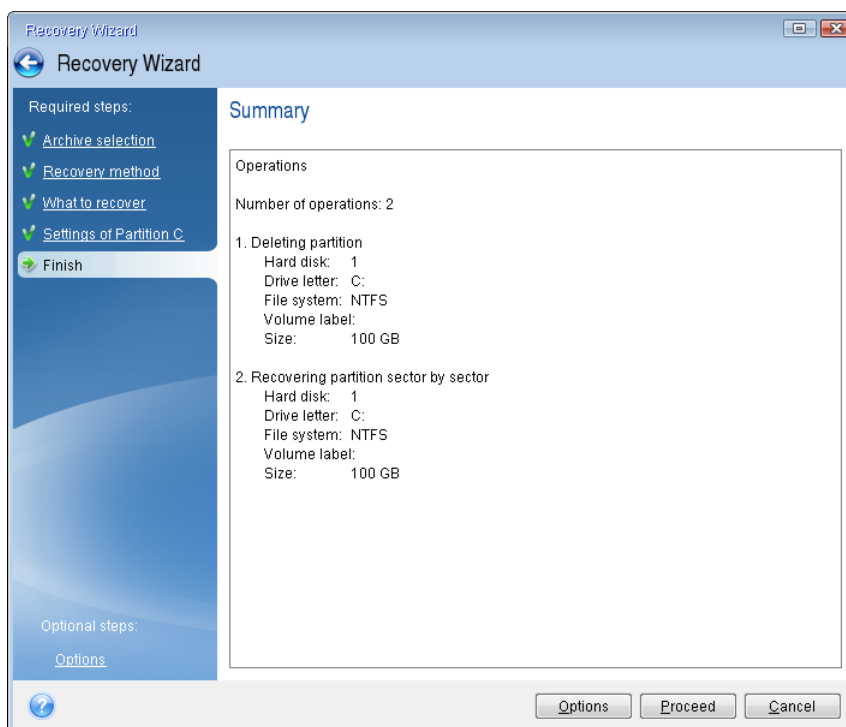


7. Select the system partition (usually C) on the **What to recover** screen. If the system partition has a different letter, select the partition using the **Flags** column. It must have the **Pri, Act** flags.

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



- At the "Settings of partition C" (or the letter of the system partition, if it is different) step check the default settings and click **Next** if they are correct. Otherwise, change the settings as required before clicking **Next**. Changing the settings will be needed when recovering to the new hard disk of a different capacity.
- Carefully read the summary of operations at the **Finish** step. If you have not resized the partition, the sizes in the **Deleting partition** and **Recovering partition** items must match. Having checked the summary click **Proceed**.



10. When the operation finishes, exit the standalone version of Acronis True Image 2015, remove the rescue media and boot from the recovered system partition. After making sure that you have recovered Windows to the state you need, restore the original boot order.

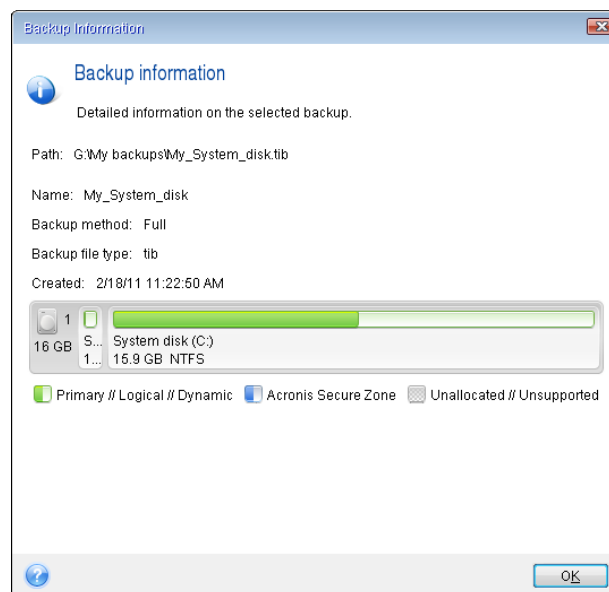
Recovering your system to a new disk under bootable media

Before you start, we recommend that you complete the preparations described in Preparing for recovery (p. 61). You do not need to format the new disk, as this will be done in the process of recovery.

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

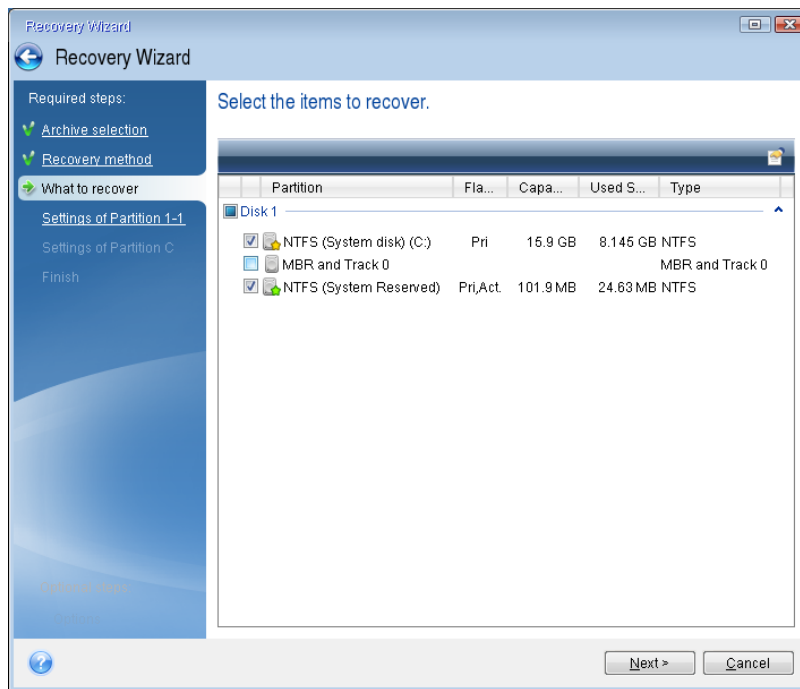
To recover your system to a new disk:

1. Install the new hard drive to the same position in the computer and use the same cable and connector that was used for the original drive. If this is not possible, install the new drive to where it will be used.
2. Attach the external drive if it contains the backup to be used for recovery and make sure that the drive is powered on.
3. Arrange the boot order in BIOS so as to make your rescue media device (CD, DVD or USB stick) the first boot device. See Arranging boot order in BIOS (p. 74).
4. Boot from the rescue media and select **True Image**.
5. On the **Home** screen, select **My disks** below **Recover**.
6. Select the system disk or partition backup to be used for recovery. When the backup is not displayed, click **Browse** and specify path to the backup manually.
7. If you have a hidden partition (for example, the System Reserved partition or a partition created by the PC manufacturer), click **Details** on the wizard's toolbar. Please remember the location and size of the hidden partition, because these parameters need to be the same on your new disk.



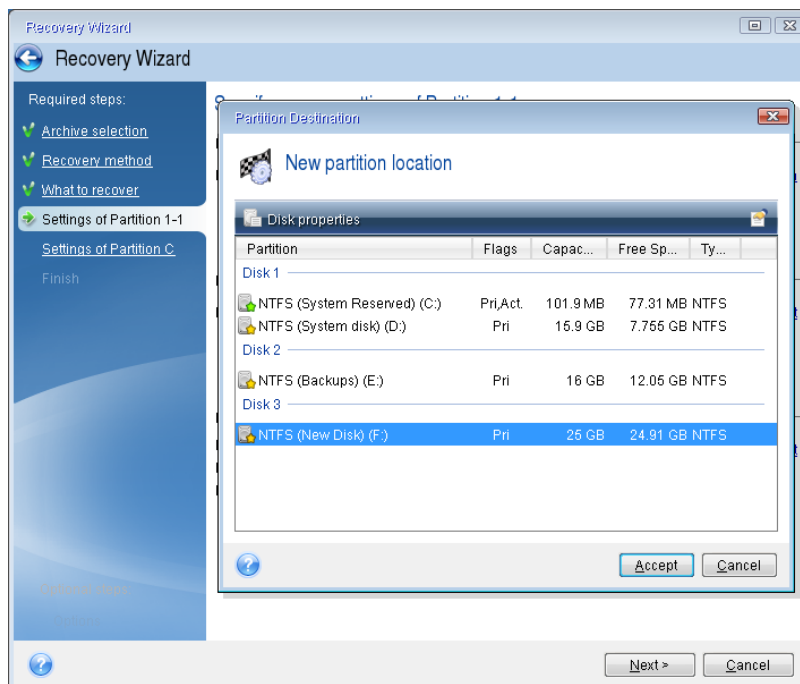
8. Select **Recover whole disks and partitions** at the **Recovery method** step.

9. On the **What to recover** step, select the boxes of the partitions to be recovered. Do not select the **MBR and Track 0** box.

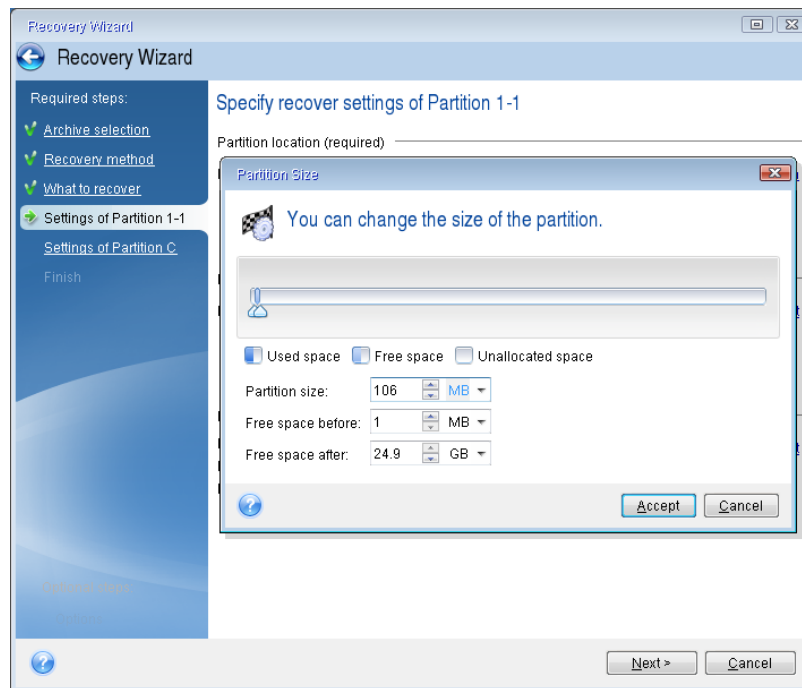


Selecting partitions leads to appearance of the relevant steps "Settings of partition ...". Note that these steps start with partitions which do not have an assigned disk letter (as usually is the case with hidden partitions). The partitions then take an ascending order of partition disk letters. This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

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

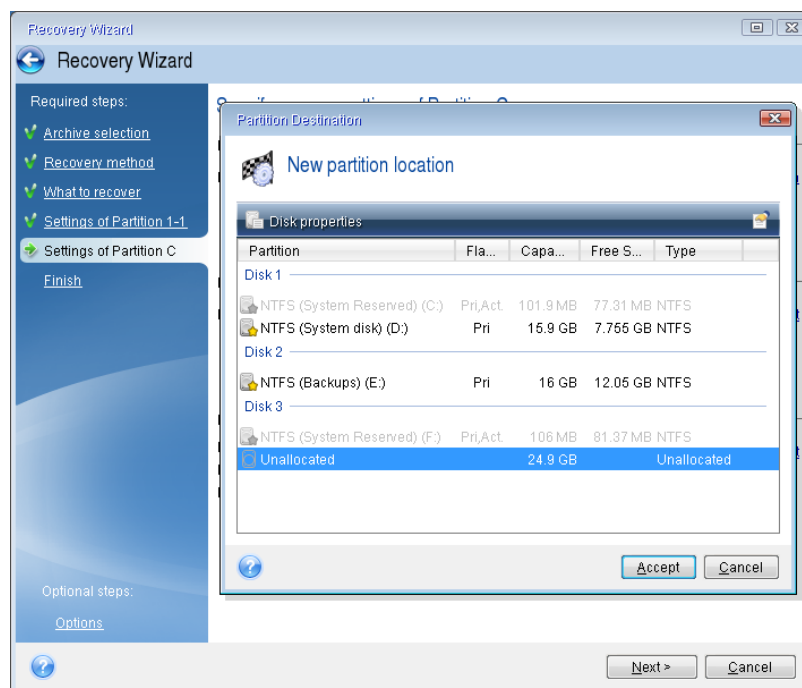


- **Type.** Check the partition type and change it, if necessary. Ensure that the System Reserved partition (if any) is primary and marked as active.
- **Size.** Click **Change default** in the Partition size area. By default the partition occupies the entire new disk. Enter the correct size in the Partition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



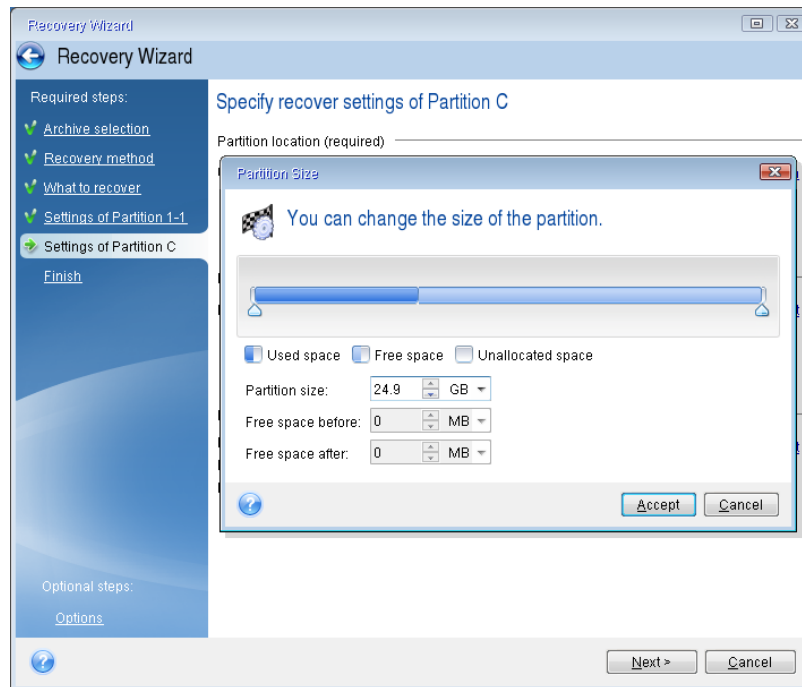
11. On the **Settings of Partition C** step, specify the settings for the second partition, which in this case is your system partition.

- Click **New location**, and then select unallocated space on the destination disk that will receive the partition.



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

- Specify the partition size, which by default equals the original size. Usually there is no free space after the partition, so allocate all the unallocated space on the new disk to the second partition. Click **Accept**, and then click **Next**.



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

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

- Select the same backup again. Right-click and select **Recover** in the shortcut menu. Choose **Recover whole disks and partitions** at the Recovery method step and then select the **MBR and Track 0** box.
- At the next step, select the destination disk as the target for MBR recovery, click **Next** and then **Proceed**. After MBR recovery is complete, exit the standalone version of Acronis True Image 2015.

When the recovery is complete

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

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

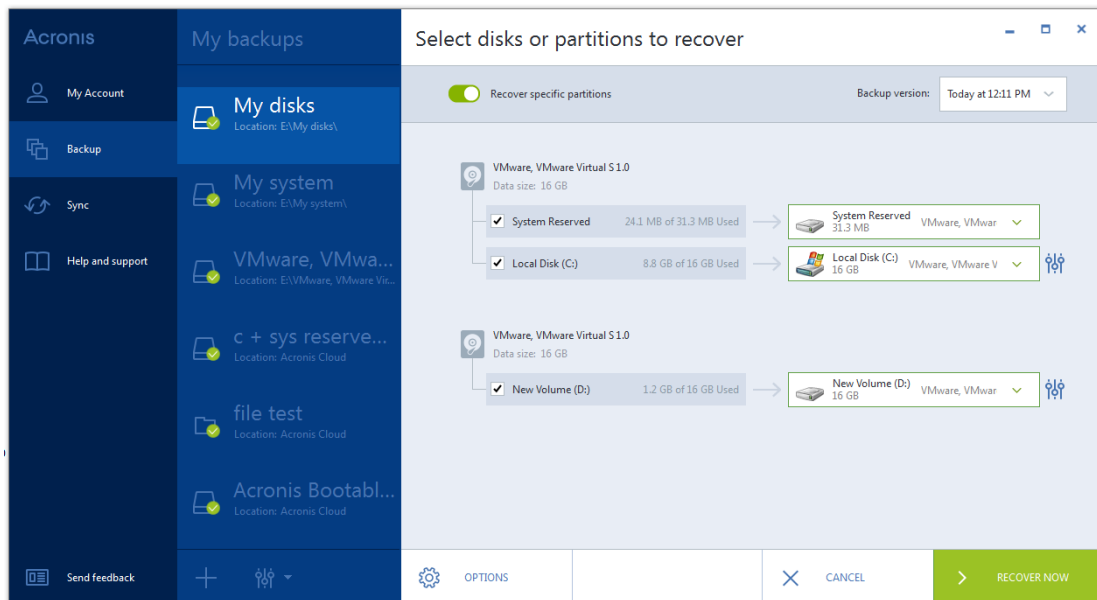
5.1.2 Recovering partitions and disks

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

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 2015.
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, 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 to recover.
If you need to recover separate partitions, click **Recover specific partitions**, and then select the partitions to recover.
6. In the recovery destination field below the partition name, select the destination partition. Unsuitable partitions are marked by red lettering. Note that all data on the destination partition will be lost because it is replaced by the recovered data and file system.

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

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

Do I need to recover MBR?

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

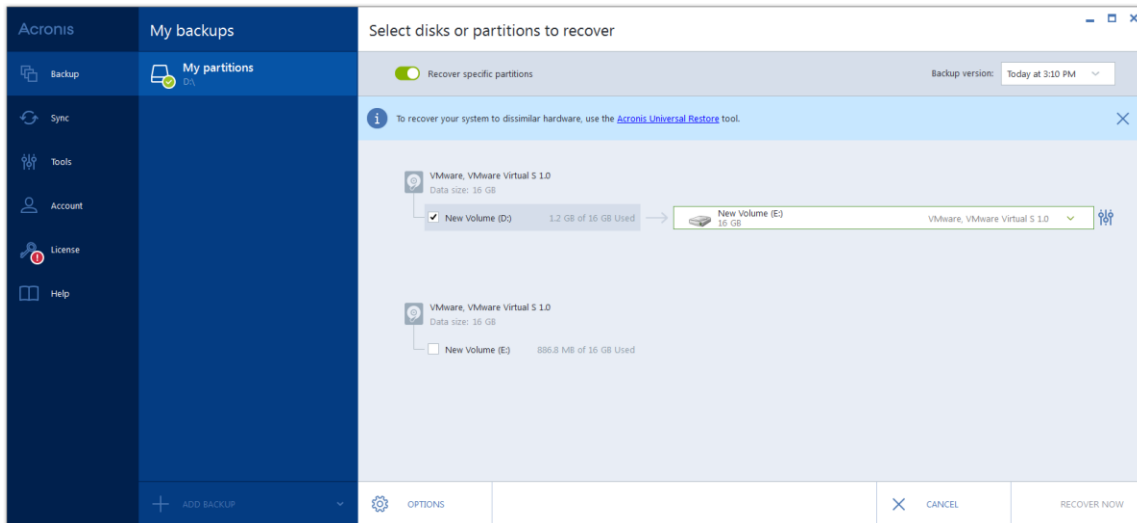
5.1.2.1 Recovering to a different partition or disk

Here we describe recovery of two partitions. If an image of a hard disk has more than two partitions, the procedure is similar.

The following procedure is valid only for recovery to a basic disk. Recovery to a dynamic disk with partition resizing is impossible.

1. Start Acronis True Image 2015.

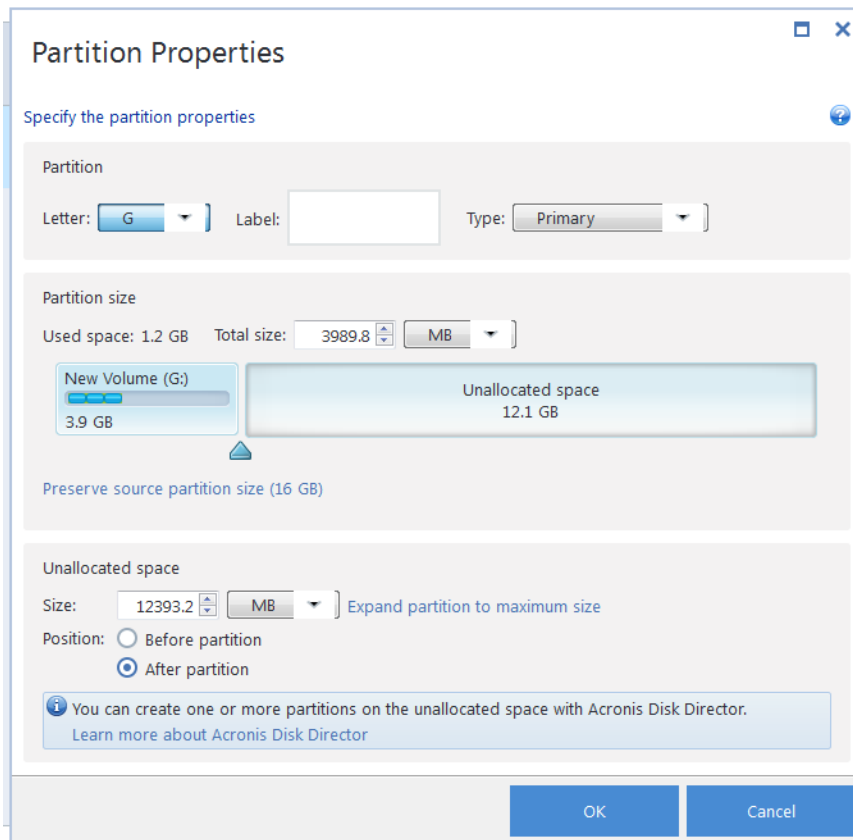
2. In the **Backup** section, select the backup which contains the partitions you want to recover, and then click **Recover disks**.
3. In the **Backup version** list, select the backup version you want to recover by its backup date and time.
4. Select a partition to recover. This opens the recovery destination field.



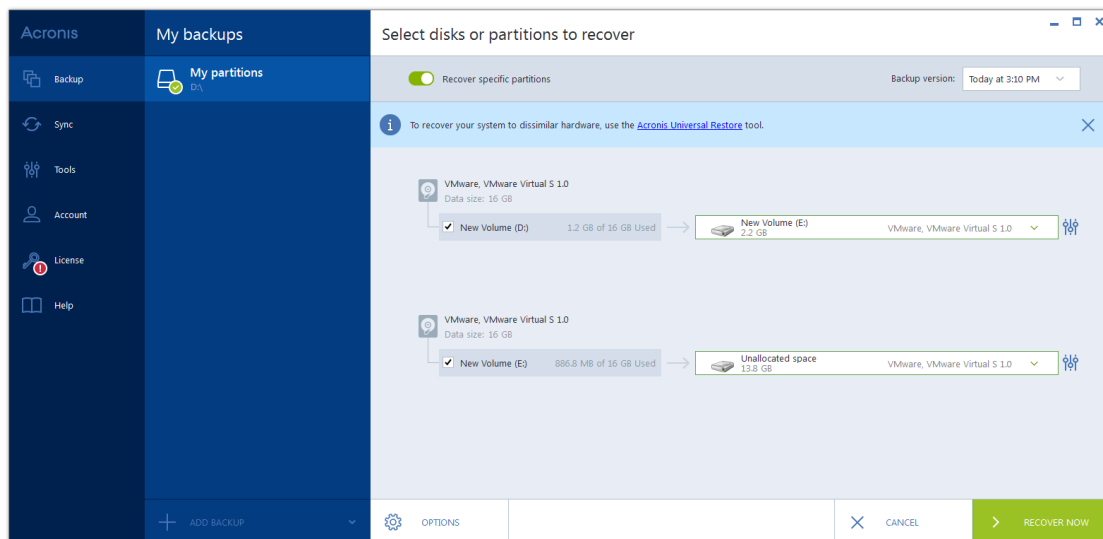
5. Click the down arrow to the right of the field and select the destination hard disk. The partition to be recovered is then placed on the selected hard disk. It occupies all the available disk space. To reduce the partition size so as to leave enough disk space for the remaining partition, click the **Partition properties** icon to the right of the recovery destination field. The **Partition Properties** window appears.
6. You can resize the partition by dragging its right border with a mouse on the horizontal bar on the screen.

*To assign the partition a specific size, enter the appropriate number into the **Total size** field.*

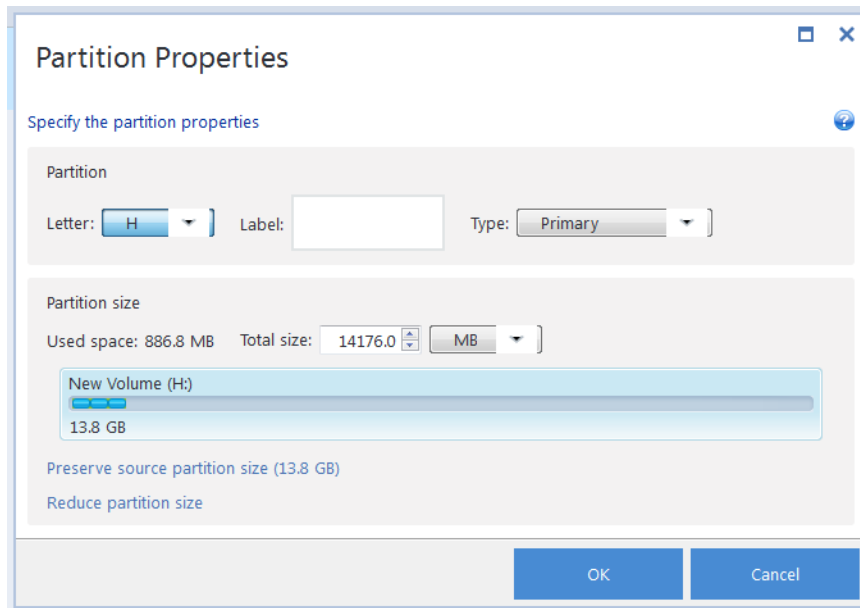
Remember that you need to leave as much unallocated (free) space after having resized the partition as will be needed for the remaining partition. Select a disk letter and partition type. When you finish the settings, click **OK** to confirm them and return to the main Disk Recovery window.



7. Select the next partition's check box.
8. Select the unallocated space on the destination hard disk. The program creates a partition occupying the entire unallocated space.



9. Click the **Partition properties** link and make the settings for the partition. Select a disk letter and partition type. When you finish the settings, click **OK** to confirm them and return to the main Disk Recovery window.



If the image contains more than two partitions, leave enough unallocated space for other partitions to be recovered and repeat steps 5-7 until you make the settings for all partitions.

10. Click **Recover now** to recover the partitions to the destination hard disk.

5.1.3 About recovery of dynamic/GPT disks and volumes

Recovery of dynamic volumes

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

- **Dynamic volume.**

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

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

The target volume type does not change.

- **Another dynamic disk or volume.**

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

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

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

- **Basic volume or disk.**

The target volume remains basic.

- **Bare-metal recovery.**

When performing a so called "bare-metal recovery" of dynamic volumes to a new unformatted disk, the recovered volumes become basic. If you want the recovered volumes to remain

dynamic, the target disks should be prepared as dynamic (partitioned and formatted). This can be done using third-party tools, for example, Windows Disk Management snap-in.

Recovery of basic volumes and disks

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

Partition style after recovery

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

	My system is BIOS-booted (Windows or Acronis Bootable Media)	My system is UEFI-booted (Windows or Acronis Bootable Media)
My source disk is MBR and my OS does not support UEFI	The operation will not affect neither partition layout nor bootability of the disk: partition style will remain MBR, the destination disk will be bootable in BIOS.	After operation completion, the partition style will be converted to GPT style, but the operating system will fail booting from UEFI, since your operating system does not support it.
My source disk is MBR and my OS supports UEFI	The operation will not affect neither partition layout nor bootability of the disk: partition style will remain MBR, the destination disk will be bootable in BIOS.	The destination partition will be converted to GPT style that will make the destination disk bootable in UEFI. See Example of recovery to UEFI system (p. 73).
My source disk is GPT and my OS supports UEFI	After operation completion, the partition style will remain GPT, the system will fail booting on BIOS, because your operating system cannot support booting from GPT on BIOS.	After operation completion, the partition style will remain GPT, the operating system will be bootable on UEFI.

Example of recovery procedure

See Example of recovery to a UEFI system (p. 73).

5.1.3.1 Example of recovery to a UEFI system

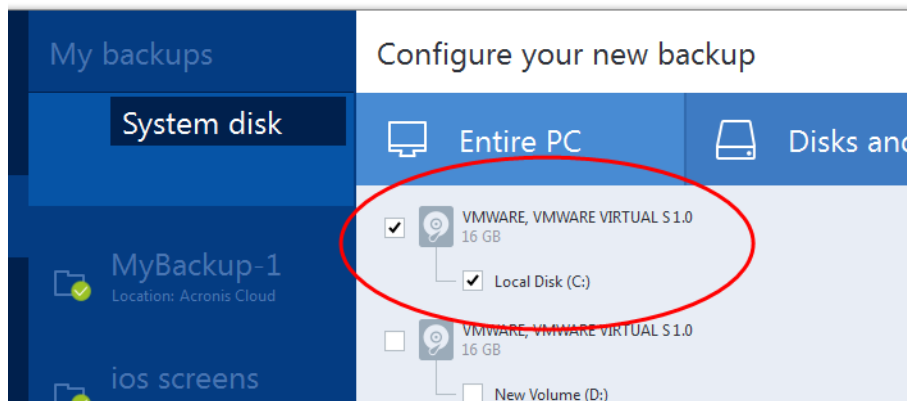
Here is an example for transferring a system with the following conditions:

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

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

- **Bootable rescue media.**
Refer to Creating bootable rescue media (p. 15) for details.
- **Backup of your system disk created in disk mode.**

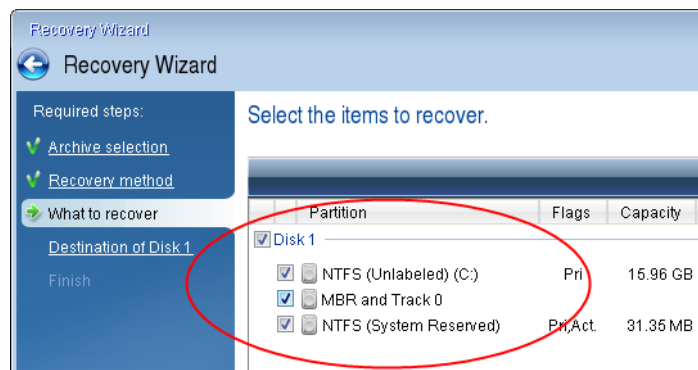
To create this backup, switch to disk mode, and then select the hard drive that contains your system partition. Refer to Backing up disks and partitions (p. 35) for details.



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

1. Boot from the rescue media in UEFI mode and select True Image.
2. Run the **Recovery wizard** and follow the instructions described in Recovering your system (p. 62).
3. On the **What to recover** step, select the check box next to the disk name to select the entire system disk.

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



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

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

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

5.1.4 Arranging boot order in BIOS

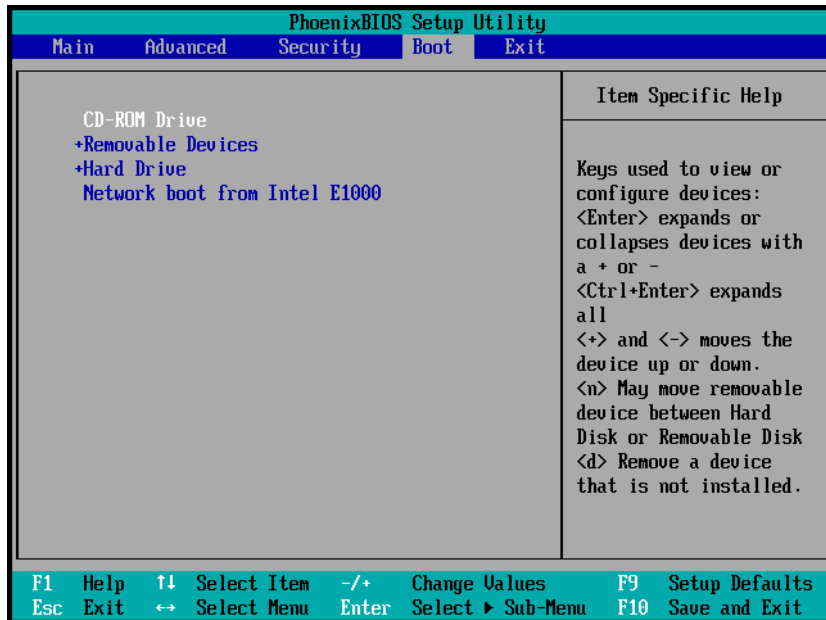
To boot your computer from Acronis bootable rescue media, you need to arrange boot order in BIOS so the media is the first booting device.

To boot from Acronis bootable media:

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

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

4. If you use a CD or DVD as a bootable media, insert it in the CD or DVD drive.
5. Make your rescue media (CD, DVD or USB drive) device the first booting device:
 1. Navigate to the Boot order setting by using the arrow keys on your keyboard.
 2. Place the pointer on the device of your bootable media and make it the first item in the list. You can usually use the Plus Sign and the Minus Sign keys to change the order.



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

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

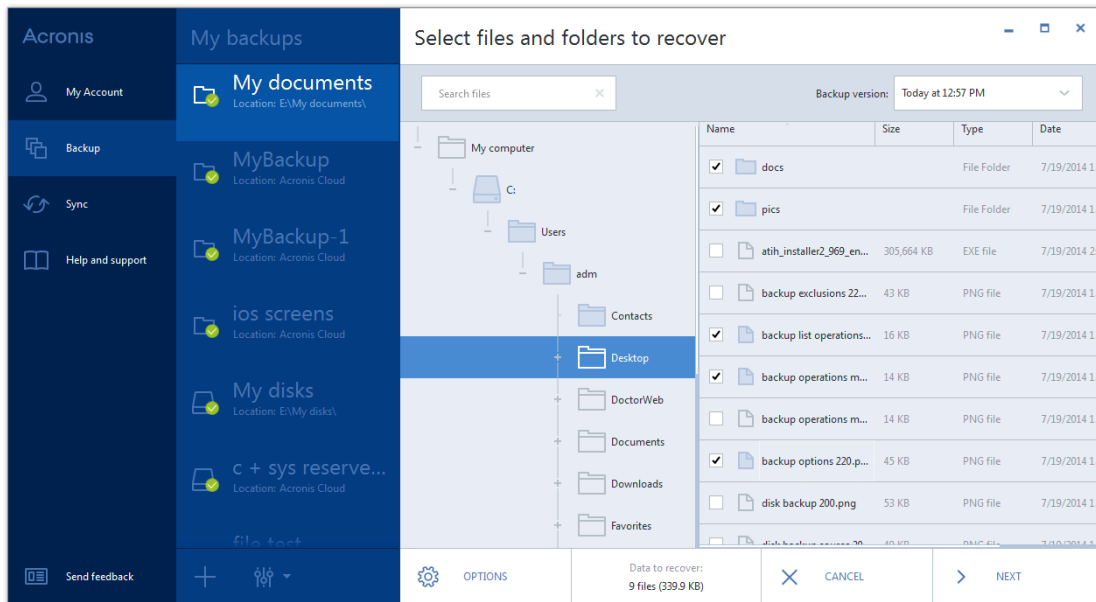
5.2 Recovering files and folders

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

To recover files and folders:

1. Start Acronis True Image 2015.
2. On the sidebar, click **Backup**.
3. From the backup list, select the backup which contains the files or folders that you want to recover.
4. On the right panel, click **Recover files**.
5. Select backup version (data state on specific date and time).

- Select the files and folders that you want to recover, and then click **Next**.



- Select a destination on your computer to where you want to recover selected files/folders. You can recover data to its original location or choose a new one, if necessary. To choose a new location, click the **Browse** button.
When you choose a new location, the selected items will be recovered by default without recovering the original, absolute path. You may also wish to recover the items with their entire folder hierarchy. In this case select the **Keep the original folder structure** check box.
- When needed, set the options for the recovery process (recovery process priority, file-level security settings, etc.). To set the options, click **Options**. The options you set here will be applied only to the current recovery operation.
- To start the recovery process, click the **Recover now** button.
You can stop the recovery by clicking **Cancel**. Please keep in mind that the aborted recovery may still cause changes in the destination folder.

Recovering files in Windows Explorer

To recover files and folders directly from Windows Explorer:

- Double-click the corresponding .tib 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.

5.3 Recovery from Acronis Cloud

In this section

Recovering data from online backups	77
Selecting a version to recover.....	77
Disk recovery from Cloud.....	78

5.3.1 Recovering data from online backups

With Acronis True Image 2015 you can browse and recover data that was backed up on Acronis Cloud. If you have backed up data from several computers, select the online backup box for the computer from which you backed up the data you want to recover.

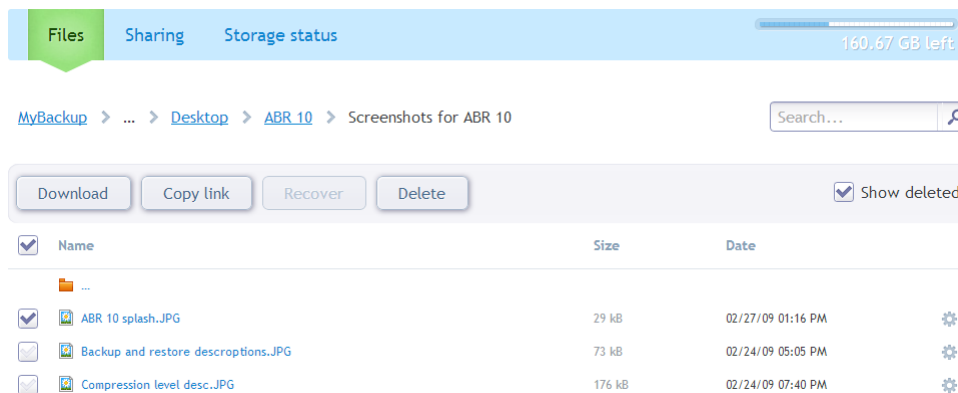
To recover files and folders from Acronis Cloud:

1. Start Acronis True Image 2015.
2. On the sidebar, click **Backup**.
3. From the backup list, select the backup which contains the files or folders that you want to recover.
4. On the right panel, click **Recover files**.

You will be taken to Acronis Cloud website.

If the data from the selected computer is stored on the Cloud in encrypted form, you will be asked to enter the encryption key which has been used for encryption. You will not be able to access the data until you enter the correct encryption key.

5. After the **Files** tab on the Acronis Cloud website opens, select the required online backup in the **Backups** area.
6. Select the files and folders you want to recover. Click the **Download** button to start recovery.



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

By default the data will be downloaded to the **Downloads** folder. You may change the download path.

5.3.2 Selecting a version to recover

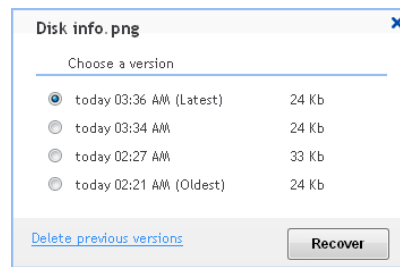
By default Acronis True Image 2015 selects the latest versions with respect to the date you specified. However, for any file you can select a specific version of the file to recover.

Note that this option is not applicable to folders.

To recover a specific file version:

1. In the backup contents, select the file which version you want to recover, then click the gear icon at the right-hand side. Select **View versions** in the opened menu.

2. In the window that appears, select the required version and then click **Recover**.



3. Select the version to which you want to rollback. The version's exact date and time will be displayed. Your current version will be reverted to the state it was at that point in time.
4. Click **Recover** to proceed. The selected version will become the latest version on Acronis Cloud.
5. After the process finishes, refresh the **Files** page in your web browser.
6. Select the file once more and then click **Download** to download the selected version to your Downloads folder.

5.3.3 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 2015, please refer to Recovering partitions and disks (p. 68).
- When Windows cannot start, please refer to Recovering your system from Acronis Cloud (p. 79).

How it works

Your computer should be connected to the Internet either by an Ethernet cable or via Wi-Fi. Acronis True Image 2015 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 2015 does not download the entire disk space to your computer. It 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. 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 2015 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 please run recovery again manually and make sure the recovery is complete.

Regardless of an interruption reason, Acronis True Image 2015 does not start recovery from the very beginning. It resumes the process and downloads only the data that was not recovered.

5.3.3.1 Recovering your system from Acronis Cloud

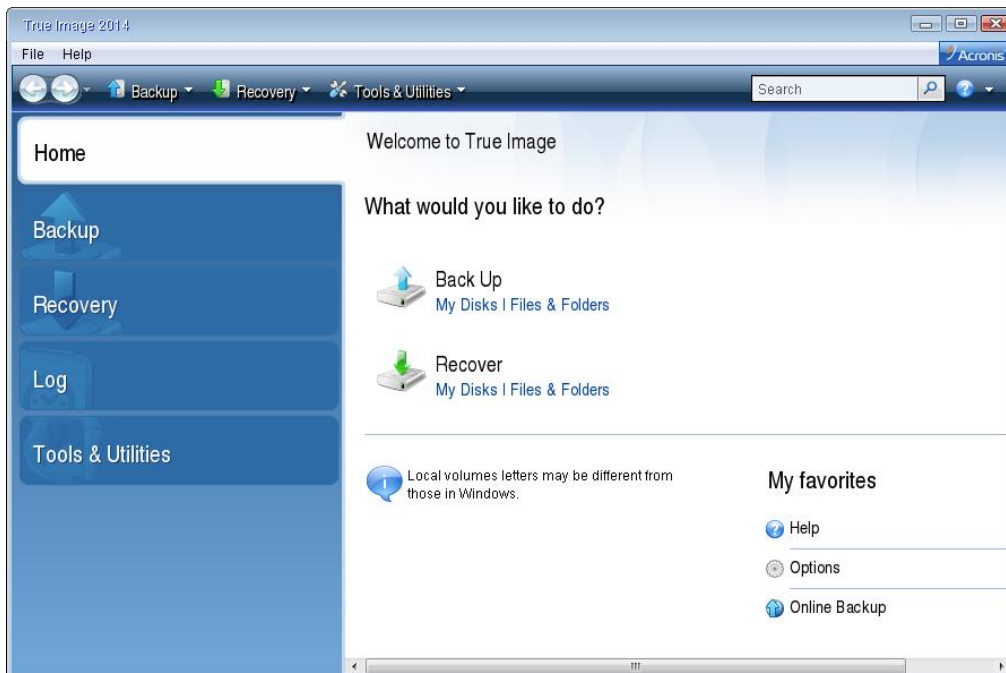
Depending on your Internet connection speed, disk recovery from Acronis Cloud may take a long time.

Before you start, we recommend that you complete the preparations described in Preparing for recovery (p. 61). 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, please make sure that your computer is connected to the Internet by an Ethernet cable or over Wi-Fi.

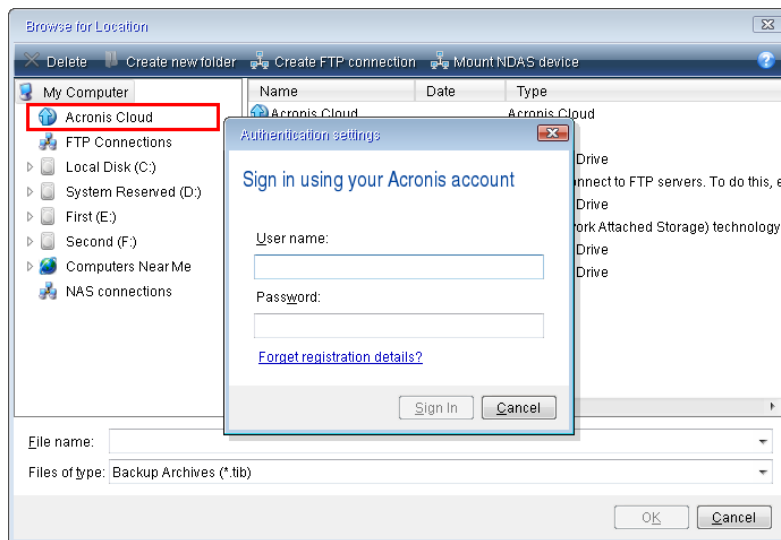
To recover a system disk from Acronis Cloud:

1. Arrange the boot order in BIOS so as to make your rescue media device (CD, DVD or USB stick) the first boot device. See Arranging boot order in BIOS (p. 74).
2. Boot from the rescue media and select **True Image**.
3. On the **Home** screen, select **My disks** below **Recover**.

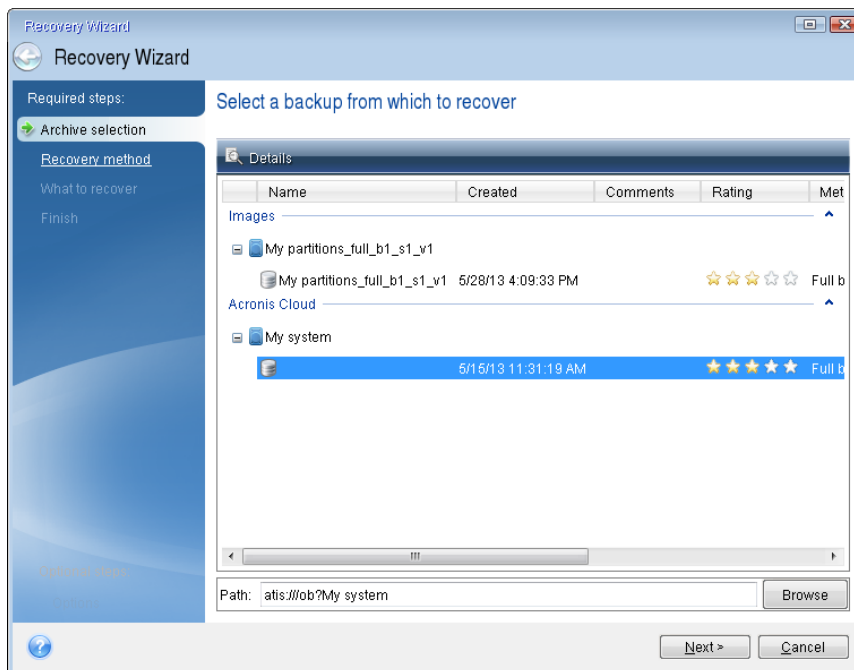


4. To add the online backup of the system disk or system partition to the list of available backups, click **Browse**.

- In the directory tree of the opened window, select Acronis Cloud and enter credentials of your Acronis account.

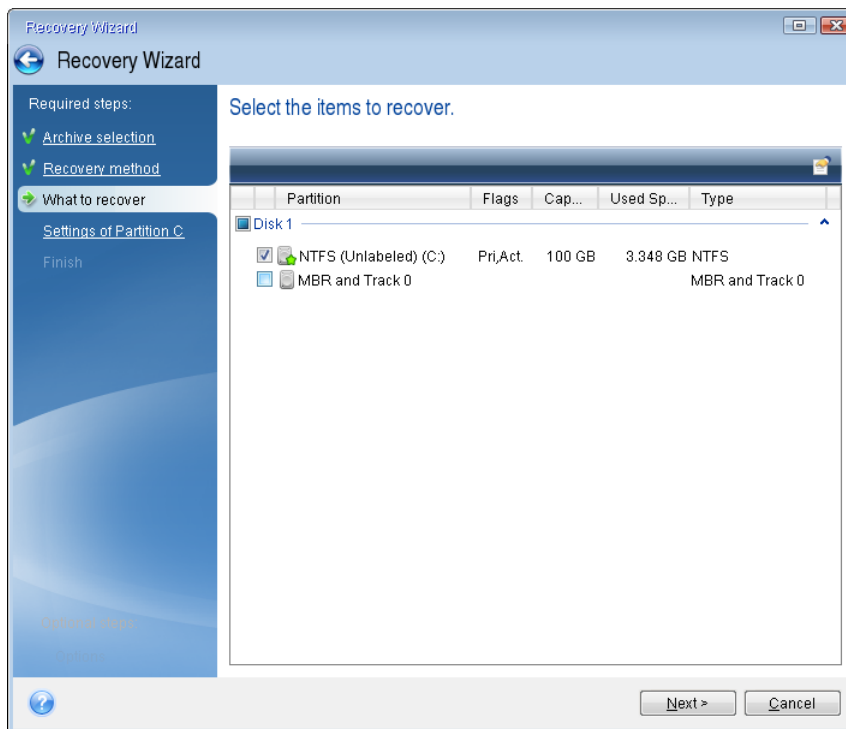


- Select the backup you want to use for recovery, and click **OK**.
- On the **Archive selection** step, select the online backup and click **Next**.



- On the **Recovery method** step, select **Recover whole disks and partitions**.

- 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.



- 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.
- 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**.
- When recovery is complete, exit the standalone version of Acronis True Image 2015, remove the rescue 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.

5.4 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.

In this section

Disk recovery mode	82
Pre/Post commands for recovery	82
Validation option.....	82
Computer restart	83
File recovery options.....	83

Overwrite file options	83
Performance of recovery operation	84
Notifications for recovery operation	84

5.4.1 Disk recovery mode

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

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

5.4.2 Pre/Post commands for recovery

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

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

To specify commands (batch files):

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

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

5.4.2.1 Edit user command for recovery

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

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

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

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

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

5.4.3 Validation option

- **Validate backup before recovery**—Enable this option to check the backup integrity before recovery.

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

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

The file system will not be checked if a reboot is required during recovery, for example, when recovering the system partition to its original place.

5.4.4 Computer restart

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

5.4.5 File recovery options

You can select the following file recovery options:

- **Recover files with their original security settings** - if the file security settings were preserved during backup (see File-level security settings for backup (p. 53)), you can choose whether to recover them or let the files inherit the security settings of the folder where they will be recovered to. This option is effective only when recovering files from file/folder backups.
- **Set current date and time for recovered files** - you can choose whether to recover the file date and time from the backup or assign the files the current date and time. By default the file date and time from the backup will be assigned.

5.4.6 Overwrite file options

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

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

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

If you do not need to overwrite some files:

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

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

5.4.7 Performance of recovery operation

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

Operation priority

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

You can set up the operation priority:

- **Low** (enabled by default) - the backup or recovery process will run slower, but the performance of other programs will be increased.
- **Normal** - the backup or recovery process will have the equal priority with other processes.
- **High** - the backup or recovery process will run faster, but the performance of other programs will be reduced. Be aware that selecting this option may result in 100% CPU usage by Acronis True Image 2015.

5.4.8 Notifications for recovery operation

Sometimes a backup or recovery procedure can last an hour or longer. Acronis True Image 2015 can notify you when it is finished via e-mail. The program can also duplicate messages issued during the operation or send you the full operation log after operation completion.

By default all notifications are disabled.

Free disk space threshold

You may want to be notified when the free space on the backup storage becomes less than the specified threshold value. If after starting a backup Acronis True Image 2015 finds out that the free space in the selected backup location is already less than the specified value, the program will not begin the actual backup process and will immediately inform you by displaying an appropriate message. The message offers you three choices - to ignore it and proceed with the backup, to browse for another location for the backup or to cancel the backup.

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

To set the free disk space threshold:

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

Acronis True Image 2015 can monitor free space on the following storage devices:

- Local hard drives

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

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

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

E-mail notification

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

To configure the email notifications:

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

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

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

Additional notification settings:

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

5.5 Restoring computer to factory settings

If your brand new computer was bundled with a backup of the computer's factory configuration, Acronis True Image 2015 can recover this backup and restore the computer to its factory settings. The system will be reverted to the state it was in when the computer was received from the store.

Caution: Restoration will erase all personal data and programs on the computer including all your backups in Acronis Secure Zone.

How to check if factory configuration can be restored on your computer

Acronis True Image 2015 offers three ways to restore a computer to factory settings:

- Directly in Windows by using the standard recovery feature of Acronis True Image 2015.
- When booting into Acronis Startup Recovery Manager.
- When booting from factory bootable media.

Recovery of the original configuration under Windows or by using Acronis Startup Recovery Manager is possible if the computer has an Acronis Secure Zone that has a backup of the computer's factory configuration. This backup is normally created and provided to Acronis Secure Zone by a hardware supplier who delivers computers to end-users.

When recovery is from factory bootable media, the media includes a backup with factory image configuration.

Restoring factory settings under Windows

In Windows, the factory configuration is restored by using the standard recovery feature of Acronis True Image 2015.

To restore the computer to factory settings:

1. Start Acronis True Image 2015.
2. Click the **Backup and recovery** tab.
3. In the list of backups, choose the backup named *Original configuration*.
4. Click **Recover**.
5. When prompted, click **Reboot**.

The operation will continue after the computer restart. Once the operation is complete, the computer will load the original Windows installation.

Restoring factory settings using Acronis Startup Recovery Manager

To restore the computer to factory settings:

1. Power on the computer.
2. When prompted, press **F11** to run Acronis Startup Recovery Manager.
3. Select **Recover**.

If the backup consists of several versions, select the version that you want to recover.

4. Confirm the operation by clicking **Yes**.

Once the operation is complete, the computer will be restarted or powered off. At the next computer boot up, it will load the original Windows installation.

Restoring factory settings from factory bootable media

These instructions apply to factory bootable media that you either created yourself or received from your hardware supplier together with your brand new computer.

For instructions on how to create factory bootable media, see *Creating factory bootable media* (p. 115).

To restore the computer to factory settings:

1. Boot up the computer using the factory bootable media.
2. Select **Recover**.
3. Confirm the operation by clicking **Yes**.

Once the operation is complete, the computer will be restarted or powered off. At next computer boot up, it will load the original Windows installation.

6 Synchronizing data

In this section

About the Sync feature	88
How we ensure security of your data	88
What you can and cannot synchronize	88
Sync icons	89
Sync creation	90
What is True Image for mobile devices?	91
Versions of synchronized files	92
How to clean up your space on Acronis Cloud	93
How to recover a deleted file	94
How to unlink a device from your account	95

6.1 About the Sync feature

The main highlights of the Sync feature:

- An Acronis Cloud subscription is required to use the Sync feature. Refer to Subscription information (p. 20) for details.
- You can have the same data - documents, photos, videos, etc. - on all of your computers and mobile devices with iOS and Android operating systems. Your data is within easy reach anywhere and anytime. No more emailing files to yourself or carrying an USB drive all the time.
- You can create as many syncs as you need.
- The Acronis Cloud keeps your synced files and versions of those files. This lets you roll back to a previous file version whenever you need it.
- You can access files in the Acronis Cloud from all your computers and mobile devices.
- You can also access the Cloud using a web browser, without having to install our application.

6.2 How we ensure security of your data

You may 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 synced 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 synced data, sign in to your account by providing the e-mail address and password for that account.

Furthermore, we store your data on our servers in encrypted form. Only you have access to your encrypted data.

6.3 What you can and cannot synchronize

You can synchronize data stored in two or more folders. Let's consider where these folders may be located and what data they may contain.

Storage types

A synchronization process may be established between:

- Two or more folders on two or more computers.
- One or more computers and Acronis Cloud.
Acronis Cloud always contains the last versions of the synced files. At the same time you cannot select a folder on Acronis Cloud to participate in a sync, such folder is created automatically.
- A mobile device and Acronis Cloud. See details in What is True Image for mobile devices (p. 91).

Within one sync process you may assign only one sync folder on every computer.

You cannot select for synchronization a single file. To synchronize the file, select for synchronization the folder that contains that file.

Data types

You can synchronize the following data:

- Files (your photos, music, videos, documents, etc.), except those listed below
Only the native FAT32 and NTFS file attributes are synchronized. If the synced folders belong to different file systems, the program synchronizes only the attributes supported by the both file systems.
- Other folders inside the sync folder (that is, sync subfolders) and their content

You cannot synchronize the following data:

- Disks and partitions
- System files and folders
- Hidden files and folders
- Temporary files and folders
- System registry
- Databases
- Data of e-mail programs (including Microsoft Outlook and others)
- Other data that cannot be represented as separate files or folders (for example, contacts from your address book)
- Windows 7 and Windows 8 libraries (Documents, Music, etc.)




6.4 Sync icons


While working with syncs you will see special icons. The icons give you the following information:

- Type and current state of your syncs (the icons are shown on sync boxes and in the notification area).
- Current state of synced files and folders (the icons are shown in Windows Explorer).

Sync boxes




Sync state icons:

-  The last synchronization completed successfully.
-  The sync is in progress at the moment.
-  The sync is paused.

-  An error occurred during the last synchronization.





Windows Explorer

Sync state icons for files and folders:

-  The file or folder is synchronized.
-  The file or folder is being synced at the moment.
-  The file or folder has not been synchronized because of an error.

The notification area

Sync state icons:

-  The last synchronization completed successfully.
-  (rotating) The sync is in progress at the moment.
-  (static) All syncs are paused or each sync has only one participant.
-  An error occurred during the last synchronization.

6.5 Sync creation

Before you begin a new sync creation, please make sure that the following conditions are met:

- You have an Acronis account and a subscription to the Acronis Cloud service. Refer to Subscription information (p. 20) for details.
- True Image Home 2012 or later version is installed on every computer.
- If you connect your computers through a local area network, make sure that local connection is established.
- Every computer has connection to the Internet.

To sync files and folders:

1. On the sidebar, click **Sync**.
2. If you are not signed in, enter your Acronis account credentials.
3. Perform one of the following:
 - If this is your first sync, click **Start**, and then select the folder that you want to synchronize. True Image will start synchronizing with Acronis Cloud. This is your default sync. Refer to Default sync (p. 90) for details.
 - For the second and later syncs, you first need to decide if you want to include Acronis Cloud in your new sync. Choose the appropriate sync type, and then select the folder that you want to synchronize.
4. To join this sync, start Acronis True Image 2015 on your other computers, select this sync in the Sync section, click **Join sync**, and then select the folder that you want to synchronize.

6.5.1 Default sync

When you start using the Sync feature, your first sync is always the default one.

This sync has the following main features:

- The default sync always syncs with the Acronis Cloud. You cannot unsync the storage.
- It also always stores file versions on the Acronis Cloud.
- As long as Acronis True Image 2015 is installed, you cannot delete the default sync folder. If you delete the folder, for example, using Windows Explorer, it will be recreated during the next program start.
- The contents of the default sync folder automatically sync with the default sync folders on other computers registered under the same Acronis account.
- It also automatically syncs with your mobile devices that have True Image app installed.

Using the default sync is the easiest way to sync your data. If needed, you can also create other syncs.

6.6 What is True Image for mobile devices?

Acronis Cloud might be unavailable in your region. For more information, click here:
<http://kb.acronis.com/content/4541>

This section contains short information about True Image mobile app. Please refer to True Image mobile app user guide for details. You can download it from the Acronis website:
http://download.acronis.com/pdf/ATIM_userguide_en-US.pdf.

True Image for mobile devices allows you to access data you stored on Acronis Cloud, and sync this data with your other mobile devices and computers. Note that True Image for mobile devices is useless without Acronis Cloud, so you need to subscribe to the service first.

Which devices does the mobile app support?

You can install True Image on any mobile devices that have iOS (iPhone, iPad, iPod) and Android (mobile phones and tablets) operating systems.

Key features

True Image for mobile devices allows you to:

- Get access to your Acronis Cloud
- Sync Gallery (in Android) and Camera Roll (in iOS) across devices
- Add files to Favorites (in Android) or Pinned (in iOS) to keep them up-to-date and get offline access
- Share files with your friends by using public links
- Upload both newly created photos, videos, etc. and existing files from your SD card to Acronis Cloud

Where can I get these apps?

You can view additional information and download True Image for mobile devices from App Store or Google Play:

- True Image for iOS devices: <https://itunes.apple.com/us/app/true-image/id486764267?mt=8>
- True Image for Android devices:
<https://play.google.com/store/apps/details?id=com.acronis.acronis>

How much does the mobile app cost?

True Image for mobile devices is available for free.

6.6.1 How to install True Image app on your mobile device

To sync with your mobile device, you need to install the appropriate True Image app.

Depending on your mobile device, go to App Store or Google Play and search for the Acronis True Image app.

For example, to find and install True Image app for iOS:

1. On your iPhone, open **App Store**.
2. Tap the Search icon.
3. Enter **acronis** in the search field.
4. Select **acronis true image** in the search results to go to the app page.
5. Follow the standard installation procedure.

The procedure to find and install the Android app is similar.

6.6.2 Synchronizing a mobile device

Your mobile device automatically syncs your data in the default sync with Acronis Cloud and with all computers where you have installed Acronis True Image 2015. See details in Default sync (p. 90).

To start syncing:

1. Install Acronis True Image app. See How to install True Image app on your mobile device (p. 92).
2. Open the app.
3. Type in the email and password for your account.
4. Tap **Sign in**.

Once you sign in, your device automatically starts syncing.

If you do not change the default settings, subsequent signing in and syncing will proceed automatically.

6.7 Versions of synchronized files

Acronis True Image 2015 gives you an opportunity to undo the changes that were made to your files as a result of synchronization. If you find that one of your files contains an undesirable change, you can view previous versions of this file and then choose and rollback to its correct version. See details in Reverting to a previous file version (p. 93).

All versions are stored on the Acronis Cloud which is accessible via the Internet. To use the Acronis Cloud, you must have a subscription to the Acronis Cloud service. If you do not have a subscription, a trial subscription with unlimited storage space will be automatically provided. See details in Subscription information (p. 20).

To delete obsolete versions, run the cleanup operation in the Acronis Cloud web application. See details in How to clean up your space on Acronis Cloud (p. 93).

If you use a trial version of Acronis True Image 2015, all stored versions, including the latest one, are deleted from the Cloud when the trial period expires.

6.7.1 Reverting to a previous file version

If you store sync history on the Acronis Cloud, you can revert the current version of a synchronized file to its previous version. This is useful when you want to undo some undesirable sync operation.

To revert to a previous file version:

1. In the **Sync** section, find the sync box with the needed file. Then click the **Acronis Cloud** link.
2. After the list of sync items opens in your Web browser, select the file which you want to revert to a previous version. Then click the gear icon at the right-hand side. Select **View versions** in the opened menu.
3. Select the version to which you want to rollback. The version's exact date and time will be displayed. Your current version will be reverted to the state it was at that point in time.
4. Click **Recover** to proceed. The selected version will become the latest version on the Cloud. Then, it will be downloaded to the computer that owns the sync.

6.8 How to clean up your space on Acronis Cloud

You can clean up your Acronis Cloud space to free it up for fresher data.

To clean up the Acronis Cloud space:

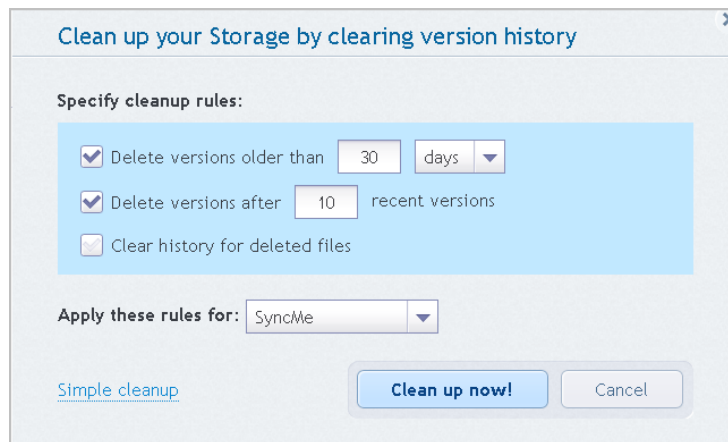
1. On the sidebar, click **Sync**, select the default sync, and then click the **Acronis Cloud** link. The Acronis Cloud web application opens.
2. On the **Storage status** tab, click **Clean up space**.
3. When the appropriate dialog appears, choose which versions you want to delete:
 - All versions.
 - Versions older than one month.
 - Versions older than one week.

The program shows how much space will be freed up.



Be careful! Deleted versions cannot be restored.

4. Clicking **Advanced cleanup** allows you to select more cleanup rules.



You can apply the cleanup rules for:

- individual syncs and online backups
- all syncs and online backups you have on Acronis Cloud

5. Choose the desired rules and click **Clean up now!**.

One more way to clean up is to delete a sync or online backup which you no longer need. In this case, all version history for the sync or online backup is deleted from Acronis Cloud.

6.9 How to recover a deleted file

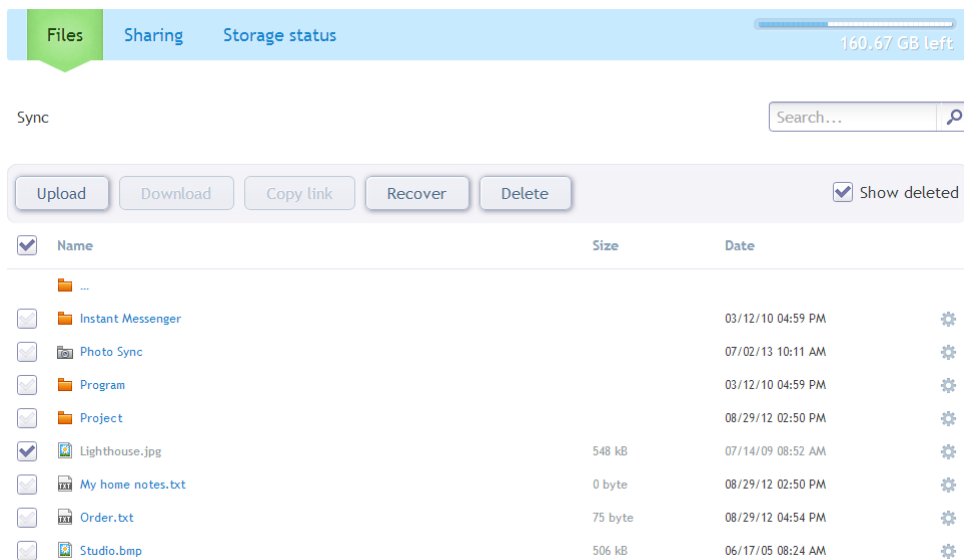
Sometimes you may delete a file from a sync by mistake. Then, you need to recover the deleted file. This may be possible for the syncs that keep file versions on Acronis Cloud.

One condition - the deleted file must not be removed during Cloud clean-up.

To recover a deleted file:

1. Start Acronis True Image 2015.
2. On the sidebar, click **Sync**, select the sync that contains the file to recover, and then click the **Acronis Cloud** link.
3. Click the **Files** tab and then select the sync from which you deleted the file.
4. After you select the sync, a list of files and folders appears.

- Select the **Show deleted** check box and then select the deleted file you want to recover.



- Click the **Recover** button to recover the deleted file to its folder.

6.10 How to unlink a device from your account

Sometimes you may need to unlink one of your computers or mobile devices from your account. For example, when a computer fails or gets stolen.

To unlink a device:

Go to your Acronis account page at <http://www.acronis.com/my/index.html>.

- Log in to your account.
- Click **Synchronization** in the left-hand side of the screen. The **Computers** tab in the Manage synchronization area is displayed by default.



3. Click **Unlink** to the right of the name of the computer you want to unlink.
4. Click **OK** in the confirmation message.

Unlinking the computer:

- Removes it from the Computers list.
- Removes it from all syncs in which the computer participates.
- Blocks the sync participant certificate.

7 Disk cloning and migration

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

- Use the Clone disk utility (p. 97).
- Back up your old disk drive, and then recover it to the new one (p. 65).

In this section

Disk cloning utility97


Migrating your system from an HDD to an SSD102


7.1 Disk cloning utility

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

Please read 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.

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

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

- On program screens, damaged partitions are marked with a red circle and a white cross inside in the upper left corner. Before you start cloning, you should check such disks for errors and correct the errors using the appropriate operating system tools.
- We strongly recommend that you create a backup of the entire original disk as a safety precaution. It could be your data saver if something goes wrong with your original hard disk during cloning. For information on how to create such a backup see Backing up partitions and disks. After creating the backup, make sure that you validate it.

7.1.1 Clone Disk wizard

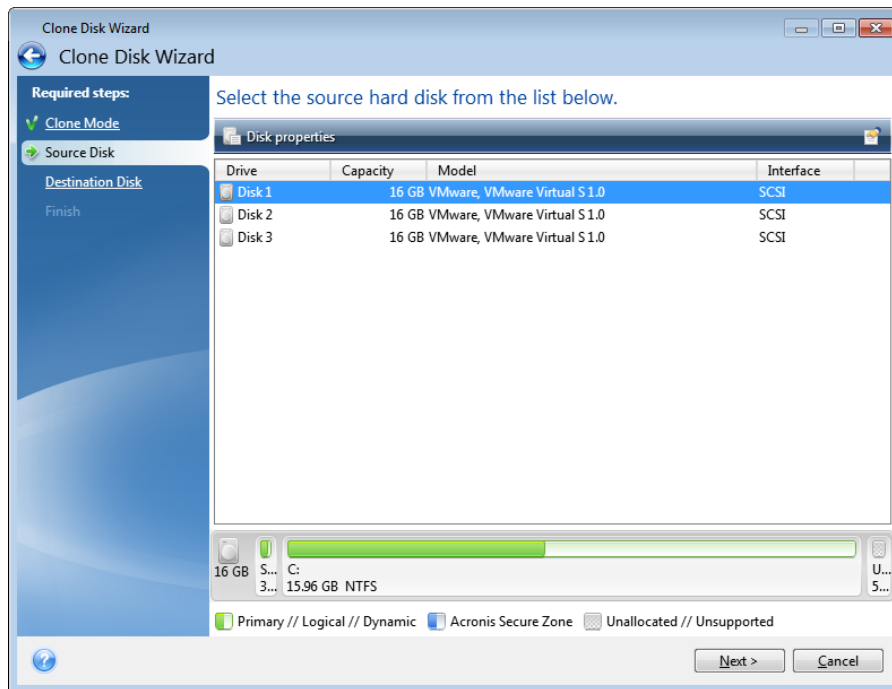
Before you start, we recommend that you read general information about Disk cloning utility (p. 97).

To clone a disk:

1. On the sidebar, click **Tools**, and then click **Clone disk**.
2. On the **Clone Mode** step, choose a transfer mode.
 - **Automatic**—Recommended in most cases.
 - **Manual**—Manual mode will provide more data transfer flexibility. Manual mode can be useful if you need to change the disk partition layout.

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

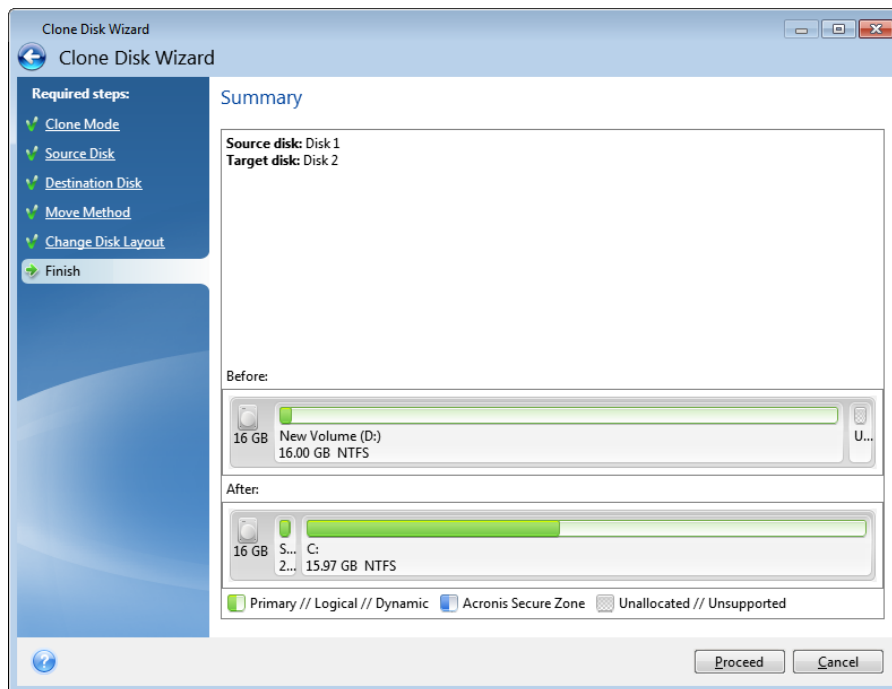
3. On the **Source Disk** step, select the disk that you want to clone.



Acronis True Image 2015 does not support cloning of dynamic disks.

4. On the **Destination Disk** step, select the destination disk for the cloned data.
If the selected destination disk contains partitions, you will need to confirm deletion of the partitions. Note that the real data destruction will be performed only when you click **Proceed** on the last step of the wizard.
If any disk is unpartitioned, the program will automatically recognize it as the destination and bypass this step.
5. [This step is only available in the manual cloning mode]. On the **Move method** step, choose a data move method.
 - **As is**—a new partition will be created for every old one with the same size and type, file system and label. The unused space will become unallocated.
 - **Proportional**—the new disk space will be proportionally distributed between cloned partitions.
 - **Manual**—you will specify a new size and other parameters yourself.
6. [This step is only available in the manual cloning mode]. On the **Change disk layout** step, you can edit settings of the partitions that will be created on the destination disk. Refer to Manual partitioning (p. 100) for details.
7. [Optional step] On the **What to exclude** step, you can specify files and folders that you do not want to clone. Refer to Excluding items from cloning (p. 101) for details.

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

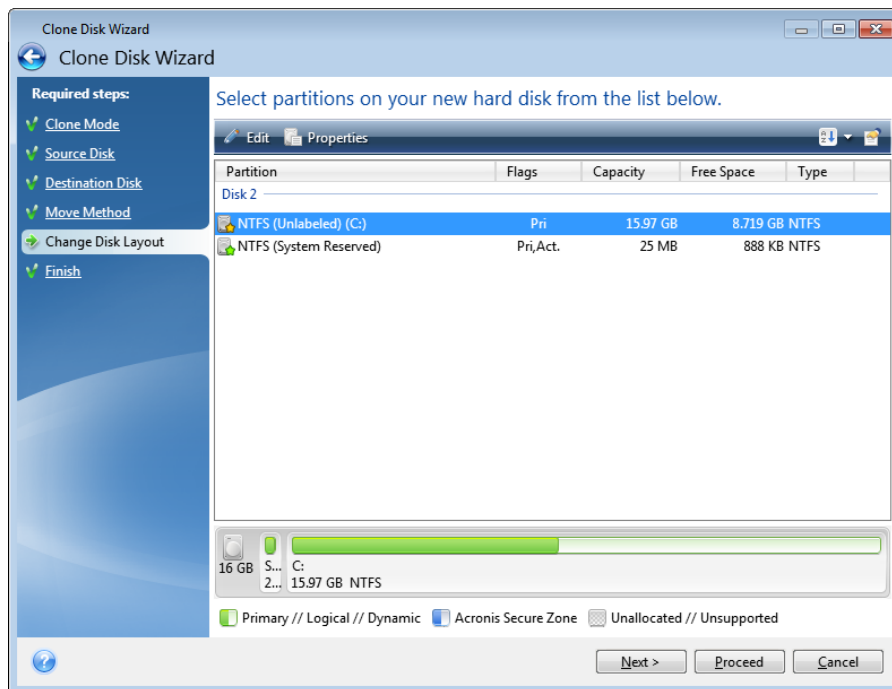


If the cloning operation is stopped for some reason, you will have to configure and start the procedure again. You will not lose your data, because True Image does not alter the original disk and data stored on it during cloning.

Cloning a disk containing the currently active operating system will require a reboot. In that case, after clicking **Proceed**, you will be asked to confirm the reboot. Canceling the reboot will cancel the entire procedure. By default, Acronis True Image 2015 shuts down the computer after the clone process finishes. This enables you to change the position of master/subordinate jumpers and remove one of the hard drives.

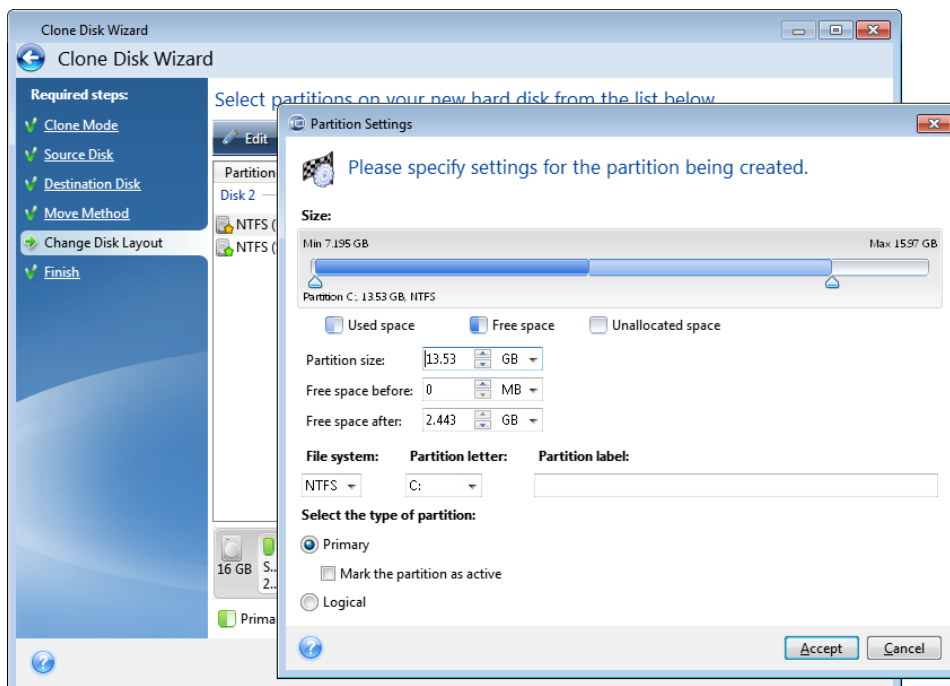
7.1.2 Manual partitioning

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



To edit a partition:

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




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

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

Refer to Partition settings (p. 123) for details.

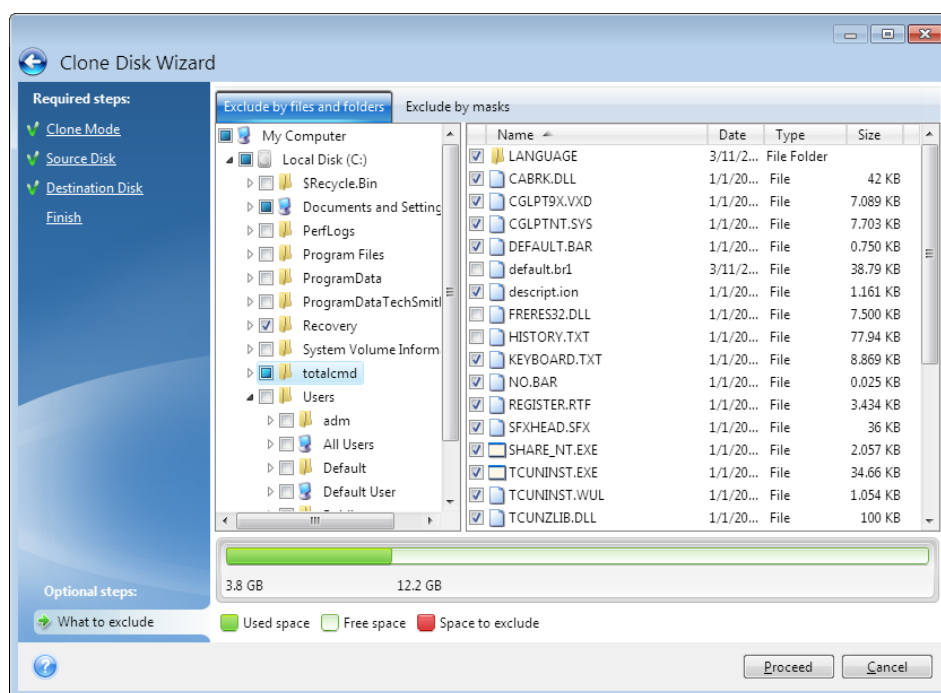
3. Click **Accept**.

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

7.1.3 Excluding items from cloning

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

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



You have two ways to exclude files and folders:

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

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

Examples of exclusion criteria:

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

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

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

7.2 Migrating your system from an HDD to an SSD

In this section

Preparing for migration.....	102
Migrating to SSD using the backup and recovery method	104

7.2.1 Preparing for migration

First of all, make sure that Acronis True Image 2015 detects your new SSD both in Windows and under the Acronis rescue media. If there is a problem, see [What to do if Acronis True Image 2015 does not recognize your SSD \(p. 102\)](#).

SSD size

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

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

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

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

Which migration method to choose

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

However, we recommend to use the backup and recovery method in most cases. This method provides more flexibility and control over migration. See [Migrating to an SSD using the backup and recovery method \(p. 104\)](#).

7.2.1.1 What to do if Acronis True Image 2015 does not recognize your SSD

Sometimes Acronis True Image 2015 may not recognize an SSD.

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

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

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

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

*For Windows XP, type **cmd** in the Run field and press **Enter**.*

At the command line prompt type:

diskpart

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

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

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

exit

exit

Start Acronis True Image 2015 and check whether it detects the SSD. If it detects the SSD, use the Add new disk tool to create a single partition on the disk occupying the entire disk space. When creating a partition, check that the free space before partition is 1 MB. For more information, see Adding a new hard disk (p. 120).

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

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

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

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

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

1. Shut down the computer.
2. Boot to BIOS, change the mode from AHCI to IDE (or ATA in some BIOS brands).
3. Boot from Acronis rescue media.
4. Recover or clone the disk.
5. Boot to BIOS and change IDE back to AHCI.
6. Start Windows.

What to do if the above suggestions do not help

You can try to create a WinPE-based rescue media. This may provide the necessary drivers. For more information, see Creating WinPE-based rescue media.

One more option is to request a custom rescue media from Acronis Support. For more information, see *Creating a custom rescue CD* (p. 139).

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

7.2.2 Migrating to SSD using the backup and recovery method

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

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

To migrate your system to an SSD:

1. Start Acronis True Image 2015.
2. Create Acronis rescue media, if you do not have it yet. To do this, in the **Tools** section, click **Create bootable media** and follow the instructions on the screen.
3. Back up your entire system drive (in the disk backup mode) to a hard disk other than your system hard disk and the SSD.
4. Switch off the computer and remove your system hard disk.
5. Mount the SSD into the slot where the hard disk was.

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

6. Boot from your Acronis rescue media.
7. Validate the backup to make sure that it can be used for recovery. To do this, click **Recovery** on the left pane and select the backup. Right-click, select **Validate Archive** in the shortcut menu and then click **Proceed**.
8. After the validation finishes, right-click the backup and select **Recover** in the shortcut menu.
9. Choose **Recover whole disks and partitions** at the Recovery method step and then click **Next**.
10. Select the system disk at the What to recover step.
11. Click **New location** and then select the SSD as the new location for your system disk, then click **Accept**.
12. At the next step click **Proceed** to start recovery.
13. After the recovery is complete, exit the standalone version of Acronis True Image 2015.
14. Try to boot from the SSD and then make sure that Windows and applications work correctly.

If your system hard disk also contains a hidden recovery or diagnostic partition, as is quite often the case with notebooks, the procedure will differ. You will usually need to resize the partitions manually during recovery to the SSD. For instructions see *Recovering a disk with a hidden partition* (p. 65).

8 Tools and utilities

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

Protection tools

- **Acronis Startup Recovery Manager**
Allows you to start Acronis True Image 2015 without loading the operating system by pressing F11 at boot time before the operating system starts.
- **Rescue Media Builder**
Allows you to create a bootable rescue media with Acronis products (or their specified components) installed on your computer.
- **Acronis Secure Zone**
Allows you to store your backups in a special safe partition on your disk.

Clone disk

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

Security and privacy

- **Acronis DriveCleanser**
Acronis DriveCleanser utility provides for secure destruction of data on your hard disk.
- **System Clean-up**
With the System Clean-up utility, you can clean up components (folders, files, registry sections, etc.), related to general system tasks. These Windows components retain evidence of user PC activity, so they too should be thoroughly wiped to maintain confidentiality.

Disk management

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

Image mounting

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

8.1 Creating bootable rescue media

You can run Acronis True Image 2015 from an emergency boot media on a bare-metal system or a crashed computer that cannot boot. You can even back up disks on a non-Windows computer, copying all its data into the backup by imaging the disk in the sector-by-sector mode. To do so, you

need bootable media that has a copy of the standalone Acronis True Image 2015 version installed on it.

How you can obtain bootable media:

- Use the installation CD of the boxed product.
- Make a media bootable with Acronis Media Builder:
 - Blank CD
 - Blank DVD
 - USB flash driveNote: The data it may contain will not be modified.
- Create an .iso image file to burn it afterwards onto a CD or DVD.
- Create WinPE-based media with Acronis plug-in.

8.1.1 Acronis Media Builder

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

You can create several types of bootable media:

- **Acronis bootable rescue media**
This type is recommended for most users.
- **WinPE-based media with Acronis plug-in**
Running Acronis True Image 2015 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 rescue media did not help you boot your computer.

To use this option, you need the following components to be installed:

- Acronis Media Add-on. You can download it from the Acronis website.
- One of the following:
 - Windows Automated Installation Kit (AIK).
This component is required for creating WinPE 3.0.
 - Windows Assessment and Deployment Kit (ADK).
This component is required for creating WinPE 4.0 and WinPE 5.0.
- **Acronis Universal Restore media**
If you recover your image on a computer with a dissimilar hardware configuration, the program may not be able to find some of the most critical device drivers in the default folders, especially when the target hardware has a specific mass storage controller (such as an SCSI, RAID, or Fibre Channel adapter) for the hard disk(s). Therefore Windows will not start.
Before you start the recovery to dissimilar hardware, please download the standalone Acronis Universal Restore tool from the Acronis website, and then create the rescue media. When the recovery is complete, use the media to restore the computer bootability. See details at: <https://kb.acronis.com/ati2015/aur>.

Notes

- We recommend that you create a new bootable media after each Acronis True Image 2015 upgrade.
- If you use non-optical media, the media must have FAT16 or FAT32 file system.
- Acronis Media Builder supports only x86 WinPE 3.0, WinPE 4.0 and WinPE 5.0. This WinPE distribution can also work on x64 hardware.
- A PE image based on WinPE 3.0 requires at least 256MB RAM to work, for WinPE 4.0 and WinPE 5.0 this requirement is 512 MB.
- If Acronis Media Builder does not recognize your USB flash drive, you can try using the procedure described in an Acronis Knowledge Base article at <http://kb.acronis.com/content/1526>.
- When booting from the Rescue Media, you cannot perform backups to disks or partitions with Ext2/Ext3/Ext4, ReiserFS, and Linux SWAP file systems.
- When booting from the rescue media and using a standalone version of Acronis True Image 2015 you cannot recover files and folders encrypted with use of the encryption available in Windows XP and later operating systems. For more information see File-level security settings for backup (p. 53). On the other hand, backups encrypted using the Acronis True Image 2015 encryption feature can be recovered.

8.1.1.1 Creating bootable media

To create bootable media:

1. Plug in a USB flash drive, or insert a blank CD or DVD.
2. Start Acronis True Image 2015.
3. In the **Tools** section, click **Rescue Media Builder**.
4. Choose a media type that you want to create. Refer to Acronis Media Builder for details.
5. Select a destination for the media:
 - **CD**
 - **DVD**
 - **USB flash drive** (available only for Acronis bootable rescue media)
If your drive has an unsupported file system, True Image will suggest formatting it to FAT file system.

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

 - **ISO image file**
You will need to specify the .iso file name and the destination folder.
When the .iso file is created, you can burn it onto a CD or DVD. For example, in Windows 7 and later, you can do this using a built-in burning tool. In Windows Explorer, double-click the created ISO image file, and then click **Burn**.
 - **WIM image file** (available only for WinPE-based media)
True Image adds the Acronis plug-in to the .wim file from Windows AIK or Windows ADK. You will need to specify a name for the new .wim file and the destination folder.
6. Click **Proceed**.

8.1.1.2 Bootable media startup parameters

Here, you can set bootable media startup parameters in order to configure rescue media boot options for better compatibility with different hardware. Several options are available (nousb,

nomouse, noapic, etc.). These parameters are provided for advanced users. If you encounter any hardware compatibility problems while testing boot from the rescue media, it may be best to contact Acronis Technical Support.

To add startup parameters:

- Enter a command into the **Parameters** field. You can type several commands, separated by spaces.
- Click **Next** to continue.

Additional parameters that can be applied prior to booting Linux kernel

Description

The following parameters can be used to load Linux kernel in a special mode:

- **acpi=off**

Disables ACPI and may help with a particular hardware configuration.

- **noapic**

Disables APIC (Advanced Programmable Interrupt Controller) and may help with a particular hardware configuration.

- **nousb**

Disables loading of USB modules.

- **nousb2**

Disables USB 2.0 support. USB 1.1 devices still work with this option. This option allows using some USB drives in USB 1.1 mode, if they do not work in USB 2.0 mode.

- **quiet**

This parameter is enabled by default and the startup messages are not displayed. Deleting it will result in the startup messages being displayed as the Linux kernel is loaded and the command shell being offered prior to running the Acronis program.

- **nodma**

Disables DMA for all IDE disk drives. Prevents kernel from freezing on some hardware.

- **nofw**

Disables FireWire (IEEE1394) support.

- **nopcmcia**

Disables PCMCIA hardware detection.

- **nomouse**

Disables mouse support.

- **[module name]=off**

Disables the module (e.g. **sata_sis=off**).

- **pci=bios**

Forces to use PCI BIOS, and not to access the hardware device directly. For instance, this parameter may be used if the machine has a non-standard PCI host bridge.

- **pci=nobios**

Disallows use of PCI BIOS; only direct hardware access methods are allowed. For instance, this parameter may be used if you experience crashes upon boot-up, probably caused by the BIOS.

- **pci=biosirq**

Uses PCI BIOS calls to get the interrupt routing table. These calls are known to be buggy on several machines and they hang the machine when used, but on other computers it is the only way to get the interrupt routing table. Try this option, if the kernel is unable to allocate IRQs or discover secondary PCI buses on your motherboard.

- **vga=ask**

Gets the list of the video modes available for your video card and allows selecting a video mode most suitable for the video card and monitor. Try this option, if the automatically selected video mode is unsuitable for your hardware.

8.1.1.3 Creating a custom WinPE 3.0 ISO with your drivers

Sometimes a basic WinPE disk with Acronis Plug-in does not have drivers for your specific hardware, for example, for storage device controllers. Users of Windows 7 can add such drivers to the basic WinPE 3.0 image (WIM) before creating an ISO file with Acronis Plug-in.

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 [http://technet.microsoft.com/en-us/library/dd799244\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd799244(WS.10).aspx)

To create a custom Windows PE image, proceed as follows:

1. In the **Start** menu, click **Microsoft Windows AIK**, then right-click **Deployment Tools Command Prompt** and 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 x86 C:\winpe_x86
```
3. Mount the base image by using the DISM tool to a local directory. For example,

```
Dism /Mount-Wim /WimFile:C:\winpe_x86\winpe.wim /index:1 /MountDir:C:\winpe_x86\mount
```
4. Add your hardware driver by using the Dism command with the /Add-Driver option. For example:

```
Dism /image:C:\winpe_x86\mount /Add-Driver /driver:C:\drivers\mydriver.inf
```
5. Repeat Step 4 for all other drivers you need to add.
6. Commit the changes using the Dism command with the /Unmount-Wim /Commit option.

```
Dism /Unmount-Wim /MountDir:C:\winpe_x86\mount /Commit
```

Do not exit the command prompt.

7. Start Acronis Media Builder and add Acronis plug-in to the custom .wim file. Refer to Creating bootable media (p. 107) for details.
8. Create a PE image (.iso file) from the resulting .wim file. Refer to Creating an .iso file from a .wim file for details.

8.1.1.4 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. Select **Microsoft Windows AIK** → **Windows PE Tools Command Prompt** from the **Start** menu.
Users of Windows 7 should select **Microsoft Windows AIK** → **Deployment Tools Command Prompt** from the **Start** menu.
If you create WinPE 4.0 ISO, select **Windows Kits** → **Windows ADK** → **Deployment and Imaging Tools Environment** from the **Start** menu.
2. Run the **copype.cmd** script to create a folder with Windows PE files. For example, from a command prompt, type:

```
copype x86 c:\winpe_x86
```
3. Replace the default boot.wim file in your Windows PE folder with the newly created .wim file (for example, AcronisMedia.wim). If the AcronisMedia.wim file is located on c:\, then:
For WinPE 3.0, type:

```
copy c:\AcronisMedia.wim c:\winpe_x86\ISO\sources\boot.wim
```


For WinPE 4.0 or WinPE 5.0, type:

```
copy "c:\AcronisMedia.wim" c:\winpe_x86\media\sources\boot.wim
```
4. Use the **Oscdimg** tool. To create an .iso file, type:

```
oscdimg -n -b c:\winpe_x86\etfsboot.com c:\winpe_x86\ISO  
c:\winpe_x86\winpe_x86.iso
```
5. Burn the .iso file to a CD using a third-party tool (for example, Nero) and you will have a bootable Windows PE disc with Acronis True Image 2015.

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

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

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

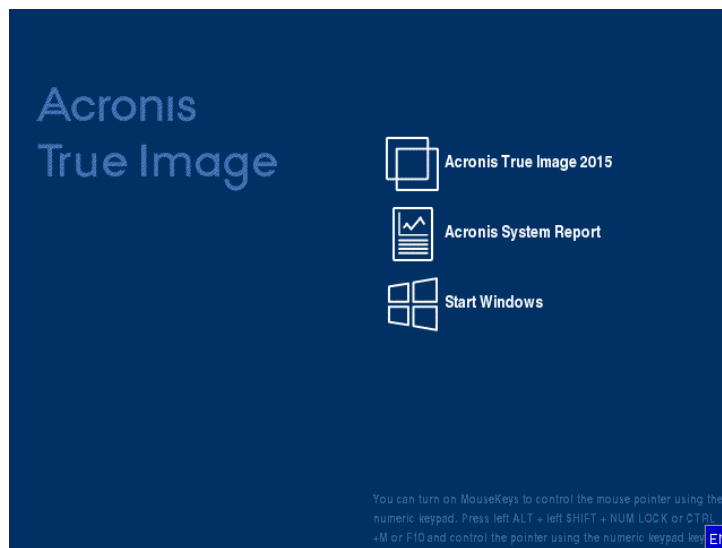
To test the rescue media

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

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

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

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



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

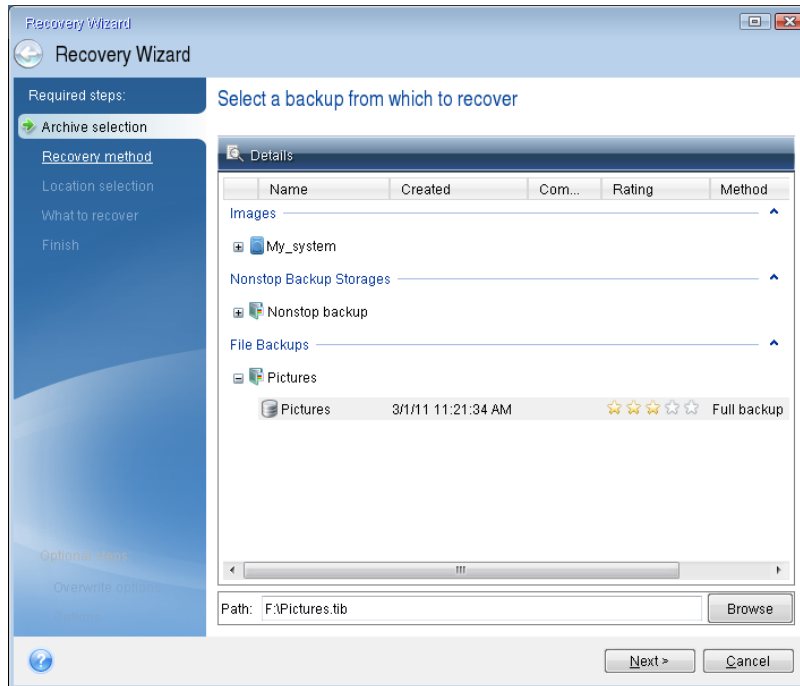
If you have a spare hard drive, we strongly recommend you to try a test recovery of your system partition to this hard drive.

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

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

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

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

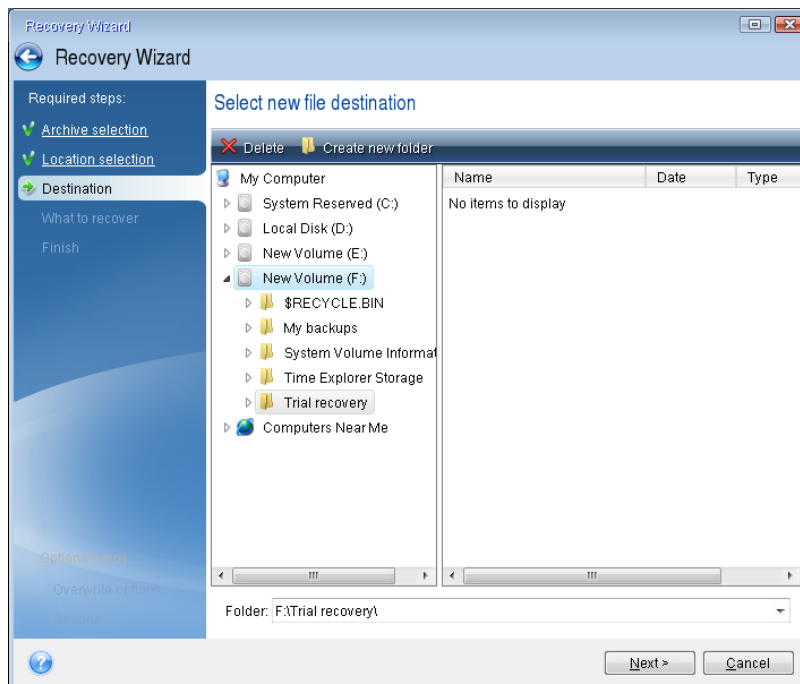


3. When recovering files with the rescue CD you are able to select only a new location for the files to be recovered. Therefore just click **Next** at the **Location selection** step.
4. After the **Destination** window opens, check that all your drives are shown under **My Computer**.

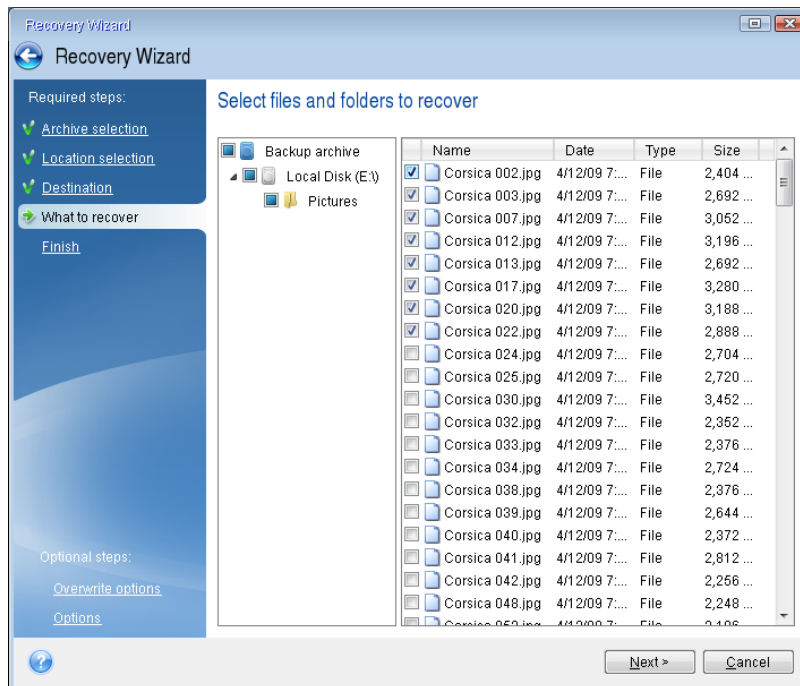
If you store your backups on the network, you should also check that you can access the network.

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

*If the **Computers Near Me** icon is not available under **My Computer**, there may be problems either with your network card or with the card driver provided with Acronis True Image 2015.*



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 2015.

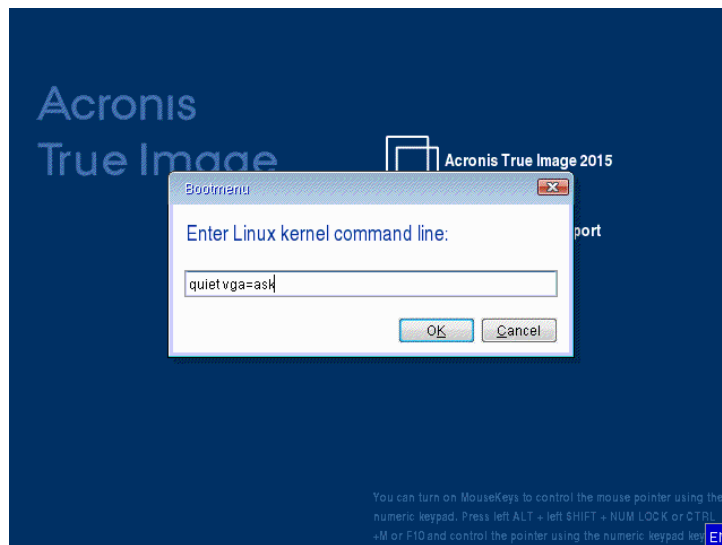
Now you can be reasonably sure that your rescue CD will help you when needed.

8.1.2.1 Selecting video mode when booting from the rescue media

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

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

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



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

```

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: _

```

- Wait until Acronis True Image 2015 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 2015 and repeat the above procedure.

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

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

8.1.3 Creating factory bootable media

This functionality is available only if the computer has an Acronis Secure Zone that has a backup of the computer's factory configuration. This backup is normally created in Acronis Secure Zone by a hardware supplier who delivers computers to end users.

Factory bootable media is a special type of rescue bootable media that includes a backup of a computer's factory configuration. You can use such media to restore your computer to factory settings. Note that the restoration will erase all personal data and programs on the computer.

You may have received factory bootable media with your new computer. However, if the hardware supplier did not include this media or if you do not have the media for any other reasons, you can create factory bootable media yourself and save it for an emergency.

With Acronis True Image 2015 you can create factory bootable media on a USB stick, CD/DVD or as an ISO image that can be burned to CD/DVD later.

To create factory bootable media:

1. Click **Create factory bootable media** on the **Backup and recovery** tab.

A dialog window with bootable media parameters opens.

2. Define the parameters of the media.

3. Click **Create**.

The program starts creating the factory bootable media. If you have selected to burn a CD or DVD, the program will ask you to insert another blank disc once the first disc is burned.

Media creation wizard

Use the wizard to choose the type of media: USB, CD/DVD or ISO image.

If you are creating bootable media on a USB stick, make sure to connect the USB stick to the computer before you begin. The USB stick must be FAT 32 formatted.

If you select to create an ISO image, you also need to specify its parameters:

- **Split into** - Choose whether the program should split the resulting ISO image into multiple .iso files of certain size.
- **Save file(s) to** - Specify the location of the resulting ISO image.

Once you select the media, click **Create** to start creating the media.

8.2 Acronis Startup Recovery Manager

How it works

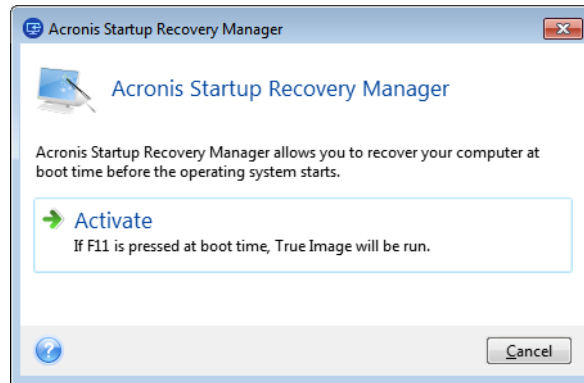
The Acronis Startup Recovery Manager lets you start Acronis True Image 2015 without loading the operating system. With this feature, you can use Acronis True Image 2015 by itself to recover damaged partitions, even if the operating system won't boot. Unlike booting from Acronis removable media, you will not need a separate media or network connection to start Acronis True Image 2015.

How to activate

To activate Acronis Startup Recovery Manager:

1. Click the **Start** button → **Acronis** (product folder) → **True Image** → **Tools and Utilities** → **Acronis Startup Recovery Manager**.

2. In the opened window, click **Activate**.



How to use

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 2015 that differs only slightly from the complete version.

Additional information

Disk letters in standalone Acronis True Image 2015 might sometimes differ from the way Windows identifies drives. For example, the D: disk identified in the standalone Acronis True Image 2015 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.

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.

8.3 Working with Acronis Secure Zone

In this section

Acronis Secure Zone.....	117
Creating and managing Acronis Secure Zone	117
Acronis Secure Zone location.....	118
Size of Acronis Secure Zone	119
Acronis Secure Zone protection.....	119

8.3.1 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.

Acronis Secure Zone in Windows Explorer

When you create an Acronis Secure Zone, it is displayed in the **Other** section of Windows Explorer. You can navigate through the Acronis Secure Zone as an ordinary partition.

Right-click a specific backup or a backup version to view all available operations:

- Explore
- Mount (for image backups)
- Recover
- Validate
- Update
- Remove
- View the version's details

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, 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, we recommended that you select the **When not enough space in ASZ, delete the oldest backup** check box in the scheduled backup options. Refer to Error handling (p. 52) for details.

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 (p. 30).

8.3.2 Creating and managing Acronis Secure Zone

To create or modify the Acronis Secure Zone:

1. Click the **Start** button → **Acronis** (product folder) → **True Image** → **Tools and Utilities** → **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 (p. 118) and size (p. 119).
 - If you want to modify the Acronis Secure Zone, select an action:
 - Increase or decrease size (p. 118)
 - Remove (p. 120)
 - Change password (p. 119)

Then follow the wizard steps.

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

Note: This operation may require a computer restart.

8.3.3 Acronis Secure Zone location

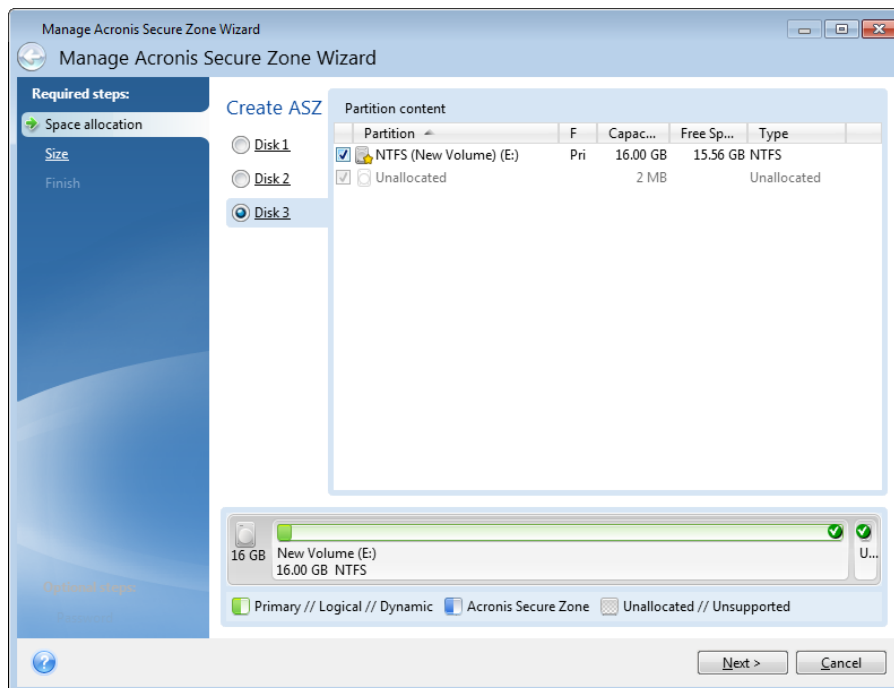
Creating the Acronis Secure Zone

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.

The Acronis Secure Zone cannot be created on dynamic disks and volumes.

3. Click **Next**.



Increasing or decreasing the size of the Acronis Secure Zone

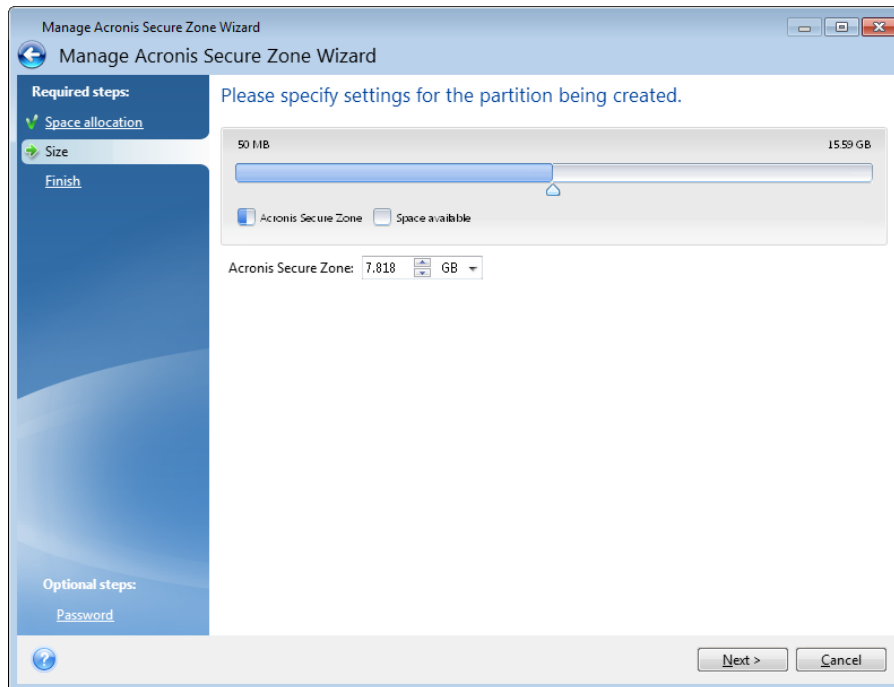
To increase/decrease the size of the Acronis Secure Zone:

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**.

8.3.4 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.

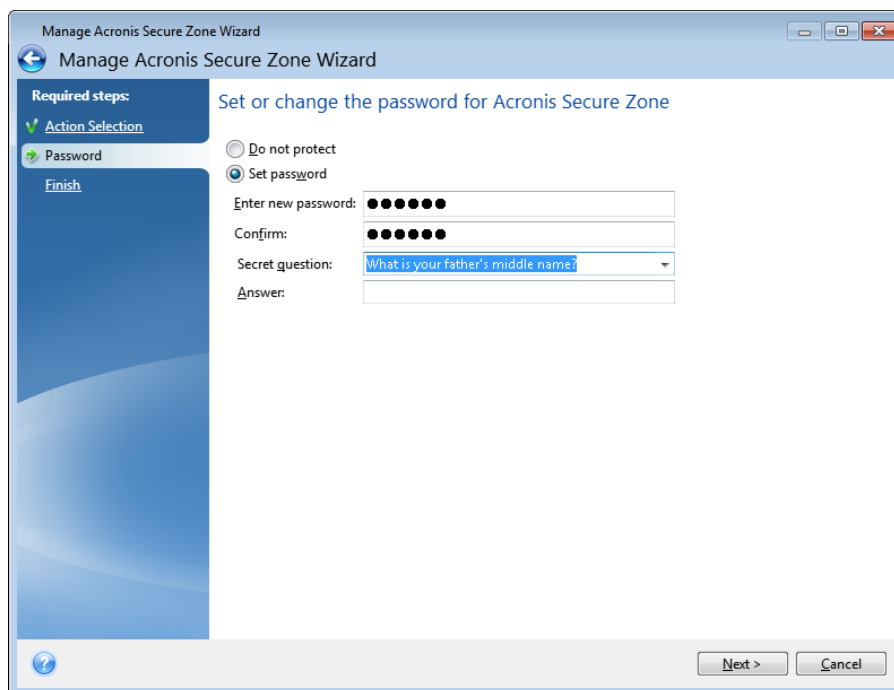
8.3.5 Acronis Secure Zone protection

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.



Acronis True Image 2015 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.

8.3.6 Removing Acronis Secure Zone

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.

8.4 Adding a new hard disk

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

To add a new hard disk:

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

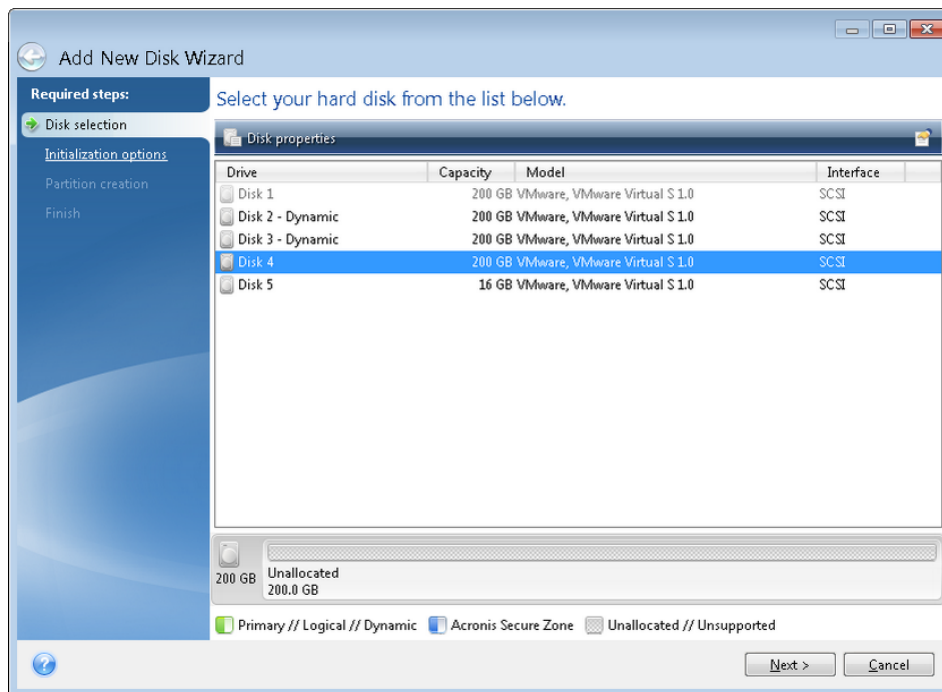
In this section

Selecting a hard disk	121
Selecting initialization method	122
Creating new partitions.....	122

8.4.1 Selecting a hard disk

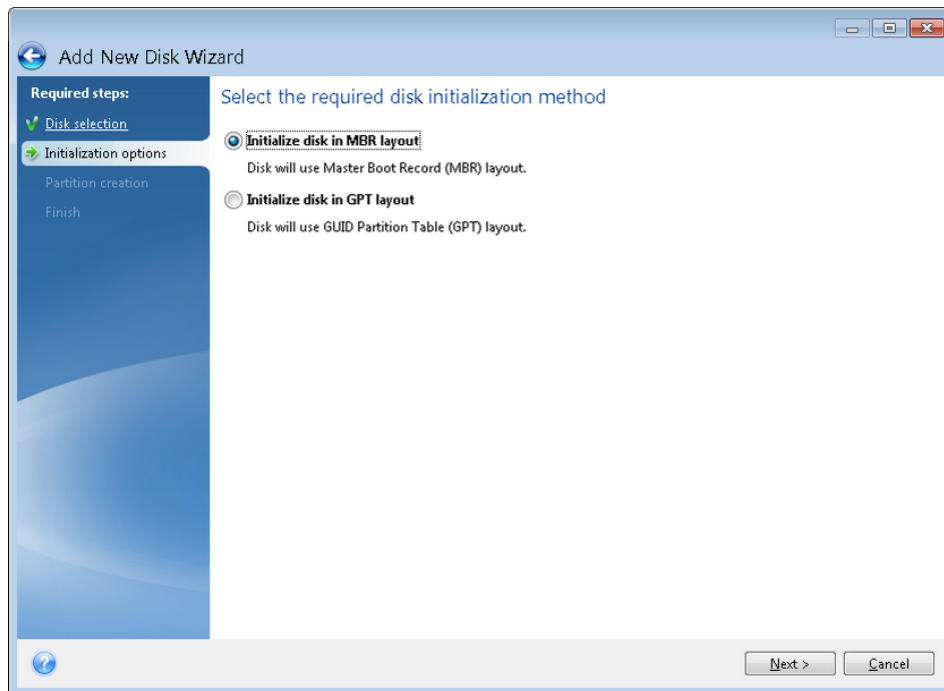
Select the disk that you have added to the computer. If you have added several disks, select one of them and click **Next** to continue. You can add the other disks later by restarting the Add New Disk Wizard.

If there are any partitions on the new disk, Acronis True Image 2015 will warn you that these partitions will be deleted.



8.4.2 Selecting initialization method

Acronis True Image 2015 supports both MBR and GPT partitioning. GUID Partition Table (GPT) is a new hard disk partitioning method providing advantages over the old MBR partitioning method. If your operating system supports GPT disks, you can select the new disk to be initialized as a GPT disk.



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

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

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

8.4.3 Creating new partitions

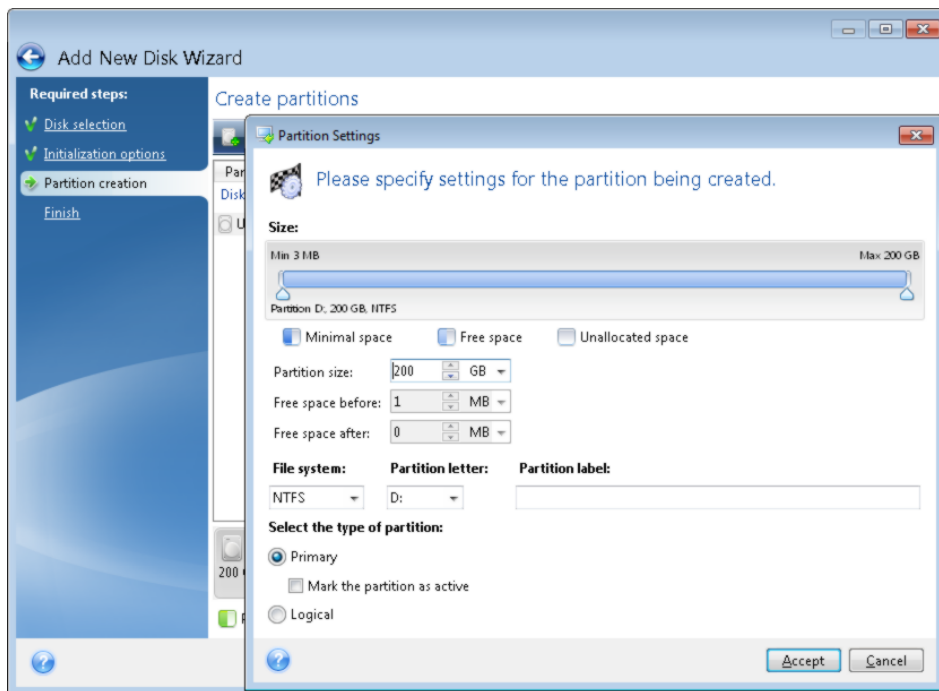
To use the space on a hard disk, it must be partitioned. Partitioning is the process of dividing the hard disk's space into logical divisions which are called partitions. Each partition may function as a separate disk with an assigned drive letter, its own file system, etc.

To create a new partition:

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

Refer to Partition settings (p. 123) for details.

3. Click **Accept**.



8.4.3.1 Partition settings

Size

To resize the partition, perform one of the following:

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

To relocate the partition, perform one of the following:

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

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

File System

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

- **NTFS** is a Windows NT, Windows 2000, Windows XP, Windows Vista, and Windows 7 native file system. Choose it if you use these operating systems. Note, that Windows 95/98/Me and DOS cannot access NTFS partitions.
- **FAT 32** is an improved 32-bit version of the FAT file system that supports volumes up to 2 TB.
- **FAT 16** is a DOS native file system. Most operating systems recognize it. However, if your disk drive is more than 4 GB, it is not possible to format it in FAT16.
- **Ext2** is a Linux native file system. It is fast enough, but it is not a journaling file system.

- **Ext3** – officially introduced with Red hat Linux version 7.2, Ext3 is a Linux journaling file system. It is forwards and backwards compatible with Linux Ext2. It has multiple journaling modes, as well as broad, cross platform compatibility in both 32-bit and 64-bit architectures.
- **Ext4** is a new Linux file system. It has improvements in comparison to ext3. It is fully backward compatible with ext2 and ext 3. However, ext3 has only partial forward compatibility with ext4.
- **ReiserFS** is a journaling file system for Linux. Generally it is more reliable and faster than Ext2. Choose it for your Linux data partition.
- **Linux Swap** is a swap partition for Linux. Choose it if you want to add more swap space using Linux.

Partition letter

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

Partition label

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

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

You can define the new partition as primary or logical.

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

8.5 Security and Privacy Tools

In this section

Acronis DriveCleanser	124
System Clean-up	128
Hard Disk Wiping methods	134

8.5.1 Acronis DriveCleanser

Acronis DriveCleanser allows you to permanently destroy all data on selected hard disks and partitions. For the destruction, you can use one of the preset algorithms or create your own. Refer to Algorithm selection (p. 126) for details.

Why do I need it?

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

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

How to use Acronis DriveCleanser

To permanently destroy data on your disk:

1. Click the **Start** button → **Acronis** (product folder) → **True Image** → **Tools and Utilities** → **DriveCleanser**.


The Acronis DriveCleanser wizard opens.


2. On the **Source selection** step, select the disks and partitions that you want to wipe. Refer to Source selection (p. 125) for details.
3. On the **Algorithm selection** step, select an algorithm that you want to use for the data destruction. Refer to Algorithm selection (p. 126) for details.
4. [optional step] You can create your own algorithm. Refer to Creating custom algorithm for details.
5. [optional step] On the **Post-wiping actions** step, choose what to do with the partitions and disk when the data destruction is complete. Refer to Post-wiping actions (p. 128) for details.
6. On the **Finish** step, ensure that the configured settings are correct. To start the process, select the **Wipe the selected partitions irreversibly** check box, and then click **Proceed**.

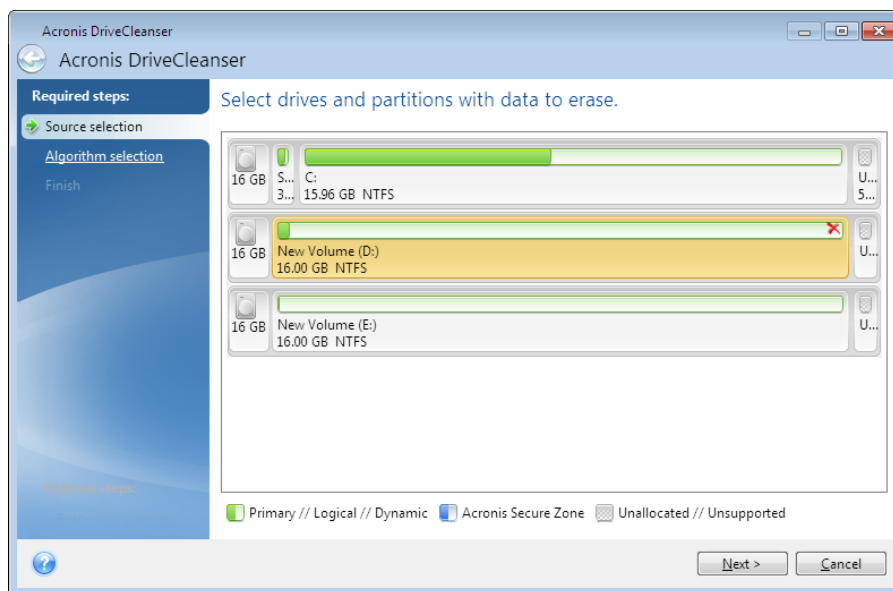
Be aware that, depending on the total size of selected partitions and the selected data destruction algorithm, the data destruction may take many hours.

8.5.1.1 Source selection

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

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

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

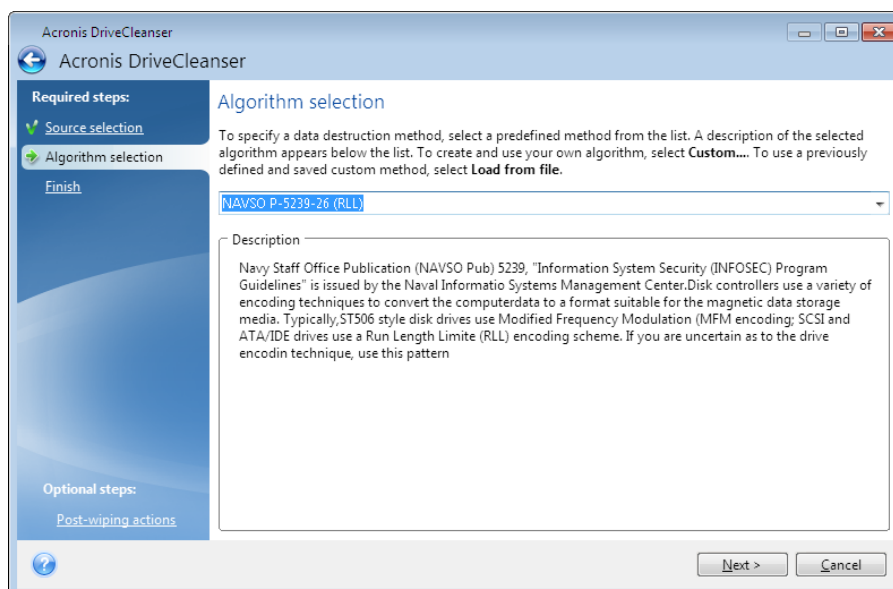


Acronis DriveCleanser cannot wipe partitions on dynamic and GPT disks, so they will not be shown.

8.5.1.2 Algorithm selection

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

- To use one of the preset algorithms, select the desired algorithm. Refer to Hard Disk Wiping Methods (p. 134) for details.
- [For advanced users only] To create a custom algorithm, select **Custom**. Then continue creating on the **Algorithm definition** step. Afterwards, you will be able to save the created algorithm to a file with *.alg extension.
- To use a previously saved custom algorithm, select **Load from file** and select the file containing your algorithm.



Creating custom algorithm

Algorithm definition

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

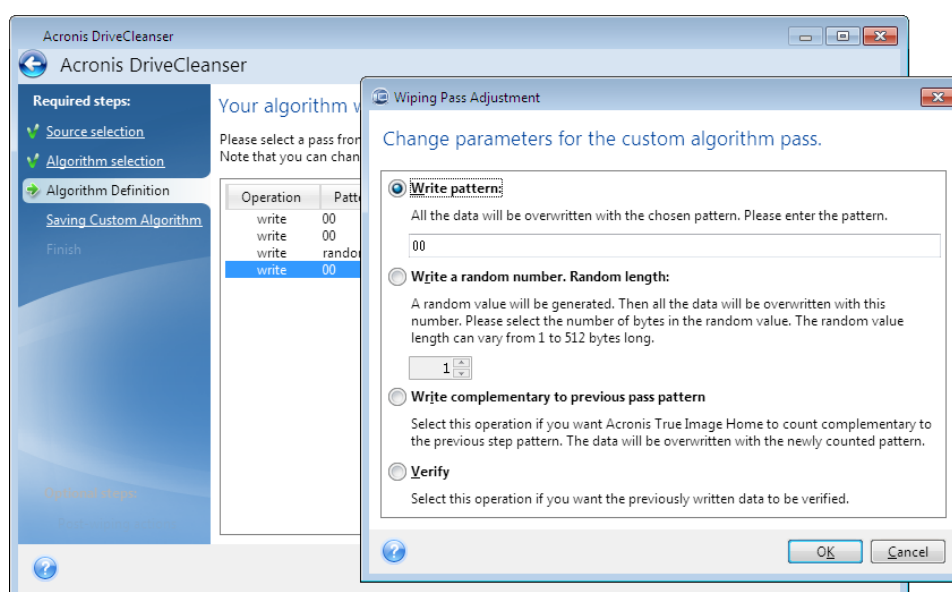
The table has the following legend:

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

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

To add a new pass:

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



2. Choose an option:

- **Write pattern**

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

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

- **Write a random number**

Specify the length of the random value in bytes.

- **Write complementary to previous pass pattern**

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

- **Verify**

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

3. Click **OK**.

To edit an existing pass:

1. Select the corresponding line, and then click **Edit**.
The Wiping Pass Adjustment window opens.

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

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

Saving algorithm to a file

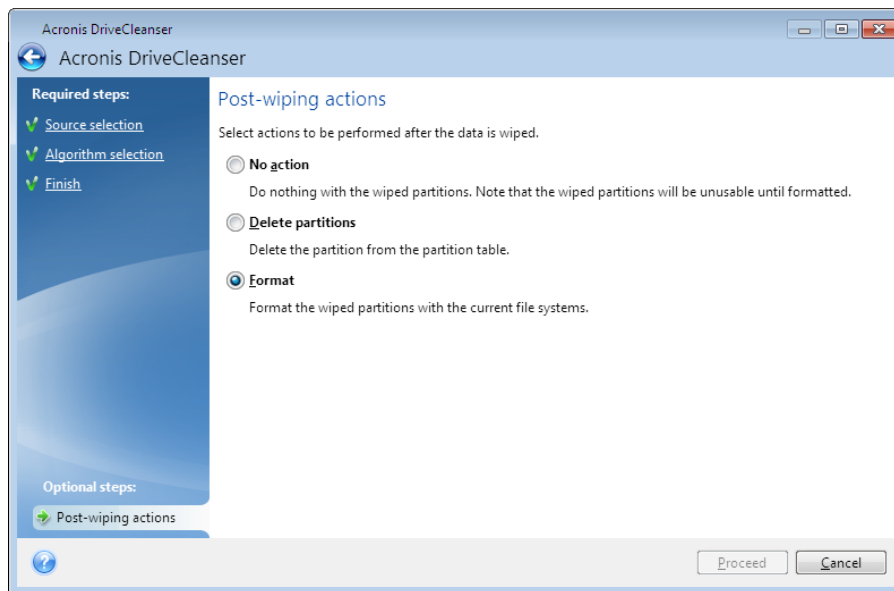
To save the created algorithm to a file in order to use this algorithm afterwards:

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

8.5.1.3 Post-wiping actions

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

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



8.5.2 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

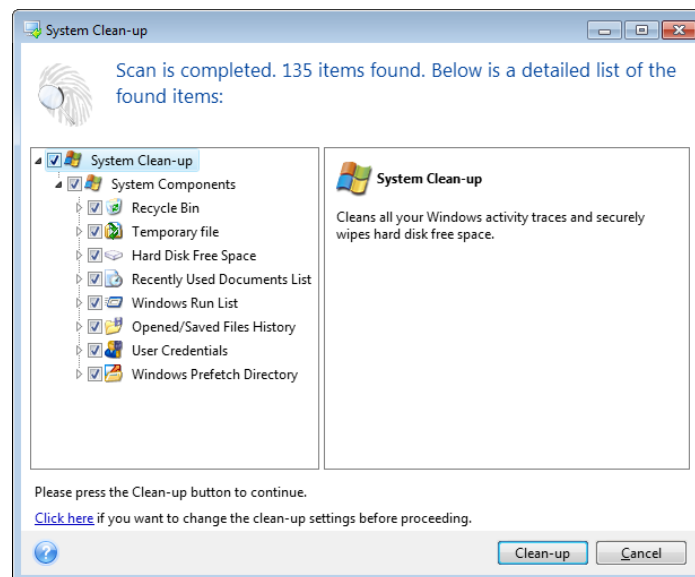
- Clean the **recently used documents** list
- Clean the **Windows Run** list
- Clean the **opened/saved files** history
- Clean the list of network places to which the user has connected using **network credentials**
- Clean the **Windows prefetch directory**, where Windows stores information about programs you have executed and run recently

Windows Vista and Windows 7 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.

Please, be aware that 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) → **True Image** → **Tools and Utilities** → **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.

If you want to change the default system clean-up settings, click the corresponding link in the first window of the System Clean-up wizard.

Click **Clean-up** to launch removing the found items.

8.5.2.1 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

8.5.2.2 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:

- Choose on the tree the component clean-up settings which you need to change.
- 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 (p. 134) of this guide.

8.5.2.3 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

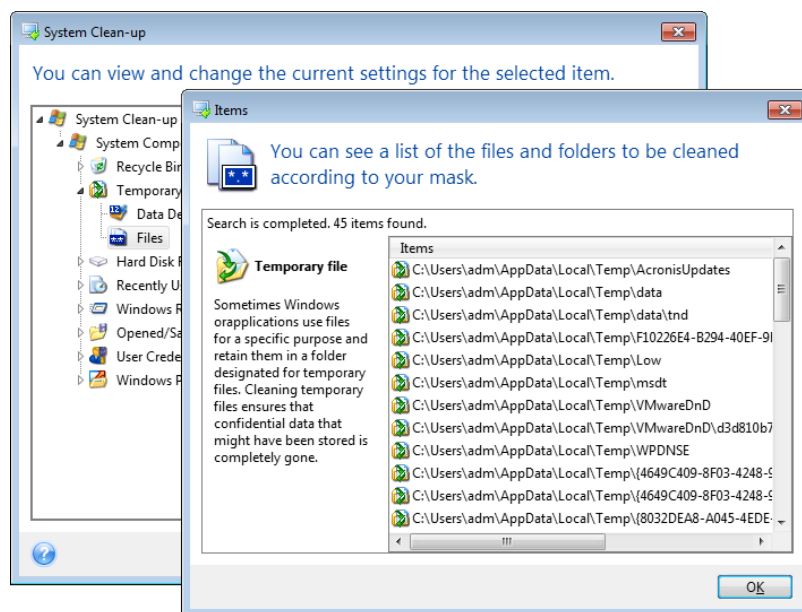
System Clean-up utilizes a number of the most popular data destruction methods. Here, you need to select the desired data destruction method.

- **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 on 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 (p. 134) 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.

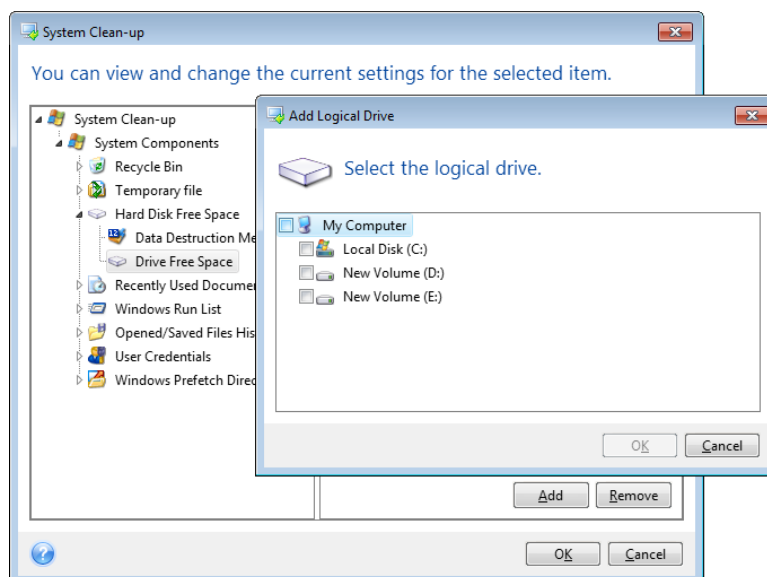
Upon entering the Files setting value, you can browse the files matching the search strings. To do this, click **Show Files**. You will see a window with the names of the found files. These files will be cleaned.

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.

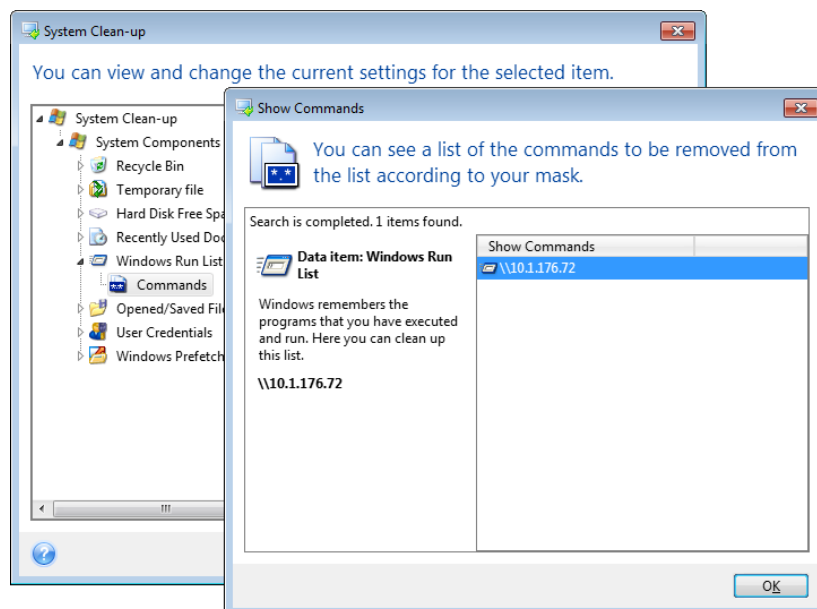
"Commands" setting

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.

8.5.2.4 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 with making the right choice, all the components are provided with brief descriptions. Just click on the component's name and its description will be displayed 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.

Windows Vista and Windows 7 do not keep 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.

8.5.2.5 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 2015 will turn the computer off.

8.5.3 Hard Disk Wiping methods

What is the problem?

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

Leakage mechanism

Data is stored on a hard disk as a binary sequence of 1 and 0 (ones and zeros), represented by differently magnetized parts of a disk.

Generally speaking, a 1 written to a hard disk is read as 1 by its controller, and 0 is read as 0. However, if you write 1 over 0, the result is conditionally 0.95 and vice versa – if 1 is written over 1 the result is 1.05. These differences are irrelevant for the controller. However, using special equipment, one can easily read the «underlying» sequence of 1's and 0's.

Information wiping methods used by Acronis

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

No.	Algorithm (writing method)	Passes	Record
1.	United States Department of Defense 5220.22-M	4	1 st pass – randomly selected symbols to each byte of each sector, 2 – complementary to written during the 1 st pass; 3 – random symbols again; 4 – writing verification.
2.	United States: NAVSO P-5239-26 (RLL)	4	1 st pass – 0x01 to all sectors, 2 – 0x27FFFFFF, 3 – random symbol sequences, 4 – verification.
3.	United States: NAVSO P-5239-26 (MFM)	4	1 st pass – 0x01 to all sectors, 2 – 0x7FFFFFFF, 3 – random symbol sequences, 4 – verification.
4.	German: VSITR	7	1 st – 6 th – alternate sequences of: 0x00 and 0xFF; 7 th – 0xAA; i.e. 0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF, 0xAA.
5.	Russian: GOST P50739-95	1	Logical zeros (0x00 numbers) to each byte of each sector for 6 th to 4 th security level systems. Randomly selected symbols (numbers) to each byte of each sector for 3 rd to 1 st security level systems.
6.	Peter Gutmann's method	35	Peter Gutmann's method is very sophisticated. It's based on his theory of hard disk information wiping (see Secure Deletion of Data from Magnetic and Solid-State Memory).
7.	Bruce Schneier's method	7	Bruce Schneier offers a seven-pass overwriting method in his Applied Cryptography book. 1 st pass – 0xFF, 2 nd pass – 0x00, and then five times with a cryptographically secure pseudo-random sequence.
8.	Fast	1	Logical zeros (0x00 numbers) to all sectors to wipe.

8.6 Mounting an image

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

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

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

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

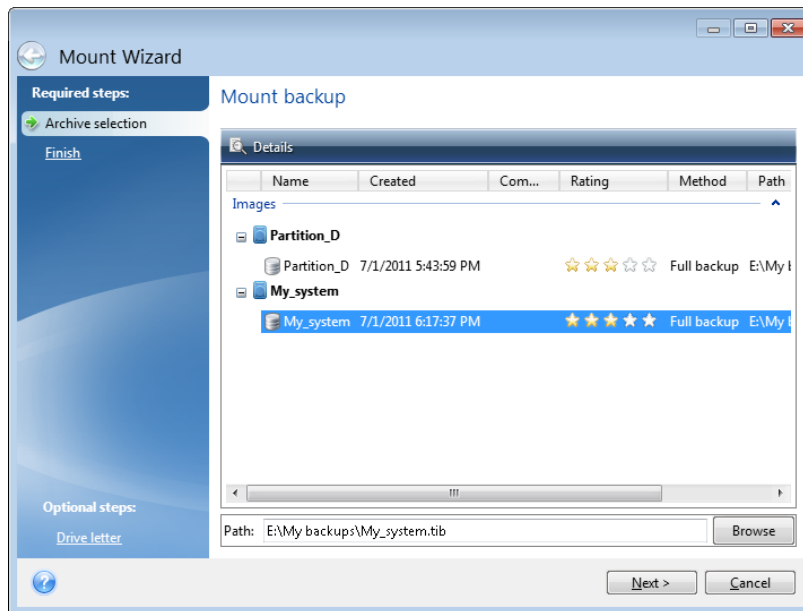
How to mount an image

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

The Mount wizard opens.

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

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



3. [optional step] On the **Drive letter** step, select a letter to be assigned to the virtual disk from the **Mount letter** drop-down list. If you do not want to mount a partition, select **Do not mount** in the list or clear the partition's check box.
4. Click **Proceed**.
5. After the image is connected, the program will run Windows Explorer, showing its contents.

8.7 Unmounting an image

We recommend that you unmount the virtual disk after all necessary operations are finished, as maintaining virtual disks takes considerable system resources.

To unmount an image, perform one of the following:

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

9 Troubleshooting

In this section

Acronis System Report	137
Acronis Smart Error Reporting	138
How to collect crash dumps.....	139
Creating a custom rescue CD	139
Acronis Customer Experience Program	140

9.1 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 simplifies the procedure. It generates a system report containing all the necessary technical information and allows you to save the information to file. When it's necessary, you can attach the created file to your problem description and send it to Acronis 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**.
- On the Windows **Start** menu, click **All Programs -> Acronis -> Acronis True Image 2015 -> Tools and Utilities -> Acronis System Report**.
- Press **CTRL+F7**. Note that you can use the key combination even when Acronis True Image 2015 is performing any other operation.

After the report is generated:

- To save the generated system report to file, click **Save** and in the opened window specify a location for the created file.
- To exit to the main program window without saving the report, click **Cancel**.

You can place the tool on your bootable rescue media as a separate component to generate a system report when your computer cannot boot. After you boot from the media, you can generate the report without running Acronis True Image 2015. 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 rescue media:

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

Creating a system report from the command line prompt

1. Run Windows Command Processor (cmd.exe) as administrator.
2. Change the current directory to the Acronis True Image 2015 installation folder. To do so, enter:

```
cd C:\Program Files (x86)\Acronis\TrueImageHome
```
3. To create the system report file, enter:

```
SystemReport
```

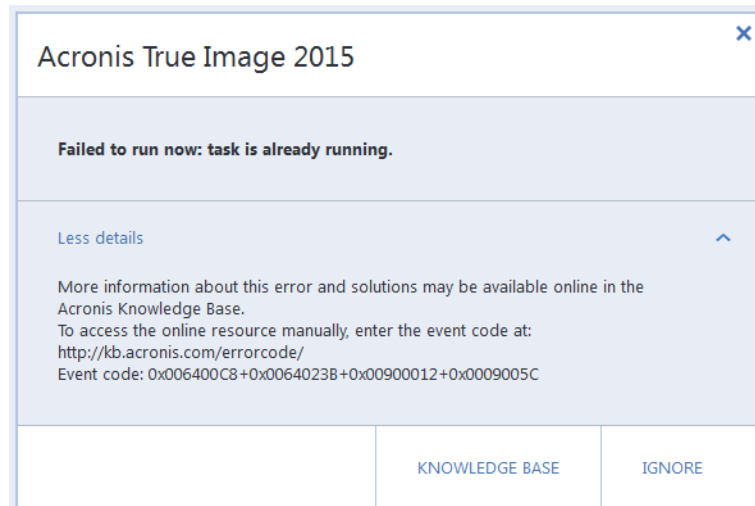

File SystemReport.zip will be created in the current folder.

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

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

9.2 Acronis Smart Error Reporting

When an issue is caused by an error in the program's operation, Acronis True Image 2015 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 Knowledge Base 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 Knowledge Base. 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, please 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.
1. When you establish Internet connection or if you can use another computer where Internet connection is available, enter the event code at: <http://kb.acronis.com/errorcode/>.

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, please open a trouble ticket with Acronis Customer Central.

9.3 How to collect crash dumps

Because a crash of Acronis True Image 2015 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 2015 crashes, please provide the following information:

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

If Acronis True Image 2015 causes a Windows crash:

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

If Acronis True Image 2015 hangs:

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

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

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

9.4 Creating a custom rescue CD

In most cases you can use a standard rescue CD created with a help of Acronis Media Builder. For more information see [Creating bootable rescue media](#).

If the recovery environment cannot detect some of the hard disk drives, the network adapter, the mouse or the keyboard, usually there is a problem with the drivers. So when the standard rescue CD lacks some of your hardware drivers, you need to create a custom one.

The Linux-based recovery environment used by Acronis does not provide the ability for users to add new drivers. Because of this, you should request Acronis Customer Service Department to create a custom rescue CD that will have all the drivers you need.

Before making a request, collect the information about your system. To do this you need to create a system report under bootable media.

To generate a system report:

1. Create Acronis bootable rescue media, if you do not have it. See details in [Acronis Media Builder](#).
2. Arrange the boot order in BIOS so as to make your rescue media device (CD, DVD or USB stick) the first boot device. See [Arranging boot order in BIOS](#) (p. 74).
3. Boot from the rescue media and select **True Image**.

*Instead of clicking **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 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.

Send the file to the Acronis Customer Service Department. They will build an iso image of a custom rescue media compatible with your computer hardware and send you the iso file. Burn this file to a CD/DVD using a program that can handle iso files such as Nero.

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

After burning your custom rescue CD, test it to make sure that all your computer hardware is now detected in the recovery environment.

9.5 Acronis Customer Experience Program

Acronis Customer Experience Program (CEP) is a new way to allow Acronis customers to contribute to the features, design and development of Acronis products. This program enables our customers to provide us with various information, including information about the hardware configuration of your host computer and/or virtual machines, the features you use most (and least), and the nature of the problems you face. Based on this information, we will be able to improve the Acronis products and the features you use most often.

To make a decision:

1. On the sidebar, click **Help**, and then click **About Acronis True Image**.
2. To leave the program, turn off the **Participate in the Acronis Customer Experience Program** switcher.

If you choose to participate, the technical information will be automatically collected every 90 days. We will not collect any personal data, like your name, address, phone number, or keyboard input. Participation in the CEP is voluntary, however, but the end results intended to provide software improvements and enhanced functionality to better meet the needs of our customers.

Copyright Statement

Copyright © Acronis International GmbH, 2002-2014. All rights reserved.

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

Linux is a registered trademark of Linus Torvalds.

VMware and VMware Ready are trademarks and/or registered trademarks of VMware, Inc. in the United States and/or other jurisdictions.

Windows and MS-DOS are registered trademarks of Microsoft Corporation.

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

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

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

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

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

Acronis patented technologies

Technologies, used in this product, are covered and protected by one or more U.S. Patent Numbers: 7,047,380; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121 and patent pending applications.

10 Glossary of Terms

A

Acronis Secure Zone

A secure partition for storing backups (p. 142) 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 Acronis True Image 2015 from bootable rescue media, through Acronis Startup Recovery Manager or BartPE.

Acronis Startup Recovery Manager

A protection tool that allows to start standalone version of Acronis True Image 2015 at boot time when F11 is pressed. Acronis Startup Recovery Manager eliminates the need for rescue media.

Acronis 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 Acronis 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.

B

Backup

1. The same as Backup operation (p. 142).
2. A set of backup versions created and managed by using backup settings. A backup can contain multiple backup versions created using full (p. 143) and incremental (p. 143) backup methods. Backup versions belonging to the same backup are usually stored in the same location.

Backup operation

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

Backup settings

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

Backup version

The result of a single backup operation (p. 142). Physically, it is a file or a set of files that contains a copy of the backed up data as of a specific date and time. Backup version files created by Acronis True Image 2015 have a TIB extension. The TIB files resulting from consolidation of backup versions are also called backup versions.

Backup version chain

Sequence of minimum 2 backup versions (p. 142) 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 flash drive or other media supported by a machine BIOS as a boot device) that contains standalone version of Acronis True Image 2015.

Bootable media is most often used to:

- recover an operating system that cannot start
- access and back up the data that has survived in a corrupted system
- deploy an operating system on bare metal
- create basic or dynamic volumes on bare metal
- 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

1. A backup method used for saving data changes that occurred since the last full backup version (p. 143) within a backup.
2. A backup process that creates a differential backup version (p. 143).

Differential backup version

A differential backup version stores changes to the data against the latest full backup version (p. 143). You need access to the corresponding full backup version to recover the data from a differential backup version.

Disk backup (Image)

A backup (p. 142) that contains a sector-based copy of a disk or a partition in packaged form. Normally, only sectors that contain data are copied. Acronis True Image 2015 provides an option to take a raw image, that is, copy all the disk sectors, which enables imaging of unsupported file systems.

F

Full backup

1. A backup method that is used to save all the data selected to back up.
2. A backup process that creates a full backup version (p. 143).

Full backup version

A self-sufficient backup version (p. 142) containing all data chosen for backup. You do not need access to any other backup version to recover the data from a full backup version.

I

Image

The same as Disk backup (p. 143).

Incremental backup

1. A backup method used for saving data changes that occurred since the last backup version (p. 142) (of any type) within a backup.
2. A backup process that creates an incremental backup version (p. 143).

Incremental backup version

A backup version (p. 142) that stores changes to the data against the latest backup version. You need access to other backup versions from the same backup (p. 142) to restore data from an incremental backup version.

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 (p. 143) and a sequence of incremental backup versions (p. 143) 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.

O

Online backup

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

R

Recovery

Recovery is a process of returning of a corrupted data to a previous normal state from a backup (p. 142).

S

Sync

1. The same as Data synchronization (p. 143).
2. Sync settings which were configured on the sync owner's computer. A created sync is managed using the corresponding

sync box. Sync creation does not mean start of sync process. Other users may join a created sync.

V

Validation

An operation that checks whether you will be able to recover data from a particular backup version (p. 142).

When you select for validation...

- a full backup version (p. 143) - the program validates the full backup version only.
- a differential backup version (p. 143) - the program validates the initial full backup version and the selected differential backup version.
- an incremental backup version (p. 143) - 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.