Acronis
COMPUTE WITH CONFIDENCE
WWW.ACRONIS.COM

Acronis® True Image Home 2009

User's Guide

ACRONIS, INC.

End User License Agreement (EULA)

BEFORE INSTALLING AND USING THE SOFTWARE PRODUCT WHICH EITHER YOU HAVE DOWNLOADED OR IS CONTAINED ON THESE DISKS ("SOFTWARE") YOU SHOULD CAREFULLY READ THE FOLLOWING LICENSE AGREEMENT ("AGREEMENT") THAT APPLIES TO THE SOFTWARE. CLICK "ACCEPT" IF YOU FULLY ACCEPT AND AGREE TO ALL OF THE PROVISIONS OF THIS AGREEMENT. OTHERWISE, CLICK "DO NOT ACCEPT." CLICKING "ACCEPT" OR OTHERWISE DOWNLOADING, INSTALLING AND OR USING THE SOFTWARE ESTABLISHES A BINDING AGREEMENT BETWEEN YOU AS THE PERSON LICENSING THE SOFTWARE (THE "LICENSEE") AND ACRONIS, INC. LOCATED AT: ACRONIS INTERNATIONAL GMBH VERWALTUNG EURO HAUS RHEINWEG 5 SCHAFFHAUSEN, SWITZERLAND CH-8200, ("LICENSOR"). IF YOU DO NOT ACCEPT ALL OF THE TERMS OF THIS AGREEMENT, YOU SHALL HAVE NOT RIGHT TO DOWNLOAD, INSTALL AND/OR USE THE SOFTWARE AND MUST DELETE THE SOFTWARE AND ASSOCIATED FILES IMMEDIATELY.

This Agreement applies to the Software, whether licensed under a Software License and/or an Evaluation License, each as defined and described below:

Purchased License of Software. Subject to the terms and conditions of this Agreement, upon purchase of a license to the Software, the LICENSOR grants and the LICENSEE accepts a nonexclusive, nontransferable, nonassignable license to use the Software only for the LICENSEE's own internal use solely on the specific number of computers that you have licensed. Installation of the Software is the LICENSEE's responsibility. The license described in this section shall be referred to as a "Software License".

Evaluation License of Software: The LICENSEE has the right to evaluate the Software for a period of time not to exceed fifteen (15) days (the "Evaluation Period') unless extended by LICENSOR. Software licensed under this Evaluation License may not be used in a production environment. There will be no charge to the LICENSEE for said evaluation of the Software under this Evaluation License. At the conclusion of the Evaluation Period, unless a Software License to the Software is purchased, the LICENSEE will delete the Software from its systems and have no further license or other rights with respect to the Software except as to the rights and responsibilities in this Agreement. THE LICENSOR SHALL NOT BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, PUNITIVE, OR CONSEQUENTIAL DAMAGES RESULTING FROM USE OF SOFTWARE UNDER THE EVALUATION LICENSE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER THEORY. THESE LIMITATIONS SHALL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY. The following sections of this Agreement also apply to the Evaluation License(s) of the Software: **Limitations, Confidentiality**, **Disclaimer of Warranties, LICENSEE Indemnity**, **Law, Export Restrictions, and Miscellaneous.** The license described in this section shall be referred to as an "Evaluation License").

Use Rights:

Assigning the License. Before you run any instance of the Software under a Software License, you must assign that license to one of your PCs and that PC is the licensed PC for that particular Software License. You may assign other Software Licenses to the same PC, but you may not assign the same PC License to more than one PC except as identified herein.

You may reassign a Software License if you retire the licensed PC due to permanent PC failure. If you reassign a Software License, the PC to which you reassign the license becomes the new licensed PC for that particular Software License.

> Running Instances of the Software. You have the rights to run the Software on one (1) PC. Every PC creating an image and every PC to which an image is either deployed to or restored from must have a valid license.

Support. By virtue of licensing a Software License and registering your Software License with LICENSOR, and at the LICENSOR'S sole discretion, the LICENSEE is entitled to: (1) "patch" or "dot releases (e.g., 11.01, 11.02, and 11.03 etc.) of the Software License. A major release(s) of the Software License (e.g., Version 12 Version 13, etc) are not included in Support and would require a paid upgrade fee; (2) email support ; and (3) other electronic services that the LICENSOR may make generally available to its customers, such as an electronically available base of knowledge ("Knowledge Base") to assist in answering general questions about the Software License. In the event that the LICENSEE makes any unauthorized modifications to the Software Product, Support services are null and void.

Limitations. Notwithstanding any references to "purchase", the Software is licensed and not sold pursuant to this Agreement. This Agreement confers a limited license to the Software and does not constitute a transfer of title to or sale of all or a portion of the Software, and the LICENSOR retains ownership of all copies of the Software. The LICENSEE acknowledges that the Software contains trade secrets of the LICENSOR, its suppliers or licensors, including but not limited to the specific internal design and structure of individual programs and associated interface information. Accordingly, except as otherwise expressly provided under this Agreement, the LICENSEE shall have no right, and the LICENSEE specifically agrees not to: (i) transfer, assign or sublicense its license rights to any other person or entity, or use the Software on any equipment other than the PC, and the LICENSEE acknowledges that any attempted transfer, assignment, sublicense or use shall be void; (ii) make error corrections to or otherwise modify or adapt the Software or create derivative works based upon the Software, or permit third parties to do the same; (iii) reverse engineer or decompile, decrypt, disassemble or otherwise reduce the Software to human-readable form, except to the extent otherwise expressly permitted under applicable law notwithstanding this restriction; (iv) use or permit the Software to be used to perform services for third parties, whether on a service bureau or time sharing basis or otherwise, without the express written authorization of the LICENSEE; or (v) disclose, provide, or otherwise make available trade secrets contained within the Software in any form to any third party without the prior written consent of the LICENSOR.

Confidentiality. The Software is a trade secret of the LICENSOR and is proprietary to the LICENSOR. The LICENSEE shall maintain the Software in confidence and prevent disclosure of the Software using at least the same degree of care it uses for its own similar proprietary information, but in no event less than a reasonable degree of care. The LICENSEE shall not disclose the Software or any part thereof to anyone for any purpose, other than to employees for the purpose of exercising the rights expressly granted under this Agreement. The License shall not, and shall not allow any third party to, decompile, disassemble or otherwise, reverse engineer or attempt to reconstruct or discover any source code or underlying ideas, algorithms, file formats or programming or interoperability interfaces of the Software or of any files contained or generated using the Software by any means whatsoever. The obligations under this paragraph shall survive any termination of the Agreement.

Disclaimer of Warranties. THE SOFTWARE IS PROVIDED "AS IS" AND THE LICENSOR DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED WITH RESPECT TO THE SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY, TITLE, NON-INFRINGEMENT OF THIRD PARTIES' RIGHTS, AND FITNESS FOR A PARTICULAR USE. WITHOUT LIMITING THE FOREGOING, THE LICENSOR DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL OPERATE IN THE COMBINATION THE LICENSEE SELECTS, THAT OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE AND/OR THAT DEFECTS IN THE SOFTWARE WILL BE CORRECTED. THE ENTIRE RISK AS TO THE RESULTS AND PERFORMANCE OF THE SOFTWARE IS ASSUMED BY THE LICENSEE. FURTHERMORE, THE LICENSOR DOES NOT WARRANT OR MAKE ANY REPRESENTATIONS REGARDING THE USE OR THE RESULTS OF THE USE OF THE SOFTWARE OR RELATED DOCUMENTATION IN TERMS OF THEIR CORRECTNESS, ACCURACY, RELIABILITY, CURRENTNESS, OR OTHERWISE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY THE LICENSOR SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY.

Liability Limitations. THE LICENSOR SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, PUNITIVE, OR CONSEQUENTIAL DAMAGES RESULTING FROM USE OF THE SOFTWARE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER THEORY. THE LICENSOR'S CUMULATIVE LIABILITY FOR DAMAGES HEREUNDER, WHETHER IN AN ACTION IN CONTRACT, WARRANTY, TORT, NEGLIGENCE, STRICT LIABILITY, INDEMNITY, OR OTHERWISE, SHALL IN NO EVENT EXCEED THE AMOUNT OF LICENSE FEES PAID BY THE LICENSEE FOR THE SOFTWARE LICENSED UNDER THIS AGREEMENT. THESE LIMITATIONS SHALL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

LICENSEE Indemnity. The LICENSEE agrees to indemnify and defend the LICENSOR, and hold it harmless from all costs, including attorney's fees, arising from any claim that may be made against the LICENSOR by any third party as a direct or indirect result of any use by the LICENSEE of the Software,

Termination. This Agreement and the license may be terminated without fee reduction (i) by the LICENSEE without cause on thirty (30) days notice; (ii) by the LICENSOR, in addition to other remedies, if the LICENSEE is in default and fails to cure within ten (10) days following notice; (iii) on notice by either party hereto if the other

party ceases to do business in the normal course, becomes insolvent, or becomes subject to any bankruptcy, insolvency, or equivalent proceedings. Upon termination for any reason, the LICENSEE shall immediately return the Software and all copies to the LICENSOR and delete all Software and all copies from the Hardware.

Law. This Agreement shall be governed by the laws of the Commonwealth of Massachusetts, exclusive of its conflicts of laws provisions and without regard to the United Nations Convention on Contracts for the International Sale of Goods, and any suit under this Agreement shall exclusively be brought in a federal or state court in Massachusetts. Any action against the LICENSOR under this Agreement must be commenced within one year after such cause of action accrues.

Government End Users. This provision applies to all Software acquired directly or indirectly by or on behalf of the United States Government. The Software is a commercial product, licensed on the open market at market prices, and was developed entirely at private expense and without the use of any U.S. Government funds. If the Software is supplied to the Department of Defense, the U.S. Government acquires only the license rights customarily provided to the public and specified in this Agreement. If the Software is supplied to any unit or agency of the U.S. Government other than the Department of Defense, the license to the U.S. Government is granted only with restricted rights. Use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c) of the Commercial Computer Software Restricted Rights clause of FAR 52.227-19.

Export Restriction. The LICENSEE will not remove or export from the United States or the country originally shipped to by the LICENSOR (or re-export from anywhere) any part of the Software or any direct product thereof except in compliance with applicable export laws and regulations, including without limitation, those of the U.S. Department of Commerce.

Miscellaneous. This Agreement contains the entire understanding of the parties and supersedes all other agreements, oral or written, including purchase orders submitted by the LICENSEE, with respect to the subject matter covered in this Agreement. The delay or failure of either party to exercise any right provided in the Agreement shall not be deemed a waiver. All notices must be in writing and shall be delivered by hand (effective when received) or mailed by registered or certified mail (effective on the third day following the date of mailing). The notices addressed to the LICENSOR shall be sent to its address set out above. If any provision is held invalid, all others shall remain in force. The LICENSEE may not assign, pledge, or otherwise transfer this agreement, nor any rights or obligations hereunder in whole or in part to any entity. Paragraph headings are for convenience and shall have no effect on interpretation. In the event that it is necessary to undertake legal action to collect any amounts payable or to protect or to defend against unauthorized use, disclosure, distribution, of the Software hereunder and/or other violation of this Agreement, the LICENSOR shall be entitled to recover its costs and expenses including, without limitation, reasonable attorney fees.

A part of the Software is licensed under the terms of the GNU General Public License, version 2. The text of the license is available at:

http://www.acronis.com/support/licensing/gpl/

More information about the part of the Software licensed under the terms of the GNU General Public License is available at:

http://www.acronis.com/enterprise/support/licensing/

Table of Contents

Chapter 1. Introduction

1.1 What is Acronis® True Image Home?

Acronis True Image Home is an integrated software suite that ensures security of all information on your PC. It can backup the operating system, applications, settings and all of your data, while also securely destroying any confidential data you no longer need. With this software, you can back up selected files and folders, Windows applications' settings, settings and messages of Microsoft e-mail clients — or even the entire disk drive or selected partitions. Should your disk drive become damaged or your system attacked by a virus or malware, you can restore the back-up data quickly and easily, eliminating hours or days of work trying to rebuild your disk drive's data and applications from scratch.

Acronis True Image Home provides you with all the essential tools you need to recover your computer system should a disaster occur, such as losing data, accidentally deleting critical files or folders, or a complete hard disk crash. If failures occur that block access to information or affect system operation, you will be able to restore the system and the lost data easily.

The unique technology developed by Acronis and implemented in Acronis True Image Home allows you to perform exact, sector-by-sector disk backups, including all operating systems, applications and configuration files, software updates, personal settings, and data.

Acronis True Image Home helps you protect your identity as well. Simply deleting old data will not remove it permanently from your computer. Acronis True Image now includes Acronis DriveCleanser that permanently destroys files and wipes personal information from partitions and/or entire disks, as well as a wizard that cleans up your Windows system of all traces of user activity.

You can store backups on almost any PC storage device: internal or external hard drives, network drives or a variety of IDE, SCSI, FireWire (IEEE-1394), USB (1.0, 1.1 and 2.0) and PC Card (formerly called PCMCIA) removable media drives, as well as CD-R/RW, DVD-R/RW, DVD+R/RW, magneto-optical, Iomega Zip and Jaz drives.

When performing scheduled backup tasks, Acronis True Image Home automatically selects a backup mode (full, incremental, differential) in accordance with the backup policy set by the user.

If you are going to install a new hard disk drive, Acronis True Image Home will help you to transfer information from the old one in minutes, including operating systems, applications, documents, and personal settings. After migrating to the new hard disk you can destroy all confidential information on the old one securely. This is the recommended procedure if you intend to donate, throw away, or sell the old hard disk drive.

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

1.2 New in Acronis True Image Home 2009

- **One-Click Protection** – During the first start of Acronis True Image Home after installation, the program will take stock of your computer storage devices and if you have enough free space on one of the hard drives or in the Acronis Secure Zone; it will offer to immediately protect your system by backing up your system volume and Master Boot Record to the storage location of its choice. In addition, Acronis True Image Home will

offer you to refresh such backups regularly (by default, once every seven days). So you simply need to click **Protect** and your system will be protected from a disaster.

- **File search using Google Desktop and Windows Search** – If you use one of these search engines, you will be able to search for files through multiple archives by name or by a part of the name and then restore individual files easily and quickly. In addition, they provide Acronis True Image Home with the ability to perform full-text indexing of the files in tib archives, so you will be able to perform searches of the files content.
- **Making reserve copies of your backups** - You can make reserve copies of your backups and save them on the file system, a network drive, or a USB stick. You have a choice of making a reserve copy as regular (flat) files, a zip compressed file, or a tib file.
- **Support for Zip format** – Now you can create file-level backup archives as zip files. Zip is one of the most widely used and popular archiving formats. In addition, Microsoft Windows has built-in support of this file format making it possible to extract files from backups created by Acronis True Image Home without using the program itself.
- **Consolidation of backup files** – you can create a consistent copy of an archive while deleting selected backups. This allows deleting the backups you do not need anymore from any archive without harming that archive.
- **Automatic consolidation** - you can set limitations for backup archives, namely maximum archive size, maximum number of backups, and maximum storage period for the archive files. In case any of the preset limits are exceeded, Acronis True Image Home will combine the first full backup with the next incremental one into one full backup which will be dated the later backup date. Then, if necessary, this backup will be combined with the next, until the occupied storage space (or number of backups) decreases to the preset limit. Thus, the archive integrity will not be affected, in spite of the fact that the oldest backups will be deleted. This procedure is called automatic consolidation. In the previous versions of Acronis True Image Home a similar procedure was used for automatically managing backup archives in so called backup locations, but now automatic consolidation is available for all archives except those stored on CD/DVDs.
- **Automatic computer shutdown after backup or restoration finishes** – you can now perform a backup at night and go to sleep without bothering about turning off the computer – the program will do this on its own.
- **Automatic backup to a USB flash drive** - if the archive storage location is a USB flash drive, the backup will begin automatically when the device is plugged in, but only when a scheduled backup has been missed. The flash drive must be the same as the one used for all previous backups; if you plug in another flash drive, the backup process won't start.
- **Archive to various places** – you can save full, incremental and differential backups of the same data entity (for example, a partition, disk, E-mail) almost anywhere you like. In the earlier versions of Acronis True Image Home all backups belonging to the same data entity could be stored only in the same place. Now you have ultimate flexibility in choosing a place for backups of the same data entity – a network share, CD/DVD, USB stick, FTP-server, any local internal or external hard drive, etc. Furthermore, you can now give meaningful names to incremental and differential backups, for example, something like "SystemDiskbeforeRepartitioning".
- **More user-friendly** – Completely redesigned user interface and usability enhancements make Acronis True Image Home easier to use than ever before.

1.3 System requirements and supported media

1.3.1 Minimum system requirements

Acronis True Image Home requires the following hardware:

- Pentium processor or higher
- 128 MB RAM
- CD-RW/DVD-RW drive for bootable media creation
- Mouse or other pointing device (recommended).

1.3.2 Supported operating systems

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

- Windows XP SP 3
- Windows XP Professional x64 Edition SP2
- Windows Vista SP 1 (all editions)

Acronis True Image Home also enables the creation of a bootable CD-R/DVD-R that can back up and restore a disk/partition on a computer running any Intel- or AMD- based PC operating system, including Linux®. The only exception is the Intel-based Apple Macintosh, which is not supported in native mode at this time.

1.3.3 Supported file systems

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

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

The Ext2/Ext3, ReiserFS, and Linux SWAP file systems are supported only for disk or partition backup/restore operations. You cannot use Acronis True Image Home for file-level operations with these file systems (file backup, restore, search, as well as image mounting and file restoring from image), as well as for backups to disks or partitions with these file systems.

1.3.4 Supported storage media

- Hard disk drives *
- 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 1.0 / 2.0, FireWire (IEEE-1394) and PC card storage devices
- ZIP®, Jaz® and other removable media

* Acronis True Image Home does not support dynamic and GPT disks.

** An FTP server must allow passive mode file transfers. Data recovery directly from an FTP server requires the archive to consist of files of no more than 2GB each. It is recommended that you change the source computer firewall settings to open Ports 20 and 21 for both TCP and UDP protocols and disable the **Routing and Remote Access** Windows service.

*** Burned rewritable discs cannot be read in Linux without a kernel patch.

1.4 Technical support

Users of legally purchased and registered copies of Acronis True Image Home are entitled to free technical support. If you experience problems installing or using Acronis products that you can't solve yourself by using this guide, then please contact Acronis Technical Support.

More information about contacting Acronis Technical Support is available at the following link: http://www.acronis.com/homecomputing/support/.

In order to open a support trouble ticket, please fill out the Web form on the Acronis site; support will only open a trouble ticket if it is initiated from this form.

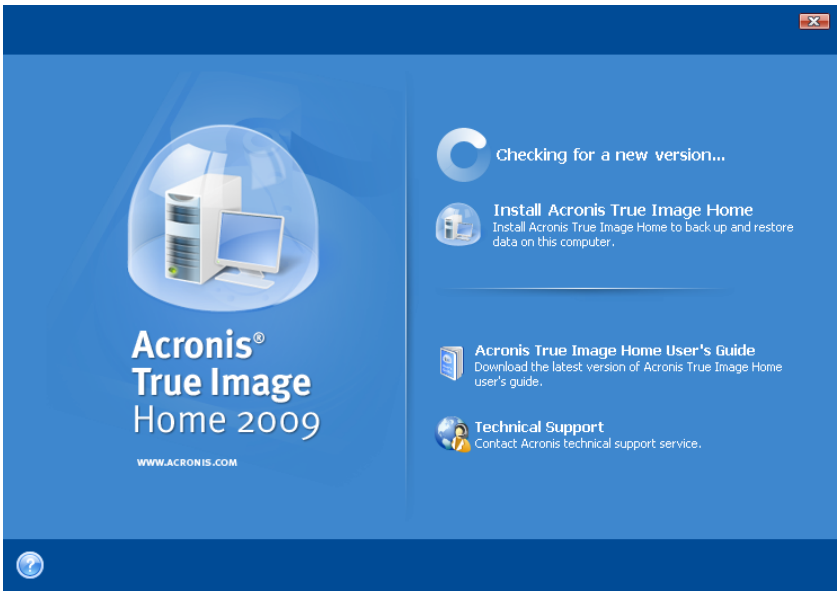
Chapter 2. Acronis True Image Home installation and startup

2.1 Installing Acronis True Image Home

2.1.1 Installing boxed version

To install Acronis True Image Home:

- Run the Acronis True Image Home setup file.
- Before installation, the setup file will check for a newer Acronis True Image Home build on the Acronis website. If available, the newer version will be offered for installation.
- In the Install Menu, select the program to install: Acronis True Image Home.
- Follow the install wizard instructions on the screen.



Typical, **Custom** and **Complete** installation is available. Having pressed **Custom**, you can choose not to install **Rescue Media Builder**.

With **Rescue Media Builder** you can create bootable rescue disks (see details in *Chapter 10. Creating bootable media*). You might not need this tool if you purchased a boxed product that contains a bootable CD. Installing the **Bootable Rescue Media Builder** will allow you to create bootable media or its ISO image at any time from the main program window or running **Bootable Rescue Media Builder** on its own.

When installed, Acronis True Image Home creates a new device in the Device Manager list (**Control Panel -> System -> Hardware -> Device Manager -> Acronis Devices -> Acronis True Image Backup Archive Explorer**). Do not disable or uninstall this device, as it is necessary for connecting image archives as virtual disks (see *Chapter 12. Exploring archives and mounting images*).

2.1.2 Installing Acronis True Image Home from Acronis website

To install Acronis True Image Home:

- Click on the download link, save the downloaded executable file to disk and then run it (or choose to run the file after downloading).
- If you have purchased the commercial version of the program, enter (or paste) the serial number. Otherwise, the installer will install the trial version, which will remain fully operational for 15 days.

Typical, **Custom** and **Complete** installation is available. Having pressed **Custom**, you can choose not to install **Rescue Media Builder**.

2.2 Extracting Acronis True Image Home

When installing Acronis True Image Home, you can save the setup (.msi) file on a local or network drive. This will help when modifying or recovering the existing component installation.

To save the setup file:

- Run the Acronis True Image Home setup file.
- In the Install Menu, right-click on the program name and select **Extract**.
- Select a location for the setup file and click **Save**.

Recovering or updating the existing Acronis True Image Home installation with use of the .msi file must be done from the command line as follows:

1. Choose **Start -> Run**
2. Type *cmd*.
3. When the command-line interpreter window opens, type the following command:
   msiexec /i path_to_msi_file\msi_file_name.msi REINSTALL=ALL REINSTALLMODE=vomus
4. After the install wizard window opens, choose **Typical**, **Custom** or **Complete** installation for repairing or changing the program's components.

2.3 Running Acronis True Image Home

You can run Acronis True Image Home in Windows by selecting **Start -> Programs -> Acronis -> Acronis True Image Home -> Acronis True Image Home** or by clicking on the appropriate shortcut on the desktop.

If your operating system does not load for some reason, you can run Acronis Startup Recovery Manager. However, this must be activated prior to use; see *3.4 Acronis Startup Recovery Manager* to learn more about this procedure. To run the program, press F11 during bootup when you see a corresponding message that tells you to press that key. Acronis True Image Home will be run in the standalone mode, allowing you to recover the damaged partitions.

If your disk data is totally corrupted and the operating system cannot boot (or if you have not activated Acronis Startup Recovery Manager), load the standalone Acronis True Image Home version from the bootable media, supplied with the retail box or created by you using Rescue Media Builder. This boot disk will allow you to restore your disk from a previously created image.

2.4 Upgrading Acronis True Image Home

If you already have Acronis True Image Home 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, so if you roll back Acronis True Image Home to an older version, you likely will have to re-create the archives using the older version. We strongly recommend that you create new bootable media after each Acronis True Image Home upgrade.

2.5 Removing Acronis True Image Home

Select **Start -> Settings -> Control panel -> Add or remove programs -> <Acronis True Image Home> -> Remove**. Then follow the instructions on the screen. You may have to reboot your computer afterwards to complete the task.

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

Chapter 3. General information and proprietary Acronis technologies

3.1 The difference between file archives and disk/partition images

A backup archive is a file or a group of files (also called “backups” in this guide), that contains a copy of selected file/folder data or a copy of all information stored on selected disks/partitions.

When you back up files and folders, only the data, along with the folder tree, is compressed and stored.

Backing up disks and partitions is performed in a different way: Acronis True Image Home stores a sector-by-sector snapshot of the disk, which includes the operating system, registry, drivers, software applications and data files, as well as system areas hidden from the user. This procedure is called “creating a disk image,” and the resulting backup archive is often called a disk/partition image.

By default, Acronis True Image Home stores only those hard disk parts that contain data (for supported file systems). Further, it does not back up swap file information (pagefile.sys under Windows XP/Vista) and hiberfil.sys (a file that keeps RAM contents when the computer goes into hibernation). This reduces image size and speeds up image creation and restoration. However, you might use the **Create an image using the sector-by-sector approach** option that lets you include all of the sectors of a hard disk in an image.

A partition image includes all files and folders. This includes all attributes (including hidden and system files), boot record, and FAT (file allocation table); as well as files in the root directory and the zero track of the hard disk with master boot record (MBR).

A disk image includes images of all disk partitions as well as the zero track with master boot record (MBR).

By default, files in all Acronis True Image Home archives have a “.tib” extension. Do not change this file extension.

It is important to note that you can restore files and folders not only from file archives, but from disk/partition images too. To do so, mount the image as a virtual disk (see *Chapter 12. Exploring archives and mounting images*) or start the image restoration and select **Restore specified files or folders**.

3.2 Full, incremental and differential backups

Acronis True Image Home can create full, incremental and differential backups.

A **full backup** contains all data at the moment of backup creation. It forms a base for further incremental or differential backup or is used as a standalone archive. A full backup has the shortest restore time compared to incremental or differential ones.

An **incremental backup** file only contains data changed since the last backup of any type (full, incremental, or differential one). Therefore, it is smaller and takes less time to create, but as it doesn’t contain all data; all the previous backups and the initial full backup are required for restoration.

Unlike an incremental backup, when every backup procedure creates the next file in a “chain”, a **differential backup** creates an independent file, containing all changes since the

last full backup. Generally, a differential backup will be restored faster than an incremental one, as it does not have to process through a long chain of previous backups.

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 files. If you are interested in saving only the last data state to be able to restore it in case of system failure, consider the differential backup. It is particularly effective if your data changes tend to be few compared to the full data volume.

The same is true for incremental backup. These are most useful when you need frequent backups and the ability to roll back to a specific point in time. Having created a full backup once, if you then create an incremental backup each day of a month, you will get the same result as if you created full backups every day. Incremental images are considerably smaller than full or differential images.

Incremental or Differential?

The difference is typically that in an incremental backup, only the files changed or added since the last time the backup ran are added to the archive. With a differential backup, all the files changed or added since the initial full backup, are added to the archive. Thus, differential backups take longer to run than incremental backups. When restoring from an incremental backup, the program must copy the entire initial backup and then step through each of the previous backups to retrieve all the updated files. A differential backup, on the other hand, can be restored more quickly because the software must copy only the original backup and the most recent 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.

3.3 Acronis Secure Zone™

The Acronis Secure Zone is a special, hidden partition for storing backups on the computer system itself. For archive security purposes, ordinary applications cannot access it. In the Acronis True Image Home wizards' windows, the zone is listed along with all partitions available for storing archives. The Acronis Secure Zone is necessary if you plan to use the Acronis Startup Recovery Manager feature (see below).

The Acronis Secure Zone is available as a location to store backup files as long as there is free space in the zone. If there is not enough space, older backups will be deleted to create free space.

Acronis True Image Home uses the following approach to clean up the Acronis Secure Zone:

- If you are in the process of creating a backup and there is not enough free space in the zone to create it, the program will display a dialog which warns you that the Acronis Secure Zone is full. You can click **Cancel** to cancel the backup operation. In that case, you may want to increase the size of the Acronis Secure Zone and then run the backup operation again. If you want to free some space in the zone, click **OK** and the oldest full backup of the type being created will be deleted with all subsequent incremental/differential backups, then the backup operation will recommence.
- If deleting the oldest backup does not free enough space, you will get the same warning message again. You may delete the next oldest backup (if any) and repeat this until all the previous backups are deleted.

- If after deleting all the previous backups there is still not enough space for completing the backup, you will get an error message and the backup will be canceled.

The program distinguishes only two types of backups in the zone: disk image backups and file-level backups. My Data, System State, My E-mail, and My Application Settings backups are considered as file-level type backups. For example, if you have an e-mail backup (My E-mail) in the zone and there is not enough space for backing up some folders (My Data), the program will delete the e-mail backup to free space for the folders backup.

You can back up data automatically on a schedule (see *Chapter 8. Scheduling tasks*). In order to not worry about zone overflow during a scheduled backup, it is recommended to enable automatic consolidation of backups in the zone by setting a limit on the archive size (see *5.3.7 Setting automatic consolidation*), though taking into account the above approach this recommendation is best suited for storing in the zone backups of the same type. However, if you keep long chains of incremental backups, it will be good practice to periodically check the zone free space, indicated on the **Protection State -> System Information** screen or on the second screen of the **Manage Acronis Secure Zone Wizard**.

For information on how to create, resize or delete Acronis Secure Zone using this wizard, see *Chapter 9. Managing Acronis Secure Zone*.

3.4 Acronis Startup Recovery Manager

3.4.1 How it works

The Acronis Startup Recovery Manager lets you start Acronis True Image Home without loading the operating system. With this feature, you can use Acronis True Image Home by itself to restore damaged partitions, even if the operating system won't start up for some reason. As opposed to booting from Acronis removable media, you will not need a separate media or network connection to start Acronis True Image Home.

3.4.2 How to use

To be able to use Acronis Startup Recovery Manager at boot time, prepare as follows:

1. Install Acronis True Image Home.

2. Create Acronis Secure Zone on the hard disk (see *Chapter 9. Managing Acronis Secure Zone*).

3. Activate Acronis Startup Recovery Manager. To do so, click **Activate Acronis Startup Recovery Manager** and follow the wizard's instructions.

If you try to activate Acronis Startup Recovery Manager before you created the Acronis Secure Zone, you will be prompted to create the zone; then the Acronis Startup Recovery Manager will be activated. If the Acronis Secure Zone already exists, Acronis Startup Recovery Manager will be activated immediately.

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 have to reactivate them after activating the Startup Recovery Manager. 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.

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 Home that differs only slightly from the complete version. For information on restoring damaged partitions, see *Chapter 6. Restoring backup data*.

Be careful! Drive letters in standalone Acronis True Image Home might sometimes differ from the way Windows identifies drives. For example, the D: drive identified in the standalone Acronis True Image Home might correspond to the E: drive in Windows.

You won't be able to use the previously activated Acronis Startup Recovery Manager if the Try&Decide mode is started.

3.5 Viewing disk and partition information

You can change the way data is represented in all schemes you see in various wizards.

To the right are three icons: **Arrange Icons by, Choose Details** and **i (Display the properties of the selected item)**, the latter duplicated in the context menu opened by right-clicking objects.

To sort messages by a particular column, click the header (another click will switch the messages to the opposite order) or the **Arrange Icons by** button and select the column.

To select columns to view, right-click the headers line or left-click the **Choose Columns** button. Then flag the columns you want to display. When left-clicking the **Choose Columns** button, you can also change the display order of columns using the **Move Up** and **Move Down** buttons.

If you click the **i (Display the properties of the selected item)** button, you will see the selected partition or disk properties window.

This window contains two panels. The left panel contains the properties tree and the right describes the selected property in detail. The disk information includes its physical parameters (connection type, device type, size, etc.); partition information includes both physical (sectors, location, etc.), and logical (file system, free space, assigned letter, etc.) parameters.

You can change the width of a column by dragging its borders with the mouse.

3.6 Try&Decide™

The Acronis True Image Home Try&Decide feature allows you to perform potentially dangerous operations such as software installation or opening e-mail attachments without putting your PC at risk. It does this by creating essentially a controlled, secure, temporary workspace that is insulated from the rest of your computer. If the system crashes or your computer stops responding during these operations, you should revert the system to the previous state by discarding changes made in the Try&Decide mode. If operations are successful, you have a choice of applying the changes to the real system. (For more details see *Chapter 7 Try&Decide.*)

3.7 Acronis DriveCleanser, File Shredder, and System Clean-up

Acronis True Image Home contains utilities for secure destruction of data on an entire hard disk drive, individual partitions, as well as for erasing individual files and eliminating user system activity traces. When replacing your old hard drive with a new, higher-capacity one, you may unwittingly leave on the old disk lots of personal and confidential information that can be recovered, even if you have reformatted it. The Acronis DriveCleanser provides for the destruction of confidential information on hard disk drives and/or partitions with the help of techniques that meet or exceed most national and state standards. You can select an

appropriate data destruction method depending on the importance of your confidential information. The File Shredder provides the same capabilities for individual files and folders. Finally, the System Clean-up wizard ensures elimination of all your activity traces; while working with a PC, you leave thousands of bytes of evidence showing your actions (records in various system files) that you don't even know about. This could include user names and passwords, as well as other personal information that could be used to steal your identity if it fell into the wrong hands. This utility wipes them completely from the disk drive.

3.8 Support for Zip format

Now you will be able to retrieve files from backups anywhere without using Acronis True Image Home, if you choose the zip format instead of the tib format. You can back up files, for example, to a USB stick and retrieve files from such archives on your notebook at home without installing Acronis True Image Home, because the most widely used operating systems, namely Microsoft Windows and Mac OS X have built-in support of the zip file format.

Please, be aware that built-in support of zip files in Windows does not cover operations with multivolume zip archives, and zip archives exceeding 4GB in size or which contain files of more than 4GB each.

The Zip format is available when backing up files and/or folders as well as when making reserve copies of your backups. Acronis True Image Home provides for the zip format most of the functionality available for the tib format, except password protection and encryption – you can schedule backups, validate zip backup archives, restore files and folders from zip archives, make incremental and differential backups, and so on.

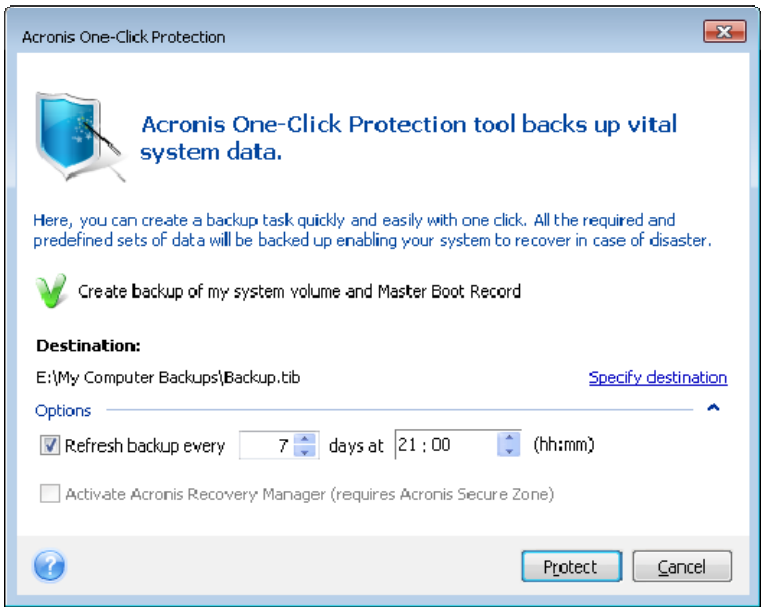
Acronis True Image Home can restore and validate only its own zip archives. If a zip archive was created by a file archiver program, it cannot be restored and validated by Acronis True Image Home.

Chapter 4. Getting to know Acronis True Image Home

4.1 Acronis One-Click Protection

Acronis One-Click Protection tool allows you to begin protecting your computer as soon as you install Acronis True Image Home. During the first start of the just installed Acronis True Image Home, the program will offer you to protect your computer by immediately backing up its system volume and Master Boot Record (MBR) as well as scheduling subsequent full backups.

The Acronis One-Click Protection tool performs only full backups of the system volume; scheduling an incremental or differential backup is not possible. In addition, it does not support backup of drives protected by BitLocker Drive Encryption in Windows Vista.



Acronis True Image Home will take stock of your computer's configuration and then offer the optimum destination for backups.

For this purpose the program will use the following algorithm:

1) First of all the program estimates the space required for operation of the One-Click Protection tool. As the *average* compression ratio when backing up data into tib files is 2:1, you can use this value as a guide. Let's say your system partition has 20GB of programs and data. Under normal conditions, that will compress down to approximately 10GB and the disk space required for operation of the One-Click Protection tool might amount to 10GB plus 250 MB for temporary files.

2) If there is an external hard drive, your backups will be stored on that drive, since such a backup place will provide maximum protection for your computer. The safety of your computer will be even greater, if you get into the habit of disconnecting the external drive and storing it at another location.

3) If you have upgraded from a previous Acronis True Image Home version and already have the Acronis Secure Zone, the program will check its size and if the zone size is sufficient

for backup, it will use the Acronis Secure Zone (if Acronis Startup Recovery Manager is activated, the program will update its bootable components). In case the zone is too small for backing up the system partition, the program will move to the next best option.

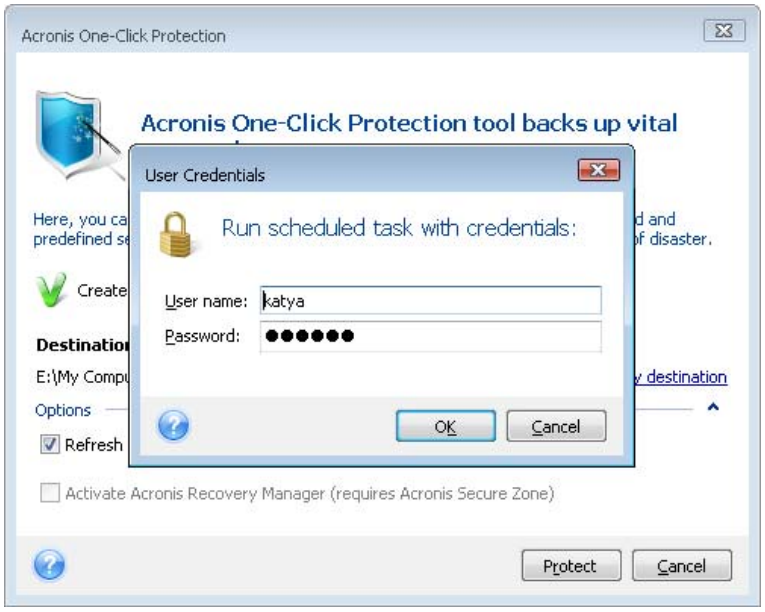
4) If the first two options are unavailable but you have at least two internal hard drives, the program will back up to a non-system hard drive using a partition with the maximum free space.

5) When your computer has only one hard drive:

- If the hard drive has several partitions (not counting hidden ones), then the program will use a non-system partition with maximum free space
- If the drive has only one non-hidden partition, namely, the system partition:
  - If the program detects any internal hidden partition (non-ASZ), it will back up to the system partition
  - If the partition has enough free space, the program will create the Acronis Secure Zone and back up there as well as activate Acronis Startup Recovery Manager
  - If the partition has insufficient free space, the program will use the writing CD/DVD drive (if it exists) and will append Acronis One-Click Restore and a full standalone version of Acronis True Image Home as well. In this case the program will use the maximum compression ratio

After applying this algorithm to your computer configuration, Acronis True Image Home will offer the optimum place for storing your backups. If you would prefer another storage location, click the **Specify destination** link and select the storage location most suitable for you.

Clicking **Protect** will start the backup task. But before proceeding with the backup, the program will ask you under whose user credentials the subsequent scheduled backups will run.

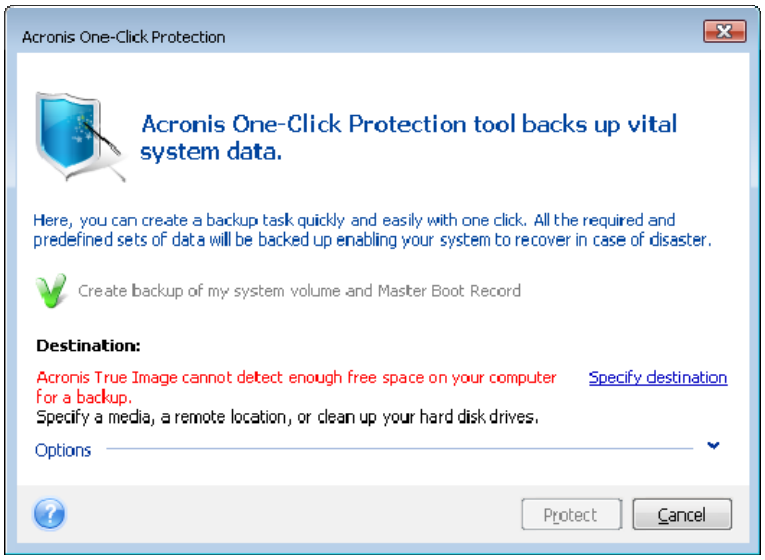


Clicking **Cancel** will cancel One-Click Protection. If you decide to use this feature later, click **Home** on the sidebar and then choose **One-Click Protection** on the right pane of the Welcome screen.

When archive storage location is a USB flash drive, the backup will begin automatically when the device is plugged in but only if a scheduled backup has been missed. The USB flash drive must be the same as the one used for all previous backups; if you plug another flash drive, the backup process won't start.

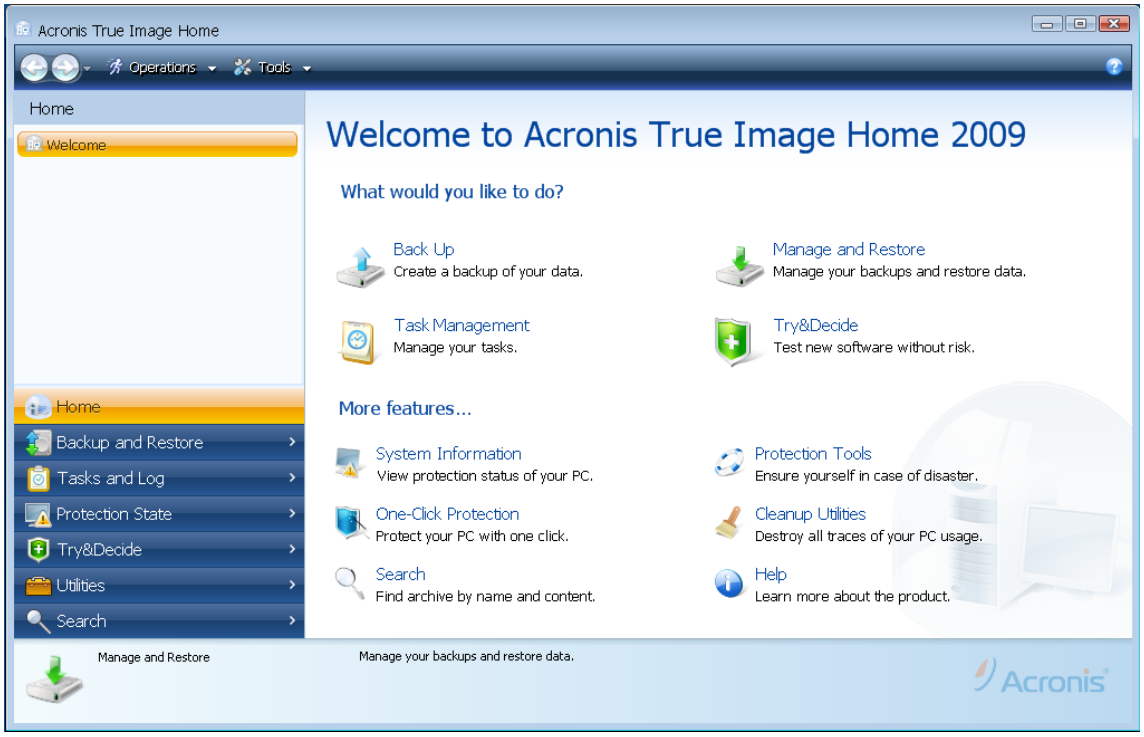
The system will always keep the last backup archive. When a task for another backup begins, the older backup is deleted – freeing space for the backup in progress.

If there is not enough free space on your PC, the program will notify you that it cannot back up the system volume and will suggest that you specify a destination for backup yourself.



4.2 Program workspace

Starting Acronis True Image Home takes you to the Welcome screen. This screen provides quick access to practically all the program's functionality.



Clicking the items in the right pane takes you to the corresponding wizard or screen where you can either start the selected task or function right away or make further selections.

All the features listed in the right pane are duplicated on the left side of the screen occupied by the so called *sidebar*. The sidebar also provides easy access to all functionality of Acronis True Image Home. The main functions are listed in the lower part of the sidebar. If you choose an item in the lower part, the upper part of the sidebar displays subitems related to the chosen item (if any) and the right part of the main window shows detailed information for the current subitem or a list of options available for that subitem.

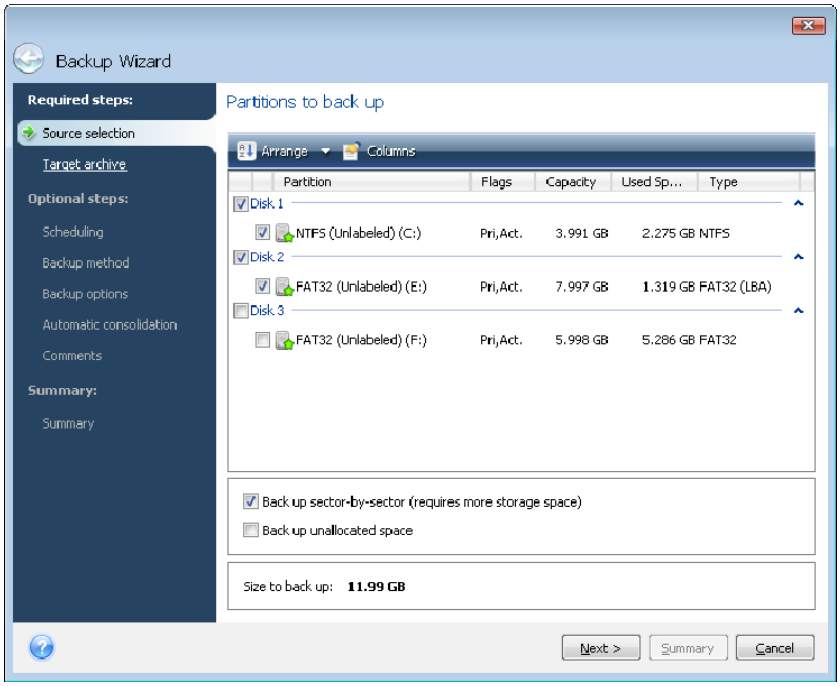
Status bar

At the bottom of the main window, there is a status bar that briefly describes the selected operation or screen. If you select a backup archive, task or log, the status bar will show information on the selected item.

Taskbar notification area icon

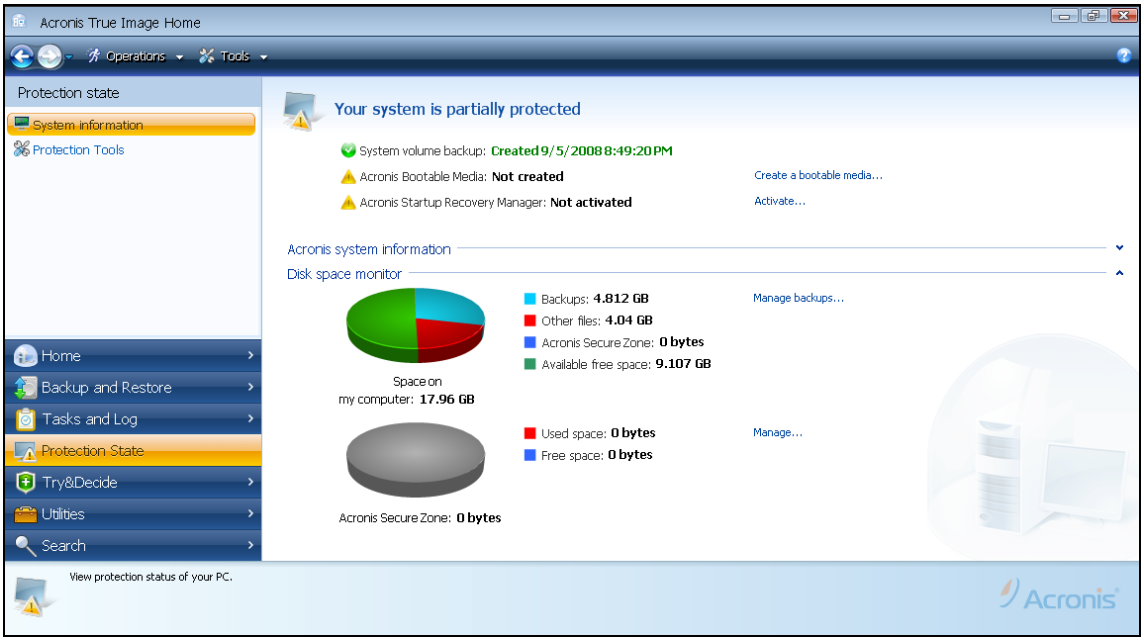
During most of the operations, a special indicator icon appears in the Windows taskbar notification area (the right portion of the status bar with the clock). If you mouse over the icon, you will see a tool tip indicating the operation's progress. Right-clicking on the icon opens a contextual menu where you can change process priority or cancel the operation if necessary. This icon doesn't depend on the main program window being open. It is present for background execution of scheduled tasks as well.

Acronis True Image Home uses wizards, which guide you through many operations. Like the main program window, wizards also have the sidebar listing all the steps (both required and optional) needed for completing the operation. For example, see the Backup Wizard screenshot below.

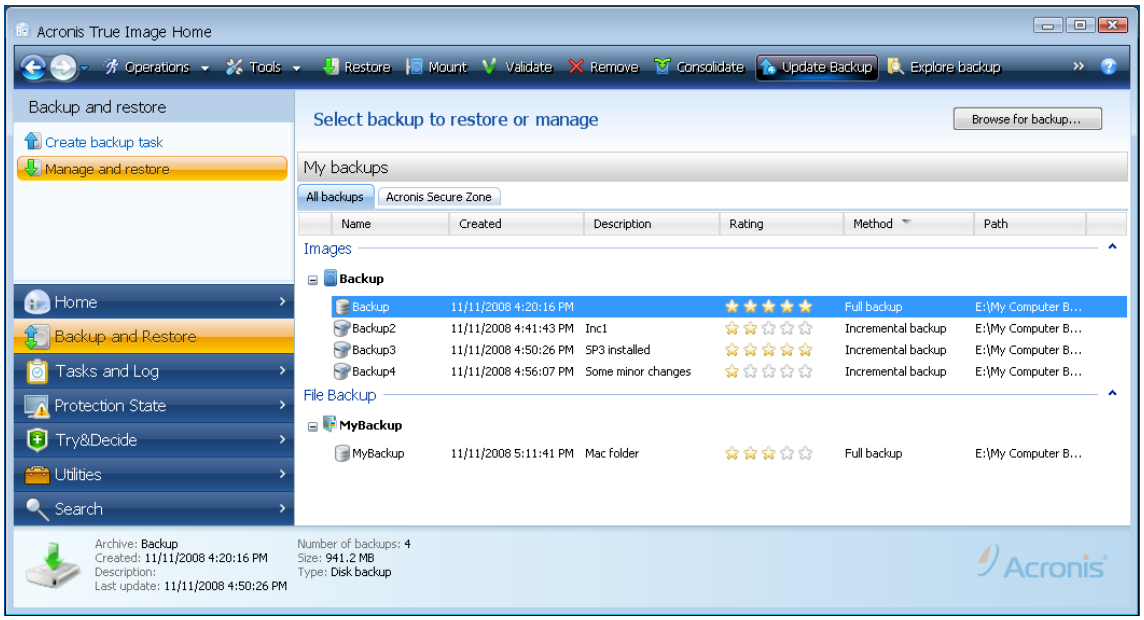


The completed steps are marked with green checkmarks. The green arrow shows the current step. After you complete all the required steps, the **Summary** button becomes available. If you wish to omit the optional steps, click **Summary**, read the summary of the operation to be performed (to make sure that the default settings satisfy you) and then click **Proceed** to start the task. Otherwise proceed to the optional steps where you can change the default settings for the current task.

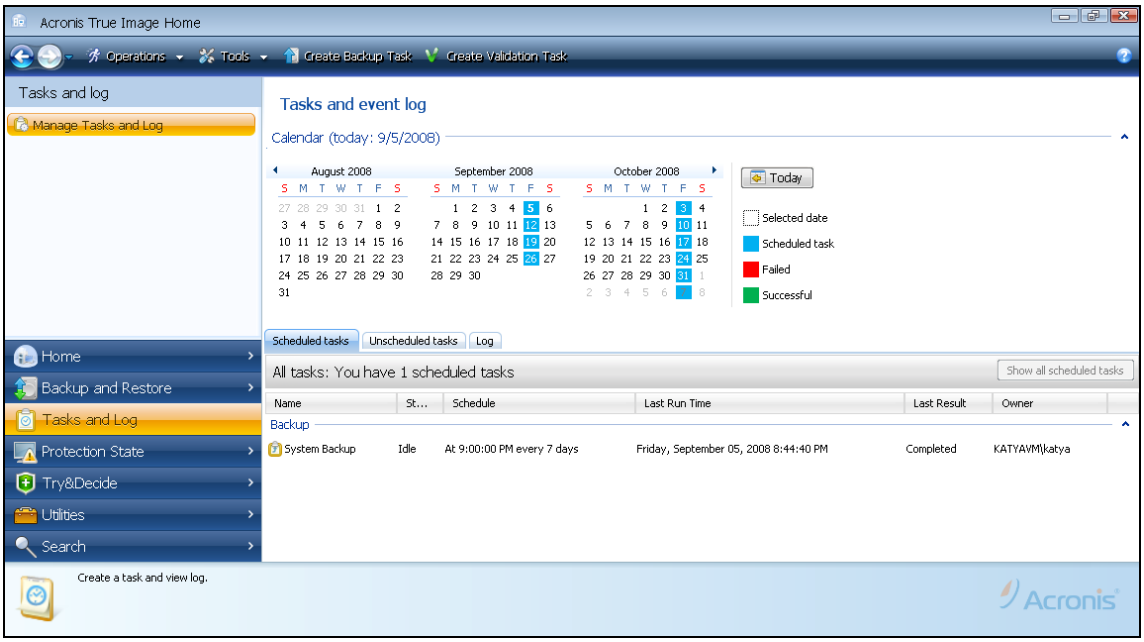
And now let's get acquainted with some other screens you will use while working with Acronis True Image Home. One of the most important and informative screens is Protection State. It shows a wealth of information on the protection state of your computer and permits taking measures that will enhance protection of your system (or provide it if the system is as of yet unprotected) – the screen has links for creating a system partition backup, and bootable rescue media, for activating Acronis Startup Recovery Manager. In addition, you will get information on the number of backup archives, as well as the date and time of the last backup, number of scheduled tasks and the last task result, and state of the Try&Decide mode. The screen also shows information on the state of your hard disks (total capacity, free space, space occupied by backup archives and other files), information on the state of the Acronis Secure Zone (free and occupied space).



To go to one more screen of interest, click **Backup and Restore -> Manage and restore** on the sidebar. This screen gives detailed information on your backup archives and provides for quickly performing operations on these archives – Restore, Validate, Remove, Consolidate, Update, Explore backup archives and Mount image backups by a single click on a button on the toolbar. Clicking the button starts the appropriate wizard or performs the appropriate action. On this screen you can assign ratings to your backups, for instance, you may want to assign a high rating to an important backup. A backup rating is indicated by the number of "stars" in the **Rating** column (more stars means higher rating). The default rating is three stars, but you can raise or lower it by clicking on the stars in the column. The assigned backup ratings may be helpful, for example, when sometime later you will need to consolidate the backups stored in an archive – it will be easier to choose which backups to keep after consolidation. For more information on manual backup consolidation see *11.5 Consolidating backups*. In addition, these ratings might save you a lot of time you will otherwise spend on exploring multiple files in your backup archives trying to guess which of the outdated backups can be deleted without losing important data.



Another useful screen shows logs of program operations and scheduled tasks. A calendar provides quick access to the logs (for past dates) or tasks (for future dates). You just click on a desired date. For more information see *11.3 Viewing Tasks and Logs*.



We will not bore you with a description of other screens, because many of them are self-explanatory and some are described in the appropriate chapters of this guide. In addition, all screens have brief descriptions of the features they allow to access or use and you can always open contextual help by clicking the corresponding button.

By the way, you can also select all the features through the main program menu, which is always at your disposal on the toolbar.

Chapter 5. Creating backup archives

5.1 Preparing for your first backup

First of all you must decide where you will store your backups. Acronis True Image Home supports quite a lot of storage devices. For more information see *1.3.4 Supported storage media*. Since hard disk drives are now quite inexpensive, in most cases purchasing an external hard drive will be an optimal storage device for your backups. In addition to enhancing the security of your data – you can keep it off-site (for example, at home if you back up your office computer and vice versa); many models are hot-pluggable, so you can attach and detach the drive as you need. You can choose various interfaces – USB 2.0, FireWire, eSATA depending on the configuration of your computer ports and the required data transfer rate. In many cases the best choice will be an external USB 2.0 hard drive, though it has a pitfall – such a drive may slow down if it works together with slower USB 1.1 devices. If you have a Gigabit Ethernet home network and a dedicated file server or NAS, for example, Buffalo TeraStation 1.0 TB NAS Gigabit Ethernet Home Server, you can store backups on the file server or NAS practically like onto an internal drive. Blank optical discs such as CD-R/RW, DVD-R/RW, DVD+R/RW are very cheap, so they will be the lowest cost solution for backing up your data, though the slowest one (not counting backups to an FTP server through a slow Internet connection).

5.2 Selecting what data to back up

As operating systems and application software become ever larger (for example, Windows Vista x64 requires 15GB of free space on a hard disk), usually it will take you several hours to reinstall your operating system and application software from original CDs or DVDs on a new hard disk. Furthermore, the practice of buying application software by downloading from the Internet is becoming more and more popular. If you lose your registration information, for example, the activation key and/or registration number, which are usually sent by software vendors through e-mail, you may have problems with restoring your right to use the application. So making a backup of your entire system disk (making a disk image) will save you a lot of valuable time in case of a disaster, as well as safeguard you against other possible problems.

Backing up the entire system disk (creating a disk image) takes more disk space, but enables you to restore the system in minutes in case of a system crash or hardware failure. Moreover, the imaging procedure is much faster than copying files and could speed up the backup process significantly when it comes to backing up large volumes of data (see details in *3.1 The difference between file archives and disk/partition images*).

You might think it would take a while to make a copy of your entire hard disk, but the proprietary technologies used in Acronis True Image Home ensure that image creation is quite fast. And the program can also back up *incrementally or differentially,* so after the first time, updating your image to reflect the current state of your hard disk requires only copying the files that are new or changed and will require much less time. Because images can save you a lot of time when you need to recover the operating system, it is recommended that you make them part of your backup strategy. In our opinion creating your system volume image backup is vital for protecting your computer system from a disaster, so now Acronis True Image Home offers to back up the system volume and Master Boot Record during the first start of the program after installation. For more information see *4.1 Acronis One-Click Protection*.

Images, however, provide no defense against damaged files. If your hard disk contains damaged files when you are making an image, those problems will appear in the image as well.

For that reason, although we strongly recommend you to create images of your hard disk on a regular basis, that is just part of a reliable backup strategy. You should supplement the images with file archives.

Do you need file-level backups?

Do you have bank records, e-mails, photos, etc. you accumulated on your computer for several years? Hardware and software can be replaced, your personal data cannot.

Though there may be some exceptions, the optimal backup strategy for most users consists of creating both images and file-level backups.

After the initial full backup, file-level backups usually take comparatively little time to run, making it easy to back up your data once (or even several times) each day. This ensures that your most recent backup is never more than a day old. Because they also offer insurance against accidental deletion (or change) and file damage, file-level backups are an essential part of a good backup strategy. But file-level backups alone are not sufficient for two main reasons:

1) If your startup hard drive completely fails, you won't be able to do any work at all until you've replaced it; and 2) Reinstalling an operating system and applications from their original CDs or DVDs is a lengthy and arduous procedure that you could avoid (or speed up greatly) with an image of your hard disk.

You should create images of your primary disk and any other volume you normally use. If you have multiple partitions on a drive, it is advisable to include all of them in the image, because failure of the hard drive in most cases will mean that all the partitions it contains also fail.

Here are some more recommendations you can use to plan your backups. You should store your system drive image in the Acronis Secure Zone or, better still, on a hard drive other than your primary hard disk C:. This gives an additional guarantee that you will be able to recover your system if your primary hard disk drive fails. You should also keep your personal data separate from your operating system and applications, for example, on disk D:. Such an arrangement allows speeding up the creation of data disk (or partition) images and reduces the amount of information you will need to restore.

5.3 Performing backup

1. Start Acronis True Image Home

2. Choose **Backup and Restore** in the lower area of the sidebar and the **Create backup task** item will be selected by default.

3. Select what type of data you want to back up.

Acronis True Image Home offers you the following backup types:

My Computer (image backup of any set of disks/partitions)

My Data (file-level backup of any set of files, folders, or an entire file category)

System State (file-level backup of system files, drivers, etc.)

My E-mail (file-level backup of Microsoft Outlook, Microsoft Outlook Express, and Windows Mail settings and messages).

My Application Settings (file-level backup of Windows applications settings)

File-level backup operations are supported only for the FAT and NTFS file systems.

We do not recommend backing up any data from drives protected by BitLocker Drive Encryption feature, because in most cases restoring data from such backups will be impossible.

Selecting a backup type starts the Backup Wizard, which will guide you through the steps of creating a backup task. You can also start the Backup Wizard by choosing **Operations -> Backup** in the main menu and then selecting a backup type. Depending on the backup type chosen, the number of steps in the Backup Wizard may change. For example, in case of backing up the System State, the program backs up predefined data and requires the minimum number of settings for configuring a backup task.

5.3.1 Selecting data for backup

When the Backup Wizard screen appears, select the data you wish to back up (in case of choosing the System State, this step will be omitted).

My Computer - select the disks or partitions to back up. You can select a random set of disks and partitions. The wizard's right pane shows the hard drives of your computer. Selecting a hard drive results in selecting all partitions on that drive. If a hard drive has more than one partition, you may want to select individual partitions for backing up. To do so, click on the Down arrow at the right of the drive's line. Select the desired partition(s) in the displayed partition list. By default the program copies only the hard disk sectors that contain data. However, sometimes it might be useful to make a full sector-by-sector backup. For example, perhaps you deleted some files by mistake and want to make a disk image before trying to undelete them because sometimes un-deleting may create havoc in the file system. To make a sector-by-sector backup, select the **Use the sector-by-sector approach** box. Please note that this mode increases processing time and usually results in a larger image file because it copies both used and unused hard disk sectors. In addition, when configuring a sector-by-sector backup of a complete hard disk you can include in the backup unallocated space on the hard disk by selecting **Back up unallocated space**. Thus you will include in the backup all physical sectors on the hard drive.

My Data - select the file category(s) to back up: **documents, finance, images, music,** and **video**. Each category represents all files of associated types found on the computer's hard drives. Furthermore, you can add any number of custom categories containing files and folders. The new categories will be remembered and displayed along with the above. You can change contents of any custom or default file category (edit the category) or delete it. The default file categories cannot be deleted.

For more information on custom categories see *5.4.12 Creating a custom data category for backups*. If you do not want to keep custom contents of the current backup by creating a data category, simply select the files/folders from the tree. This set will be effective only for the current backup task. File filtering can be applied to manually added folders in the optional **Source files exclusion** step.

My Application Settings - back up custom settings of Windows applications. This is a subset of file-level backup that backs up predefined folders and requires minimum user selections. The program displays a list of supported applications that has been found on the computer, sorted by categories. You can select a random set of categories and applications.

It is important to note that the program backs up only your settings, and not the application executable files. If an application seems to malfunction or ceases to run, reinstall it using the last updates and then recover your settings from the backup.

To select all the supported applications found on the computer for backing up, check the Installed Applications box. For instant messenger applications, the program will back up both the settings and history.

The list of supported applications will be expanded gradually. Updates will be available with new program builds or via the Internet.

My E-mail - Acronis True Image Home offers a straightforward way to back up messages, accounts and settings for Microsoft Outlook 2000, 2002, 2003, 2007, Microsoft Outlook Express, and Windows Mail. E-mail backup is a subset of file-level backups that backs up predefined folders and requires minimum user selections. However, if need be, you can select Microsoft Outlook components and folders individually. The list of supported e-mail clients will be gradually built up. Updates will be available with new program builds or via the Internet.

You can select the following items:

Messages contained in .PST/.DBX Database Files

E-mail accounts

For Microsoft Office Outlook 2000, 2002, 2003, 2007

- Mail Folders
- Calendar
- Contacts
- Tasks
- Notes
- Signatures
- News Folders
- User Settings
- Address Book

For Microsoft Outlook Express

- Mail Folders
- Address Book (select Windows Address Book).

Acronis True Image Home provides backup of IMAP (Internet Messages Access Protocol) mail folders for Microsoft Outlook. This means that you can back up folders stored on a mail server. For Microsoft Outlook Express and Windows Mail only local e-mail folders backup is available.

5.3.2 Selecting the target archive location

Select the destination location for the backup and specify the archive name.

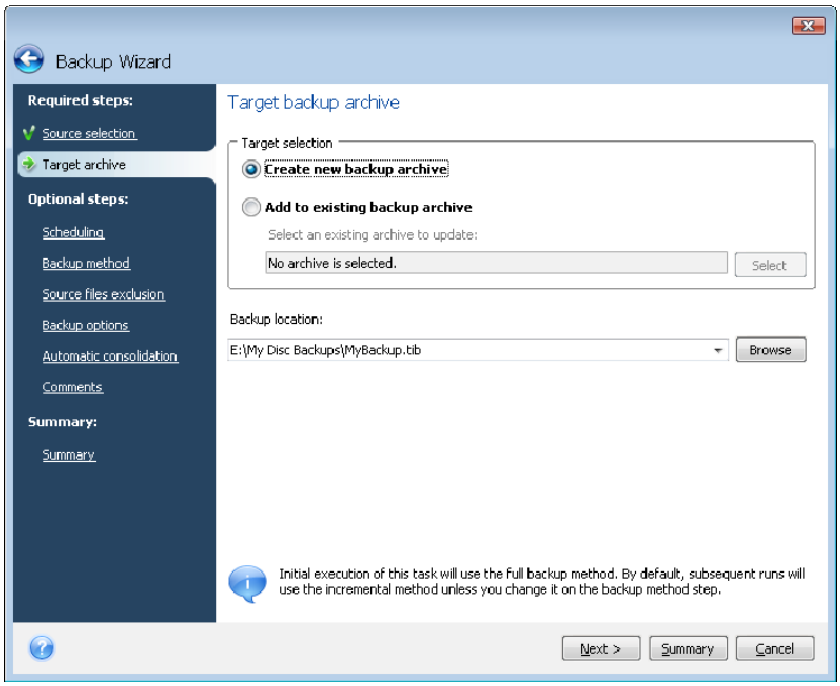
If you are going to create a new archive (i.e. perform a full backup), select **Create new backup archive** and enter the path to the archive location and new archive file name in the **Backup Location:** field below or click **Browse**, select the archive location on the directory tree and enter the new file name in the **File name** line, or use the file name generator (a button to the right of the line).

When you have chosen the **My Data** backup type for backing up files and/or folders, you can select the zip archive type. For more information see *3.8 Support for Zip format*.

CD/DVD and the Acronis Secure Zone are not supported as locations for zip archives.

If you want to append an incremental or differential backup file to an existing archive, select **Add to existing backup archive** and click the **Select** button to select the existing archive you are going to update. If the archive already has incremental or differential backups, you can select any of the target archive files. It doesn't matter which one you select, as the program recognizes them as a single archive.

If you want to change the location of added backup files, browse for a new backup location after clicking the **Browse** button, otherwise leave the location the same as that of the existing archive.



The "farther" you store the archive from the original folders, the safer it will be in case of disaster. For example, saving the archive to another hard disk will protect your data if the primary disk is damaged. Data saved to a network disk, an FTP server or removable media will survive even if all your local hard disks are damaged. You can also use the Acronis Secure Zone for storing backups (see details in *3.3 Acronis Secure Zone*).

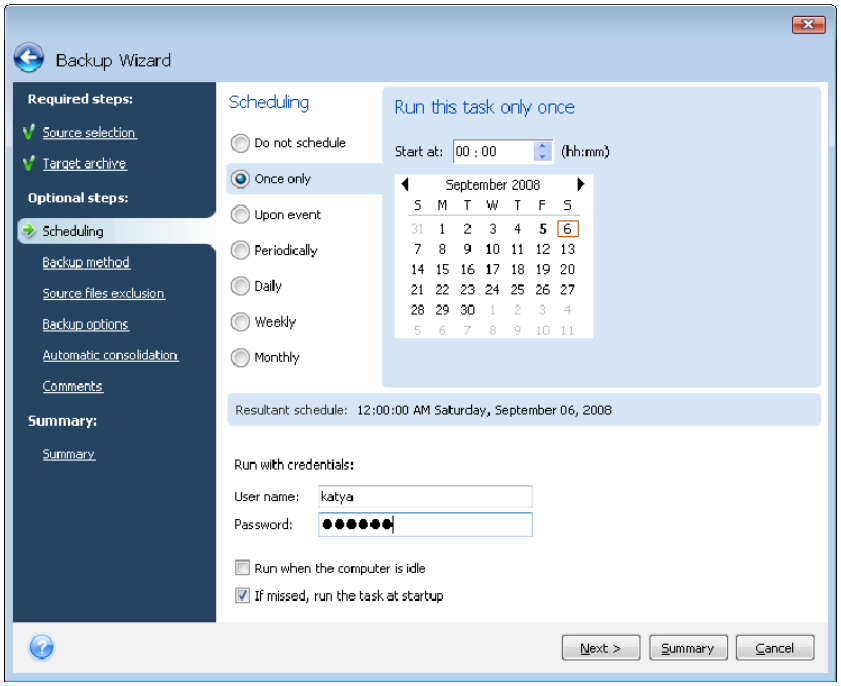
See notes and recommendations for supporting FTP servers in *1.3.4 Supported storage media*.

After selecting the archive location and naming the backup archive to be created, you have completed all the required steps for a backup task and this is confirmed by the fact that the **Summary** button becomes selectable. All the remaining steps are optional and in many cases you may omit them and just click **Summary** and then **Proceed** on the Summary page. For example, when you want to proceed with backup right away, you can omit the **Scheduling** step. If you do not want to exclude any files from the backup, you can omit the **Source files exclusion** step. When you want to use the default backup options, you can omit the **Backup options** step, and so on.

Now let's see what optional steps you can set up while configuring a backup task.

5.3.3 Scheduling

By default, the **Do not schedule** option is chosen so the task will run after completing the wizard and clicking **Proceed** on the Summary page. However, you may wish to schedule the task being configured by choosing one of the scheduling options.



For more information see *Chapter 8. Scheduling tasks*.

5.3.4 Backup method

Select whether you want to create a full, incremental or differential backup. If you have not backed up the selected data yet, or the full archive is old and you want to create a new master backup file, choose full backup. Otherwise it is recommended that you create an incremental or differential backup (see *3.2 Full, incremental and differential backups*).

If you select the **Full** method, the **Automatic consolidation** step (see *5.3.7 Setting automatic consolidation*) will be disabled. If you are adding a backup to the existing backup archive, the **Full** method will be unselectable.

You can set a backup policy for the backup task. Acronis True Image Home offers three types of backup policies:

1) create full backups only

2) create full backups after a specified number of incremental backups

3) create full backups after a specified number of differential backups

When the first backup on a schedule is executed, a full backup will be created. If you choose (2) or (3) by selecting the **Create a new full backup after** box, the next backups will be incremental (or differential) until the specified number of incremental (differential) backups is reached. After the selected number of incremental or differential backups is made, the next time a new full backup and a set of subsequent incremental (differential) backups will be created; this process will then continue until you decide to change it.

When the **Remove old archives** box is selected, creation of a new full backup in accordance with the specified backup policy results in deletion of the complete old backup chain – the old full backup and its subsequent incremental (or differential) backups

regardless of the overall limitations you set on the archive at the Automatic consolidation step.

If you decide to keep old backups (by not selecting the **Remove old archives** box) and creation of a new full backup results in violation(s) of the limits set for automatic consolidation, the program will use the following algorithm:

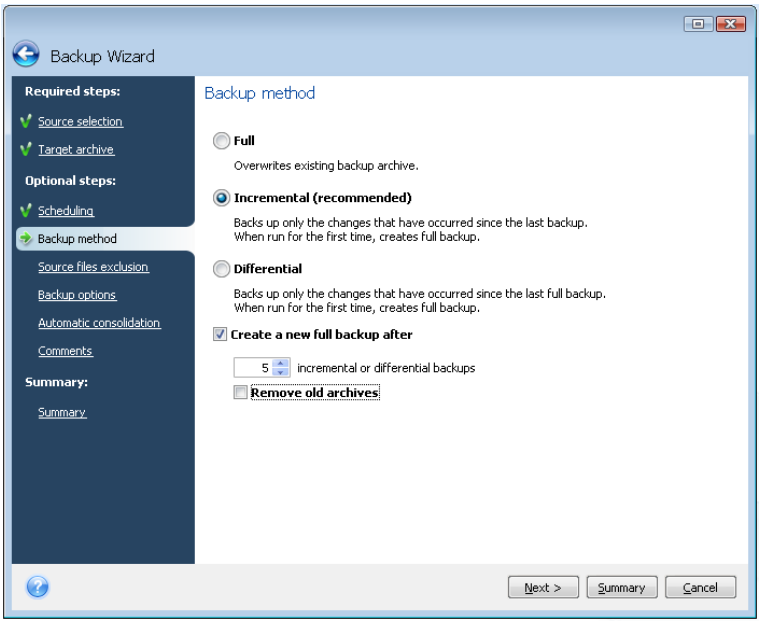
1) if the actual number of backups exceeds the maximum number of backups, the program automatically consolidates the old full backup with the oldest incremental (differential) one to correct this quota violation;

2) if after correcting the number of backups limit violation there remains other quota violation(s), the program consolidates the oldest backup to correct the storage period of old backups limit violation (if possible - otherwise it deletes the old full backup);

3) if after correcting the storage period of old backups limit violation there remains the archive size limit violation, the program consolidates the old full backup with the oldest incremental (differential) one, then will repeat consolidation (if necessary and possible);

4) if after consolidating all the previous backups the archive size quota violation remains, the old backup archive will be deleted in order to correct the violation;

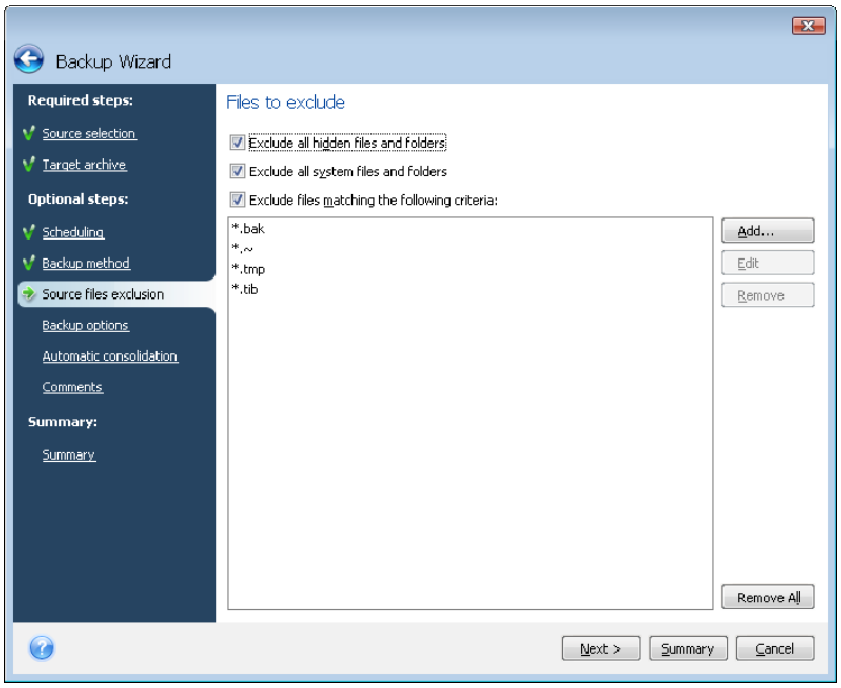
5) if the new full backup file size exceeds the archive size limit, the program will record a warning into the logs.



5.3.5 Source files exclusion

This step will be present only for the My Computer and My Data backup types. It enables you to exclude unnecessary files from your backup in case when you just want to exclude some file types without creating custom categories. You can exclude hidden or system files and folders, as well as files matching the criteria you specify. You can add your own criteria by clicking **Add**. While adding criteria, you can use the common Windows wildcard characters and type several criteria in the same line separating them by semicolons. For example, to exclude all files with .gif and .bmp extensions, you may type ***.gif;*.bmp**. One more thing – if, for example, you want to exclude all the files with the name of **test** regardless of their extension, you should specify exclusion criteria such as **test.***, otherwise those files will not be excluded. You can also specify the path to a folder to be excluded, for

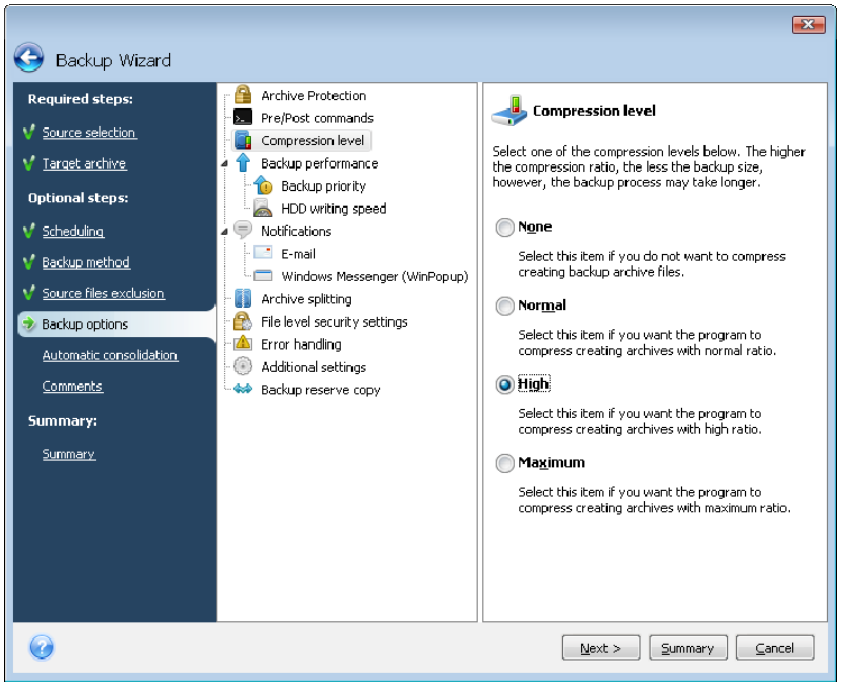
example, **C:\Program Files\Common Files**. Note that the path must end with the "\" symbol, otherwise the folder will not be excluded.



These filter settings will take effect for the current task. For information on how to set the default filters that will be used each time you select folders to back up, see *5.4.2 Source files exclusion.*

5.3.6 Selecting the backup options

Select the backup options (that is, backup file-splitting, compression level, password protection, etc.). The settings of the options will be applied only to the current backup task.

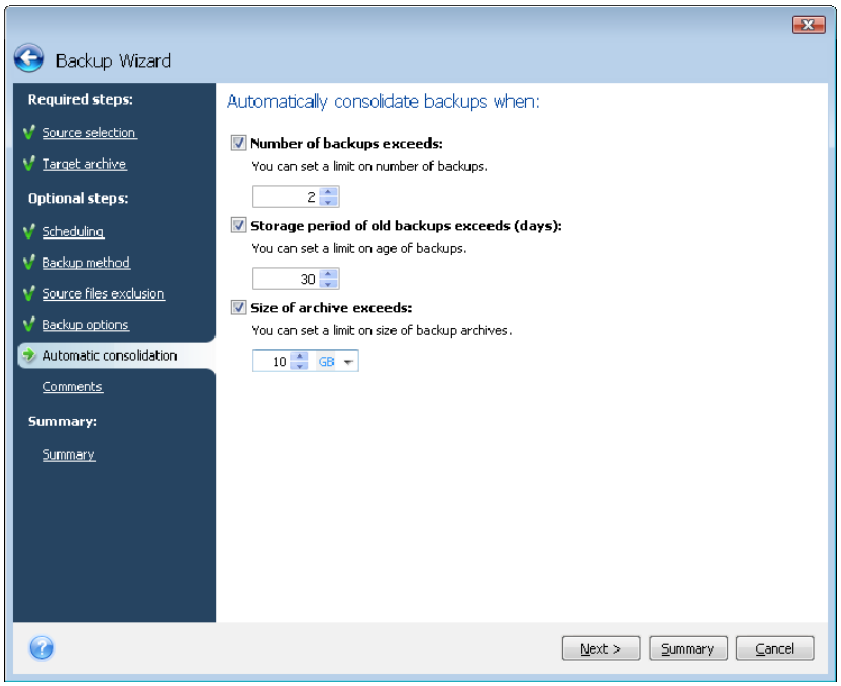


Or, you can edit the default backup options if you want to save the current settings for future tasks. See *5.4 Fine-tuning your backups* for more information.

5.3.7 Setting automatic consolidation

Automatic consolidation of a backup archive is enabled by setting the overall limitations for the archive. These limitations include:

- a maximum number of backups
- a maximum storage period for the archive files
- a maximum archive size



By default there are no limits set and automatic consolidation is not performed. To enable automatic consolidation, you must select at least one of the limits and either leave its default value or change it according to your needs.

If limits are set, then after creating a backup the program checks the archive for quota violations, such as exceeding a pre-set maximum number of gigabytes set aside for backups and, if any limitation is exceeded, consolidates the oldest backups. For example, if you've pre-set your archive to store 50GB of backup files and your backups reach 55GB, you have exceeded a quota and the system will respond automatically based on rules that you've already set. This operation creates a temporary file and thus requires disk space. Consider also that the quota must be violated so that the program can detect the violation. Therefore, to be able to consolidate the files, the program needs some space on the disk in excess of the archive quota. The extra amount of space can be estimated as the size of the largest backup in the archive.

In case of setting a limit on the number of backups, the actual number of backups can exceed the maximum number of backups by one. This enables the program to detect quota violation and start consolidation. Similarly, if you pre-set a backups storage period, for example, 30 days, the program will start consolidation when the oldest backup is stored for 31 days.

5.3.8 Providing a comment

Provide a comment for the archive. This can help identify the backup and prevent you from restoring the wrong data. However, you can choose not to make any notes. The backup file

size and creation date are automatically appended to the description, so you do not need to enter this information.

5.3.9 The operation summary and the backup process

At the final step, the backup task summary is displayed. Up to this point, you can make changes in the created task by clicking on the desired step and changing the settings. Clicking **Proceed** will start the task execution if you have configured the task to be started manually, by choosing the **Do not schedule** option at the Scheduling step, or have left selected the **Run task now** box for a scheduled task.

The task progress will be shown in a special window. You can stop the procedure by clicking **Cancel**.

You can also close the progress window by clicking **Hide**. The backup creation will continue, but you will be able to start another operation or close the main program window. In the latter case, the program will continue working in the background and will automatically close once the backup archive is ready. If you prepare some more backup operations, they will be queued after the current one.

5.4 Fine-tuning your backups

You can fine-tune your backups to specific tasks. Such fine-tuning is made by configuring backup options before starting a backup task.

You can set temporary backup options by editing the default backup options while creating a backup task.

In addition, when backing up your data files, you can create custom data categories for backup.

5.4.1 Archive protection

The preset is **no password**.

Suppose you have some files with sensitive information, for example, your tax return, which you need to back up. Acronis True Image Home can help you protect your sensitive information from getting into the wrong hands. The simplest (and the least secure) way is protecting your backup with a password. Let's remind you that to make a password more difficult to guess, it should consist of at least eight symbols and contain both letters (upper and lower case, preferably) and numbers. If you think that a password will not give you sufficient security, use encryption for your backup. Acronis True Image Home allows encrypting backup files with the industry-standard AES cryptographic algorithm. A 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, though in the case being considered this most likely will not be an issue, because the files will not be too large. The encryption settings are available only for password-protected archives.

If you try to restore data from a password-protected archive, or append an incremental/differential backup to such an archive, Acronis True Image Home will ask for the password in a special window, allowing access only to those who know the password.

5.4.2 Source files exclusion

By default, the program excludes files with the following extensions from backups: **.bak**, **.~, .tmp**, and **.tib**. You can also set other default filters for file exclusion, for example, you may want hidden and system files and folders not to be stored in the backup archives as well.

In addition, you can apply your own filters using the common Windows wildcard characters. For example, to exclude all files with extension .exe, add ***.exe** mask. **My???.exe** will exclude all .exe files with names consisting of five symbols and starting with "my".

This option affects real folders selected at **My Data** backup. If the name of a whole folder matches a mask you set, this folder will be excluded with all its content. Backup of a file category uses file filters preset at creation of the category. **My Application Settings, System State** or **My E-mail** backup implies dedicated lists of files that must not be filtered.

5.4.3 Pre/post commands

You can specify commands or batch files to be executed automatically before and/or after the *backup procedure*. For example, you may want to remove some temporary (.tmp) files from the disk before starting backup or configure a third-party antivirus product to be used each time for scanning the files to be backed up before the backup starts. Click **Edit** to open the **Edit Command** window where you can easily input the command, its arguments and working directory or browse folders to find a batch file.

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

Unselecting the **Do not perform operations until the command's execution is complete** box, selected by default, will permit the backup process to run concurrently with your commands execution.

If you want the backup to be performed even if your command fails, unselect the **Abort the operation if the user command fails** box (selected by default).

You can test execution of the command you created by clicking **Test command**.

5.4.4 Compression level

The preset is **Normal**.

Let's consider such an example - you need to backup to a USB stick some files with a total size comparable or exceeding the USB stick's capacity and want to make sure that the stick accommodates all the files. In this case use the **Maximum** compression for the files to be backed up. However, you should take into account that the data compression ratio depends on the type of files stored in the archive, for example, even the **Maximum** compression will not significantly reduce the backup size if it contains files with already compressed data like .jpg, .pdf or .mp3. It does not make any sense to select the **Maximum** compression for such files because in this case the backup operation will take significantly longer and you will not get an appreciable reduction of backup size. If you are not sure about the compression ratio of a file type, try to back up a couple of files and compare the sizes of the original files and backup archive file. A couple of additional tips: generally, you can use the **Normal** compression level, because in most cases it provides an optimal balance between backup file size and backup duration. If you select **None**, the data will be copied without any compression, which may significantly increase the backup file size, while making the fastest backup.

5.4.5 Backup performance

The three options below might have a more or less noticeable effect on the backup process speed. This depends on overall system configuration and the physical characteristics of the devices.

1. Backup priority

The preset is **Low**.

The priority of any process running in a system determines the amount of CPU usage and system resources allocated to that process. Decreasing the backup priority will free more resources for other CPU tasks. Increasing the backup priority might speed up the backup process due to taking resources from the other currently running processes. The effect will depend on total CPU usage and other factors.

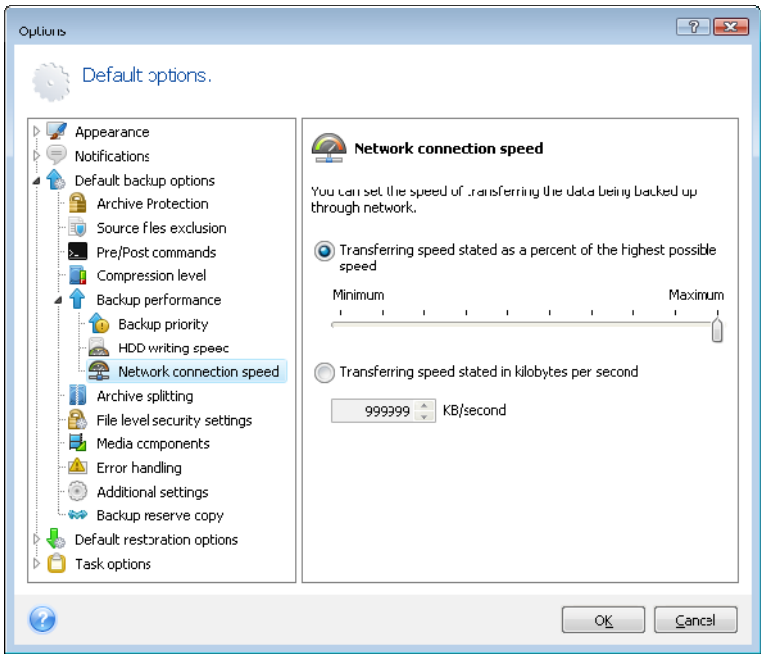
2. HDD writing speed

The preset is **Maximum**.

Backing up in the background to an internal hard disk (for example, to Acronis Secure Zone) may slow other programs' performance because of the large amounts of data transferred to the disk. You can limit the hard disk usage by Acronis True Image Home to a desired level. To set the desired HDD writing speed for data being backed up, drag the slider or enter the writing speed in kilobytes per second.

3. Network connection speed

The preset is **Maximum**.



If you frequently back up data to network drives, think of limiting the network bandwidth used by Acronis True Image Home. To set the desired data transfer speed, drag the slider or enter the bandwidth limit for transferring backup data in kilobytes per second.

5.4.6 Archive splitting

Sizeable backups can be split into several files that together form the original backup. A backup file can be split for burning to removable media or saving on an FTP server (data

recovery directly from an FTP server requires the archive to be split into files of no more than 2GB). A backup destined for the Acronis Secure Zone cannot be split.

Suppose you have a full backup of your PC on an external hard disk, but want to make one more backup copy of the system to keep it in a different location from the first one for added security. However, you do not have one more external hard disk, and a USB stick would not accommodate such a large backup. Using Acronis True Image Home you can make a reserve backup copy on blank DVD-R/DVD+R discs, which are very cheap nowadays. The program can split large backups into several files that together form the original backup. If you have enough space on your PC's hard disk, you can first create a backup archive consisting of multiple files with a specified size on the hard disk and burn the archive to DVD±R discs later on. To specify the split file size, select **Fixed size** mode for **Archive splitting** and enter the desired file size or select it from the drop-down list.

If you do not have enough space to store the backup on your hard disk, select **Automatic** and create the backup directly on DVD-R discs. Acronis True Image Home will split the backup archive automatically and will ask you to insert a new disc when the previous one is full.

Creating backups directly on CD-R/RW or DVD±R/RW might take considerably more time than it would on a hard disk.

5.4.7 File-level security settings

Preserve files' security settings in archives

By default, files and folders are saved in the archive 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 restore 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 archives. Then the restored files/folders will always inherit the permissions from the folder to which they are restored (parent folder or disk, if restored to the root).

Or, you can disable file security settings during restoration, even if they are available in the archive (see *6.4.4 File-level security settings* below). The result will be the same.

In archives, store encrypted files in decrypted state

The preset is **disabled**.

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

Check the option if there are encrypted files in the backup and you want them to be accessed by any user after restore. 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 restore encrypted files on another computer.

These options relate only to file/folder backups. In addition, they are unavailable for zip backup archives.

5.4.8 Media components

The preset is **disabled**.

When backing up to removable media, you can make this media bootable and will not need a separate rescue disk.

The **Acronis One-Click Restore** is a minimal addition to your rescue media, allowing one-click data recovery from an image archive stored on this media. This means that when booting from the media and clicking "restore," all data will be restored to its original place automatically. No options or selections such as resizing partitions will be available.

If you want more functionality during restoration, write a full standalone version of **Acronis True Image Home** to the rescue media. As a result, you will be able to configure the restore task using Restore Data Wizard.

By clicking the **Advanced** tab you can select Acronis True Image Home (full version) and Acronis True Image Home (safe version). The safe version will be available for those who purchased the boxed version of Acronis True Image Home and installed the appropriate add-on. If you have other Acronis products installed on your computer, such as Acronis Disk Director Suite, the bootable versions of these programs' components will be offered on this tab as well.

5.4.9 Error handling

1. Ignore bad sectors

The preset is **disabled**.

This option lets you run a backup even if there are bad sectors on the hard disk. Although most disks do not have bad sectors, the possibility that they might occur increases during the course of the hard disk's lifetime. If your hard drive has started making strange noises (for example, it starts making quite loud clicking or grinding noises during operation), such noises may mean that the hard drive is failing. When the hard drive completely fails, you can lose important data, so it is high time to back up the drive as soon as possible. There may be a problem though – the failing hard drive might already have bad sectors. If the **Ignore bad sectors** box is left unselected, a backup task is aborted in case of read and/or write errors that could occur on the bad sectors. Selecting this box lets you run a backup even if there are bad sectors on the hard disk ensuring that you save as much information from the hard drive as possible.

2. Do not show messages and dialogs while processing (silent mode)

The preset is **disabled**.

You can enable this setting to ignore errors during backup operations. This feature was mainly designed for unattended backups when you cannot control the backup process. In this mode no notifications will be displayed to you if errors occur during backup. Instead you can view the detailed log of all operations after the task finishes by selecting **Tools -> Show Log**. You may use this option when configuring a backup task to be run during the night.

3. When not enough space in ASZ delete the oldest archive

The preset is **disabled**.

When this setting is disabled and there is not enough space in the Acronis Secure Zone for the backup file being created, the program will display a dialog warning you that the zone is full and will require your action. The backup is suspended until you take a desired action and this makes unattended backups impossible. The dialog opens even when the **Do not show messages and dialogs while processing (silent mode)** setting is enabled. So it is

advisable to select the **When not enough space in ASZ delete the oldest archive** box when planning unattended scheduled backups to the Acronis Secure Zone.

5.4.10 Additional settings

1. Validate backup archive when it is created

The preset is **disabled**.

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

To check archive data integrity you must have all incremental and differential backups belonging to the archive and the initial full backup. If any of the successive backups are missing, validation is not possible.

2. Ask for first media while creating backup archives on removable media

The preset is **enabled**.

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 task can run unattended.

5.4.11 Backup reserve copy settings

The preset is **disabled**.

You may want Acronis True Image Home to make reserve copies of your backups in a certain location each time when you choose the My Data backup type for backing up selected files and folders. To enable creation of reserve copies, select the **Reserve my backups** checkbox and then choose the method for making reserve copies. You have three choices: duplicate the backups as tib files, make reserve copies as zip archives, or simply copy the files and/or folders to a specified location "as is".

To specify the location for storing reserve copies of your backups, click the **Location** link. Select a location – a local hard disk, USB stick, or a network share. You can create a folder for reserve copies by clicking the **Create new folder** icon. Reserve copies created as tib and zip files will be named automatically as follows:

backupfilename_reserved_copy_mm-dd-yyyy hh-mm-ss AM.tib; or

backupfilename_reserved_copy_mm-dd-yyyy hh-mm-ss PM.zip,

where mm-dd-yyyy hh-mm-ss is the date and time of reserve copy creation in the following format: month (one or two digits), day (one or two digits), year (four digits), hour (one or two digits), minute (two digits), and second (two digits). AM or PM is a 12-hour period.

For example: MyBackup_reserved_copy_8-15-2008 9-37-42 PM.zip

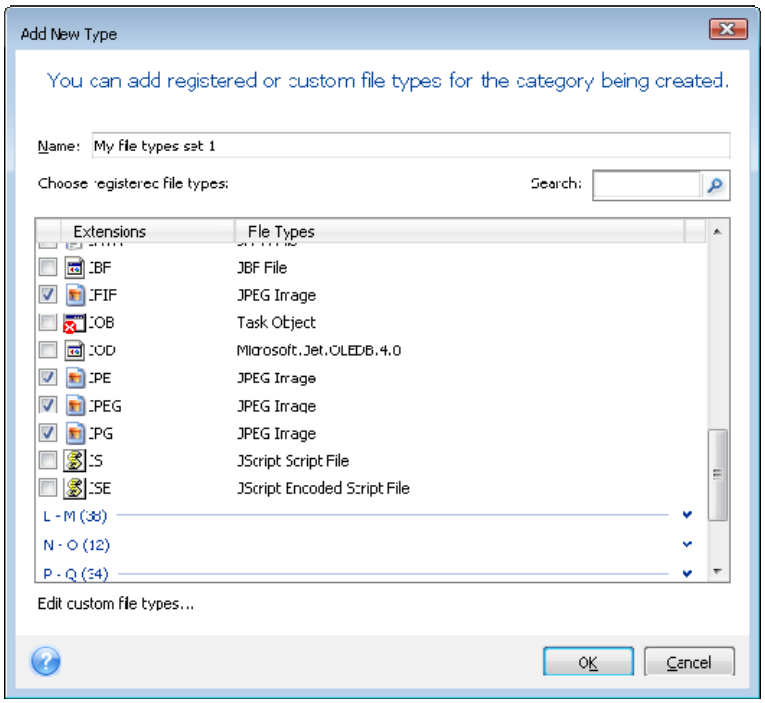
If you choose reserve copies to be made in the form of flat files, those files will be placed into folders which will be automatically created and named as follows: backupfilename_reserved_copy_mm-dd-yyyy hh-mm-ss AM (or PM).

After you make the backup reserve copy settings, Acronis True Image Home will create reserve copies each time you select the My Data backup type. If a reserve copy could not be made due to expiration of free space in the selected location or due to disconnection of the selected storage device (e.g. a USB stick), the program will write an error message to the event log.

5.4.12 Creating a custom data category for backups

To add a custom data category, click **Create** in the **Choose files to back up** screen of the Backup Wizard, select the folder (data source) and provide a name for the category. You can include in the category all files in the selected folder or apply filters to select the specific types of files that you wish or do not wish to back up.

To set a filter, select its type: **Back up files of the following types only** or **Back up files of all types in the source except the following**. Then click **Add new** and select the desired file types in the window that appears.



You can select file types as follows:

1. By name. Enter the file name in the upper **Name** field. You can use the common Windows wildcard characters. For example, ***My???.exe*** will select all .exe files with names consisting of five symbols and starting with “my”.

2. By type. Select the desired file types in the list. You can also search desired registered file types by entering their extension or description in the **Search** field.

3. By extension. Click the **Edit custom file types...** link and enter the extensions (semicolon separated) in the **File extensions** field.

If you do not want to keep custom contents of the current backup, simply select the files/folders from the tree. This set will be effective only for the current backup task.

5.5 Making reserve copies of your backups

When you choose the My Data backup type for backing up selected files and folders, you can create reserve copies of your backups and save them on the file system, a network drive, or a USB stick.

In addition to enhancing the archive security with replication, this feature allows you to copy a set of documents, for example, to a USB stick for working on them at home. So now you can perform a normal backup and copy the same files to a USB stick or any local hard drive. You have a choice of making a reserve copy in the form of regular files, a zip compressed file, or a tib file (optionally with password protection and encryption).

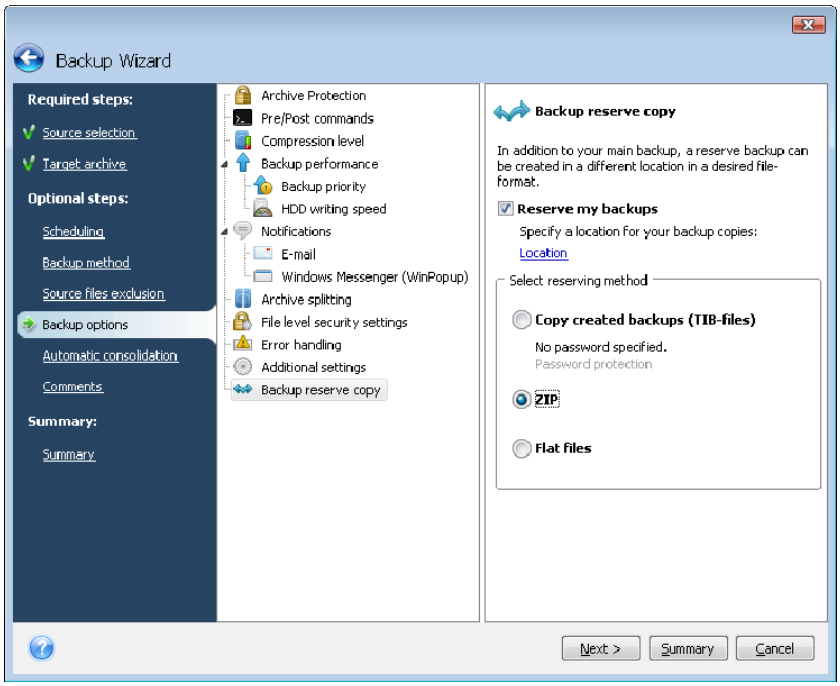
A reserve copy always contains all the files selected for backup, that is, when creating a reserve copy the program always makes a full backup of the source data. You cannot make a reserve copy in the form of an incremental or differential backup, even in tib format.

Also remember that you will pay for the enhanced convenience and increased security of your data by the time required for performing the task, because normal backup and reserve copying are performed one at a time and not simultaneously.

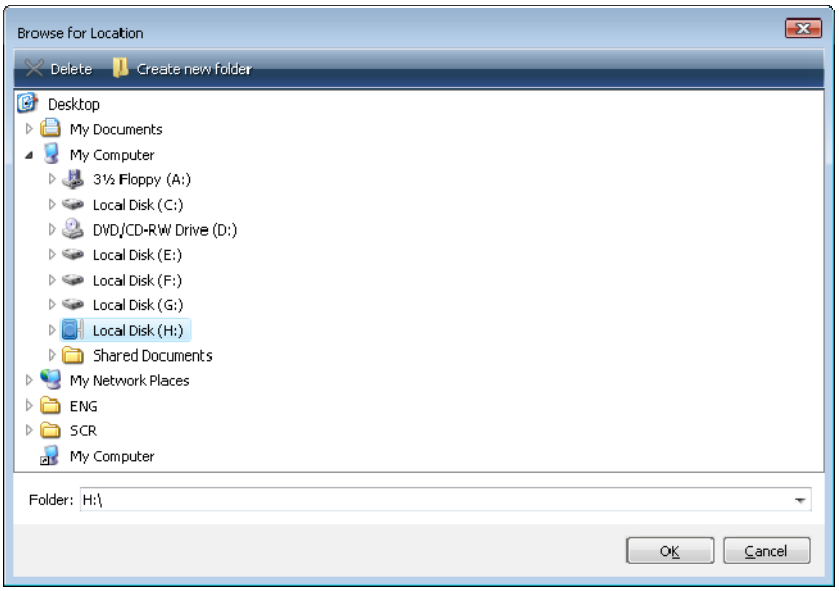
And now let us consider a case when you may need to make a reserve copy of your backup.

Suppose you have worked hard on an urgent project all day and the deadline is tomorrow morning. You decide to back up the results of the day's work in the Acronis Secure Zone and make a reserve copy of the project on a USB stick to finish the project at home. To make a reserve copy:

1. When you come to the **Backup options** step while configuring a My Data backup task in the Backup Wizard (or select that step after completing all the required steps), choose **Backup reserve copy** and then select the **Reserve my backups** box (if it is not selected in the default backup options).



2. Choose how to duplicate the project file(s) on the USB stick. If you need to save space, choose duplicating as a zip file. Click on the **Location** link, select the drive letter of the USB stick and create a folder for a reserve copy by clicking on the **Create new folder** icon.



3. Finish configuring your backup task as usual.
4. Click **Proceed** in the Summary window and do not forget to take the USB stick home.

Please, be aware that built-in support of zip files in Windows does not cover operations with multivolume zip archives, and zip archives exceeding 4GB in size or which contain files of more than 4GB each. Also remember that CD/DVDs are not supported as locations for reserve copies created as zip archives and flat files.

5.6 Archive to various places

You can save full, incremental and differential backups of the same data entity (for example, a partition, disk, E-mail, Applications settings) to various places – almost anywhere you like.

5.6.1 Why you need this feature

The previous versions of Acronis True Image Home could save incremental or differential backups only in the same place (a folder, disk, backup location, etc.) as the initial full backup. Usually this is not a problem but sometimes this could be difficult or simply impossible to achieve, for example, due to using up all the available disk space. Of course, Acronis True Image Home provided means for alleviating this problem – it could manage backups in the Acronis Secure Zone and in backup locations and was able to automatically delete the oldest backups freeing the space it needed for new ones. This is still true for the Acronis Secure Zone. Such an approach worked just fine in most cases, however, there could be exceptions.

For example, you saved a full backup of your system disk to an external USB hard disk drive and it occupied almost all the disk. If later you would like to make an incremental backup of that disk while keeping the initial full one, this was simply impossible.

Also, you could assign a meaningful name only to a full backup. Incremental and differential backups were named automatically by adding sequential numbers to the full backup name. You could add a comment with a description of the backup while configuring a backup task in the wizard, but in order to read this description you needed to launch Acronis True Image Home and select the appropriate tib archive in the Restore wizard.

There was one more drawback. Suppose you were making a large backup to a hard disk and after an hour you got a message warning you that the disk is full. You could try to free some

disk space but if this was impossible, you were forced to find some other location for the backup and start it anew wasting a lot of time as a result.

5.6.2 What makes it work

For this feature to operate, Acronis True Image Home maintains an internal database containing all the metadata information on the operations performed with tib files (such as creation, consolidation, verification, and so on), as well as on their names, sizes, time stamps, physical paths, archive types (full, incremental, differential), slice and volume IDs, and some "housekeeping" information required for program operation. The database is updated after each operation with tib files. Acronis True Image Home also adds to tib files metadata uniquely identifying the file. The last volume of a slice related to a certain backup entity contains additional information on the IDs of all the preceding volumes and backups (tib files).

In other words, thanks to this metadata information, Acronis True Image Home always knows where, when, and how it backed up your data and where it can find the data you want to restore.

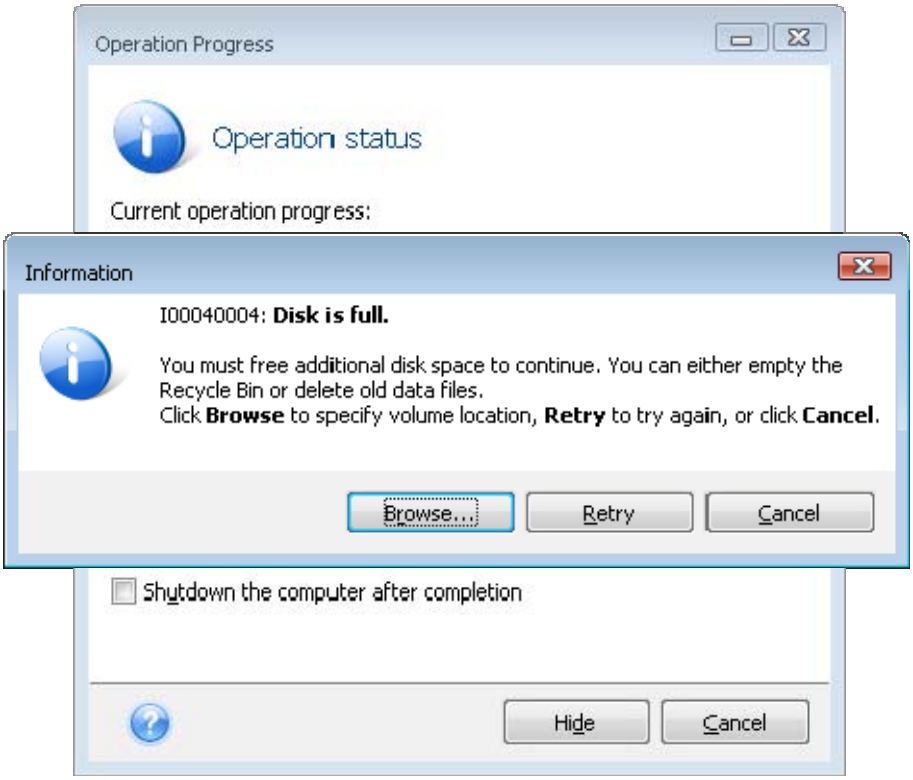
By the way, the metadata information database gives you an additional benefit. Now you can assign any name you wish to incremental and differential backups. This makes it easier to find the required backup archive when you need to restore some data.

5.6.3 Using backup to various places

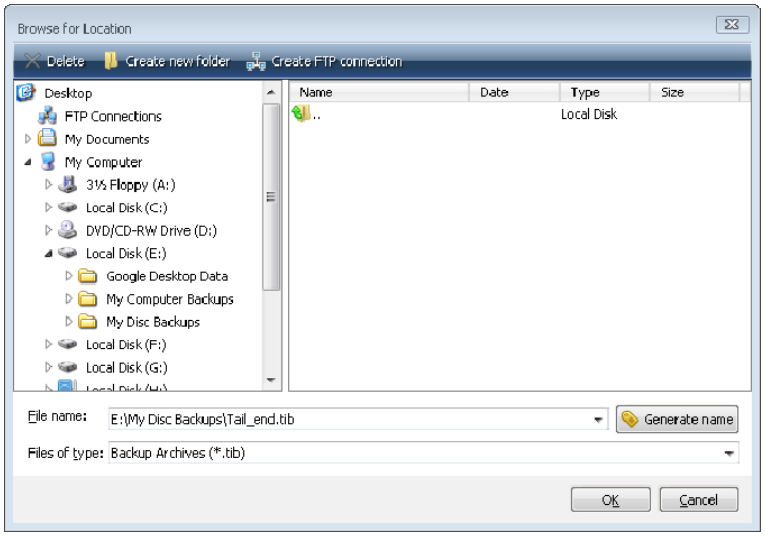
Now Acronis True Image Home offers much greater flexibility. You can save full, incremental and differential backups to different places including a network share, CD/DVD, USB stick, as well as any local internal or external hard drive.

You cannot use the Acronis Secure Zone as one of the places for storing a part of backups belonging to the same backup "chain", because such backups may be automatically deleted during automatic backups consolidation in the Acronis Secure Zone. As a result, the backup chain will be corrupted. In addition, the Archive to various places feature does not work with FTP servers.

One more useful aspect of this feature is its ability to split backups "on-the-fly". Suppose you perform a backup to a hard disk and in the middle of the backup process Acronis True Image Home finds out that the disk, to which you are backing up, does not have enough free space for completing the backup. The program displays a message warning you that the disk is full.

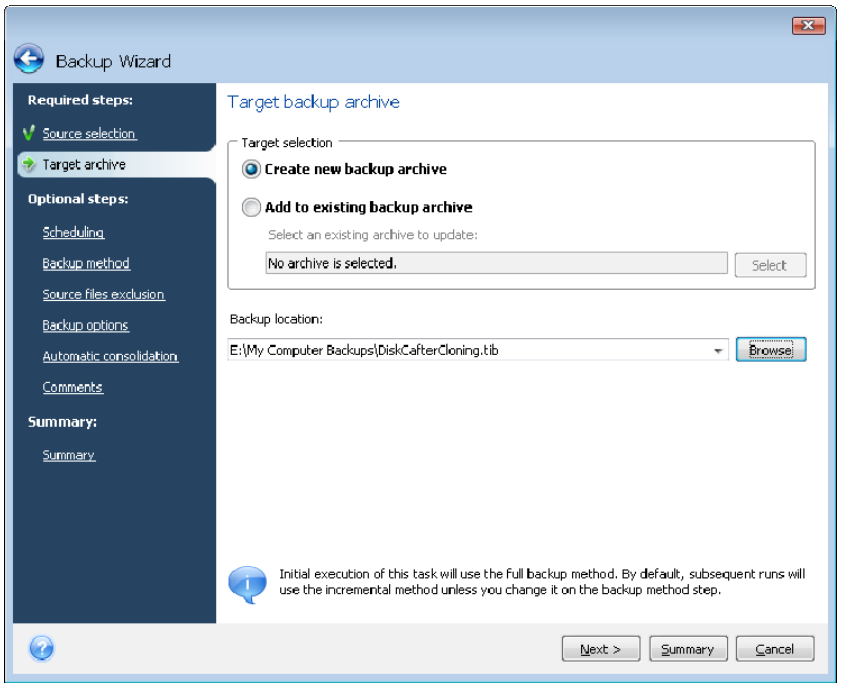


To complete the backup, you may either try to free some space on the disk and click **Retry** or select another storage device. To choose the latter option, click **Browse** in the information window. The Browse for Location window appears.

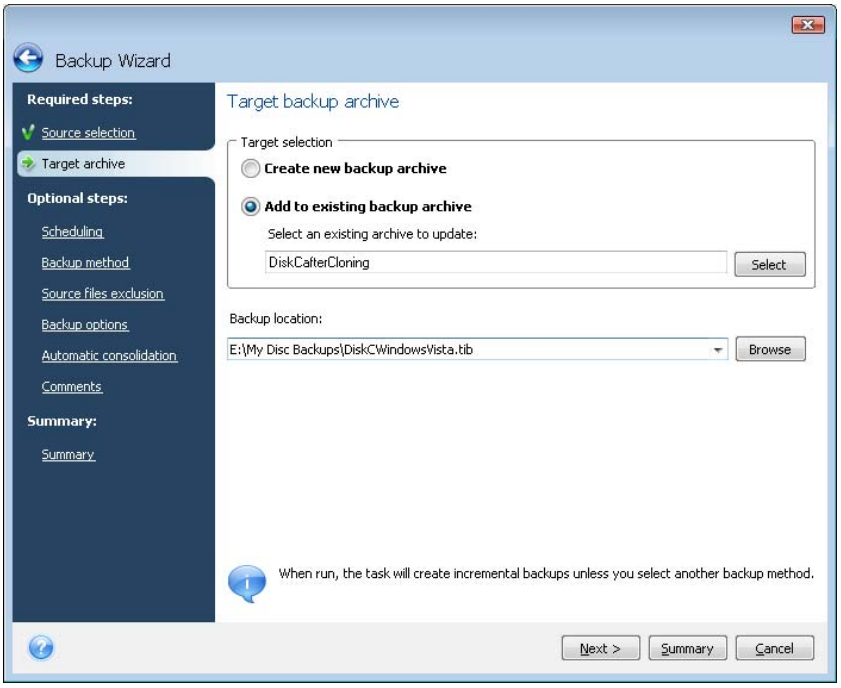


The left pane shows the storage locations available on your computer. After you select a disk in the left pane, the program shows the free space on that disk in the right pane. If the free space is enough for completing the backup, assign a name for the file that will contain the remaining data being backed up. You can either enter the name manually (for example, "Tail_end.tib") or use the file name generator (a button to the right of the line). Then click **OK** and Acronis True Image Home will complete the backup.

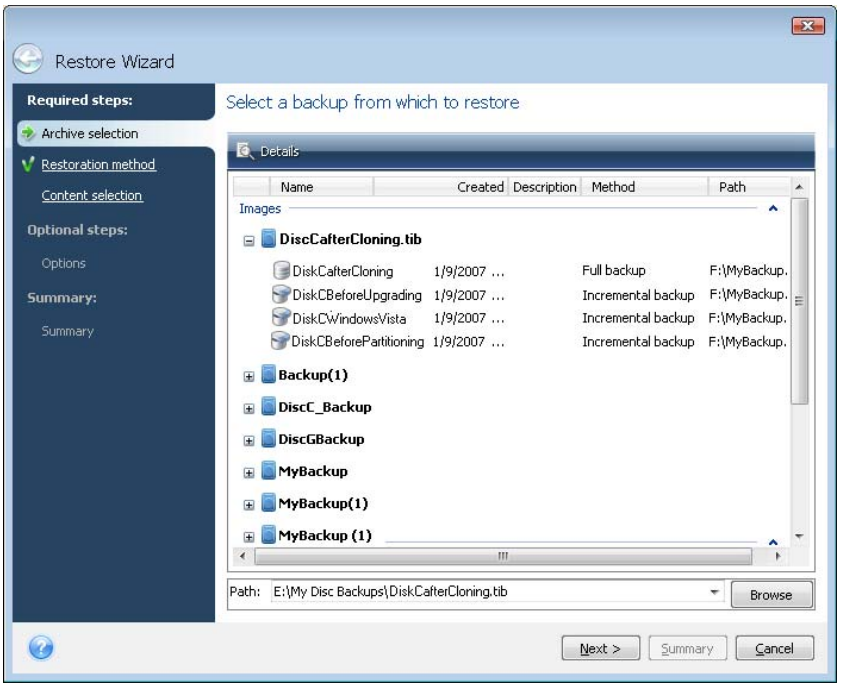
Acronis True Image Home permits to give any backup archive whatever name you wish. Suppose you bought a new hard disk drive and transferred to it the contents of the old one by cloning. You decided to perform a full backup of the new system disk and named it "DiskCafterCloning".



After a while you chose to upgrade to Windows Vista. To be on the safe side, you made an incremental backup before the upgrade and named it "DiskCBeforeUpgrading". Upon upgrading you made sure that the new system and all your applications operate normally and made one more incremental backup naming it "DiskCWindowsVista".



After working under Windows Vista for some time you decided that you would like to try Linux as well. Before creating a partition for Linux you perform an incremental backup of the system disk and name it "DiskCBeforePartitioning", and so on. As a result, if the need to recover arises, you will be able to find at a glance a backup archive corresponding to the system disk state you want to recover.



As was already mentioned, you can save full and incremental or differential backups to different locations. For example, you can save the initial full backup to an external USB hard drive, and then burn the subsequent incremental backups (or differential backups that are an even better choice) to CDs or DVDs. It is also possible to save such backups to a network share. If you have saved backups belonging to the same backup "chain" to various places, Acronis True Image Home may prompt you for the locations of previous backups during data recovery, in the case when the selected backup archive does not contain the files you want to restore (or contains only a part of them).

Chapter 6. Restoring backup data

6.1 Restore under Windows or boot from CD?

As mentioned above (see *2.3 Running Acronis True Image* Home), Acronis True Image Home can be used in several ways. We recommend that you first try to restore data using Acronis True Image Home under Windows, because this provides more functionality. Boot from the bootable media or use the Startup Recovery Manager (see *3.4 Acronis Startup Recovery Manager)* only if Windows does not start up.

The boot CD, from which you started the program, does not keep you from using other CDs or DVDs with backup archives. Acronis True Image Home is loaded entirely into RAM so you can remove the bootable CD to insert the archive disc.

Be careful! When you use the Acronis True Image Home rescue disc, the product creates disk drive letters that might differ from the way Windows identifies drives. For example, the D: drive identified in the standalone Acronis True Image Home might correspond to the E: drive in Windows. This is not an error with the software.

If a backup image is located on bootable media, you might have the choice of using Acronis One-Click Restore. This operation always restores the entire physical disk. Therefore, if your disk consists of several partitions, all of them must be included in the image. Any partitions missing from the image will be lost. Please make sure that the image contains *all* the disk data you plan to restore. For more information on Acronis One-Click Restore, see *5.4.8 Media components*.

6.1.1 Network settings in rescue mode

When booted from removable media or by Startup Recovery Manager, Acronis True Image Home might not detect the network. That can happen if there is no DHCP server in your network or your computer address was not identified automatically.

To enable network connection, specify network settings manually in the window, available at **Tools -> Options -> Network adapters.**

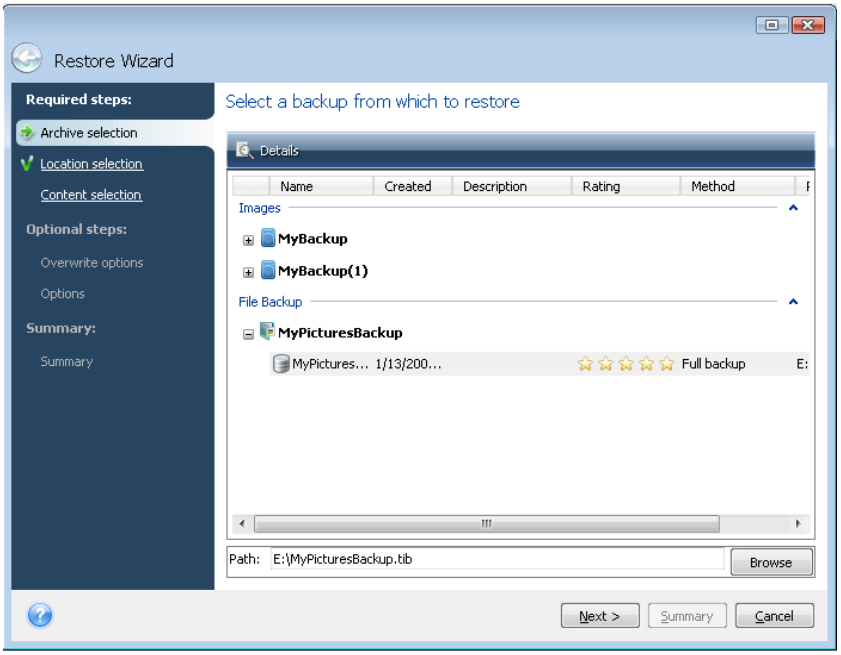
6.2 Restoring files and folders from file archives

This section describes how to restore files and folders from a file backup archive. You can restore the desired files and folders from a disk/partition image as well. To do so, mount the image (see *Chapter 12. Exploring archives and mounting images*) or start the image restoration and select **Restore files or folders.**

File backup archives are supported only for the FAT and NTFS file systems.

1. Start the **Restore Wizard** by selecting **Operations -> Restore** in the main program menu.

2. Select the archive.



If the archive is located on removable media, e.g. CD, insert the *last* disk in the series first and then insert disks in reverse order when the Restore Wizard prompts you.

Data recovery directly from an FTP server requires the archive to consist of files of no more than 2GB. If you suspect that some of the files are larger, first copy the entire archive (along with the initial full backup) to a local hard disk or a network share disk. See notes and recommendations for supporting FTP servers in *1.3.4 Supported storage media*.

Please note that before restoring Microsoft Outlook mail messages, accounts, contacts, settings, etc. from **My E-mail backup** on a new computer with a newly installed Microsoft Outlook, you should launch Outlook at least once. If Microsoft Outlook is launched for the first time after restoring the E-mail information, it may malfunction.

If you use Microsoft Outlook Express and restore its mail folders, accounts, etc. from **My E-mail backup** on another PC or after performing a so called "clean install" of Microsoft Windows, please, do not forget to switch to your identity after restoration by selecting **File -> Switch Identity** in Outlook Express and then double-clicking on your identity in the list of the dialog box.

3. If you are to restore files from an archive containing incremental backups, Acronis True Image Home will enable selecting one of the successive incremental backups by its creation date/time. Thus, you can roll back the files/folders state to a certain date.

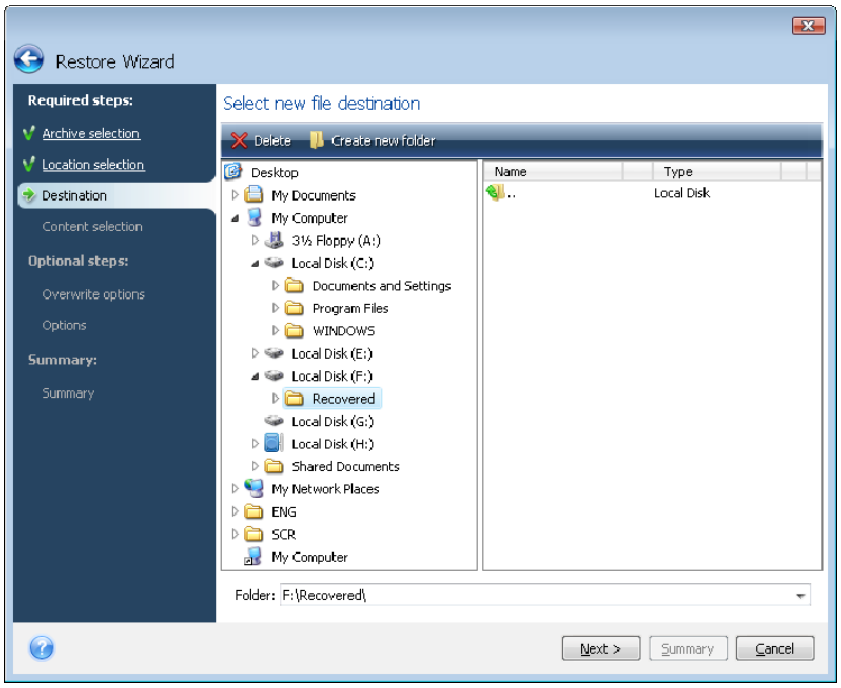
To restore data from an incremental backup, you must have all the previous backup files and the initial full backup. If any of the successive backups are missing, restoration is not possible.

To restore data from a differential backup, you must have the initial full backup as well.

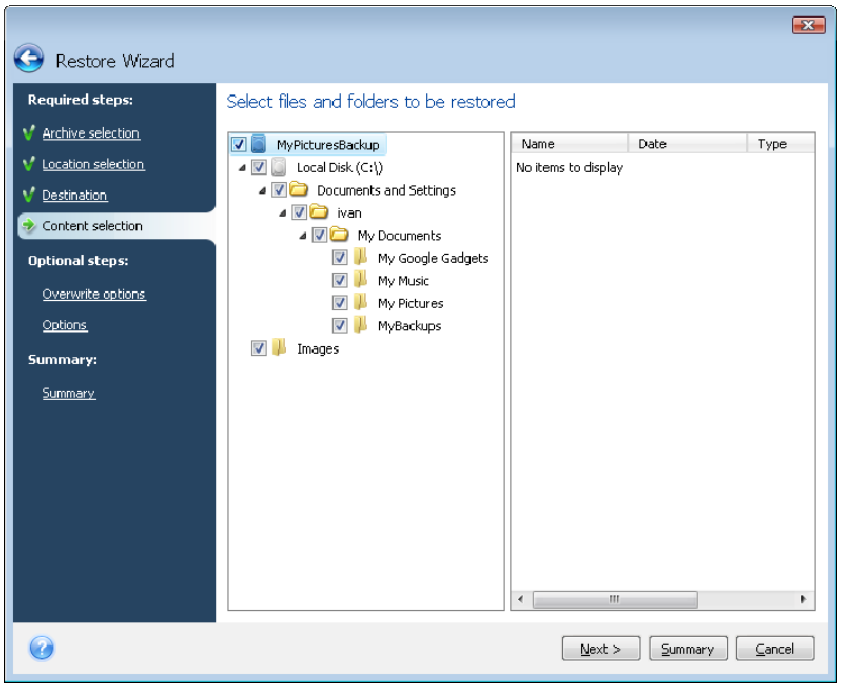
4. Select a folder on your computer where you want to restore selected folders/files (a target folder). You can restore data to its original location or choose a new one, if necessary. Choosing a new location results in the appearance of one more required step, namely, **Destination**.

When you choose a new location, the selected items by default will be restored without restoring the original, absolute path. You may also wish to restore the items with their entire folder hierarchy. If this is the case, select **Restore absolute path**.

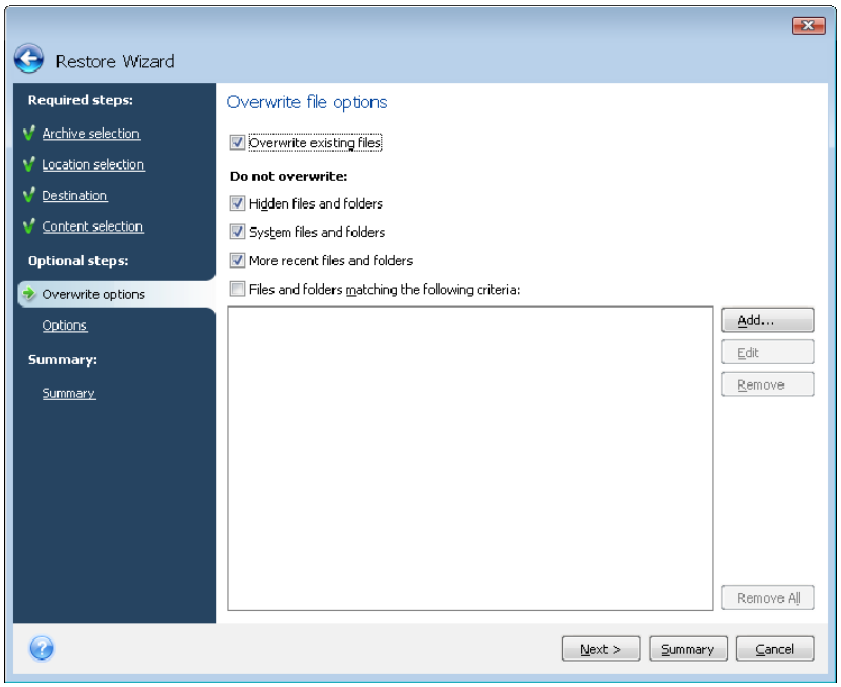
At the **Destination** step select a new location on the directory tree. You can create a new folder for the files to be restored by clicking **Create new folder**.



5. Select files and folders to restore. You can choose to restore all data or browse the archive contents and select the desired folders or files.



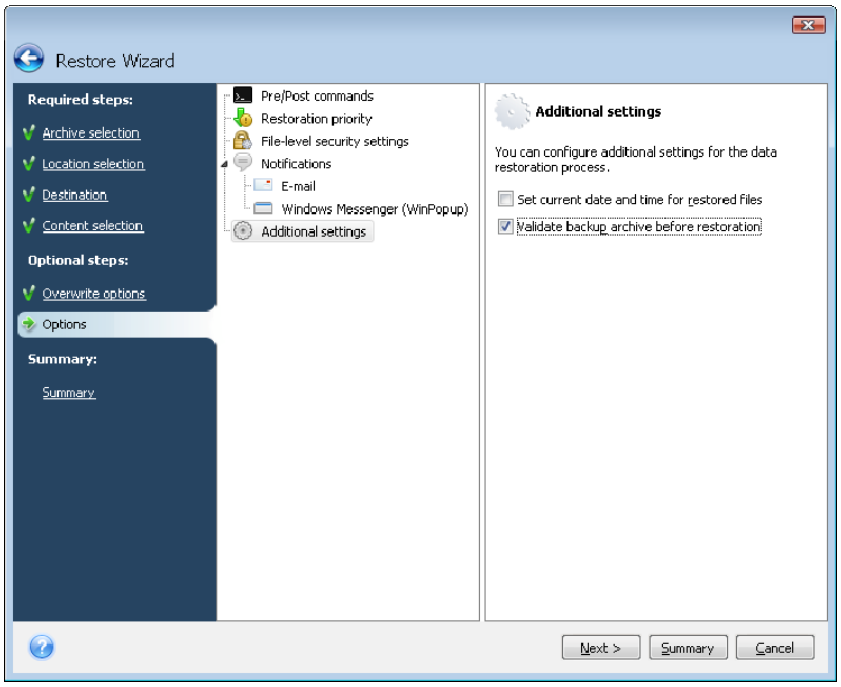
6. The next step allows you to keep useful data changes made since the selected backup was created. Choose what to do if the program finds a file with the same name as in the archive, in the target folder. By default, the program will not overwrite any files and folders, thus giving the files on the hard disk unconditional priority over the archived files.



Selecting the **Overwrite existing files** checkbox will give the archived files unconditional priority over the files on the hard disk, though, by default, the system, hidden files and folders, as well as more recent files and folders are preserved from overwriting. If you want to overwrite those files and folders too, unselect the appropriate checkboxes.

In addition, you can preserve from overwriting the files that meet the criteria you specify in this window.

7. Select the options for the restoration process (that is, restoration process priority, file-level security settings, etc.). The options you set on this page will be applied only to the current restore task. If you want to use the default restoration options, omit this step and click **Summary**.



8. At the final step, the restoration summary is displayed. Up to this point, you can make changes in the created task by choosing the step you want to change and by editing its settings. Clicking **Proceed** will launch the task execution.

9. The task progress will be shown in a special window. You can stop the procedure by clicking **Cancel**. Please keep in mind that the aborted procedure may still cause changes in the destination folder.

6.3 Restoring disks/partitions or files from images

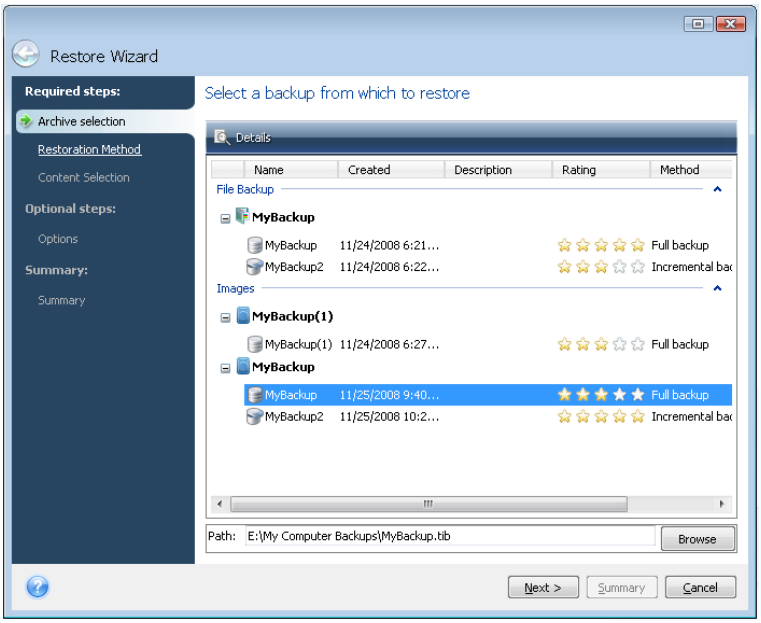
To restore a partition (disk) from an image, Acronis True Image Home must obtain **exclusive access** to the target partition (disk). This means no other applications can access it at that time. If you receive a message stating that the partition (disk) cannot be locked, close applications that use this partition (disk) and start recovery once more. If you cannot determine which applications use the partition (disk), close them all.

6.3.1 Starting the Restore Wizard

Start the **Restore Wizard** by selecting **Operations -> Restore** in the main program menu.

6.3.2 Archive selection

1. Select the archive. Acronis True Image Home will show the list of backup archives whose locations it knows from the information stored in its database. If the program has not found the backup you need (for example, when the backup was made some time ago by a previous Acronis True Image Home version), you can find it manually by clicking **Browse** and then selecting the backup location on the directory tree and choosing the backup in the right pane.



If the archive is located on removable media, e.g. CD, first insert the last CD and then insert disks in reverse order when the Restore Data Wizard prompts you.

Data recovery directly from an FTP server requires the archive to consist of files of no more than 2GB each. If you suspect that some of the files are larger, first copy the entire archive (along with the initial full backup) to a local hard disk or network share disk. See notes and

recommendations for supporting FTP servers in *1.3.4 Supported storage media*.

When restoring a backup of Windows Vista system disk containing restore points, some of your restore points (or all of them) may be missing if you boot from the restored system disk and open the System Restore tool.

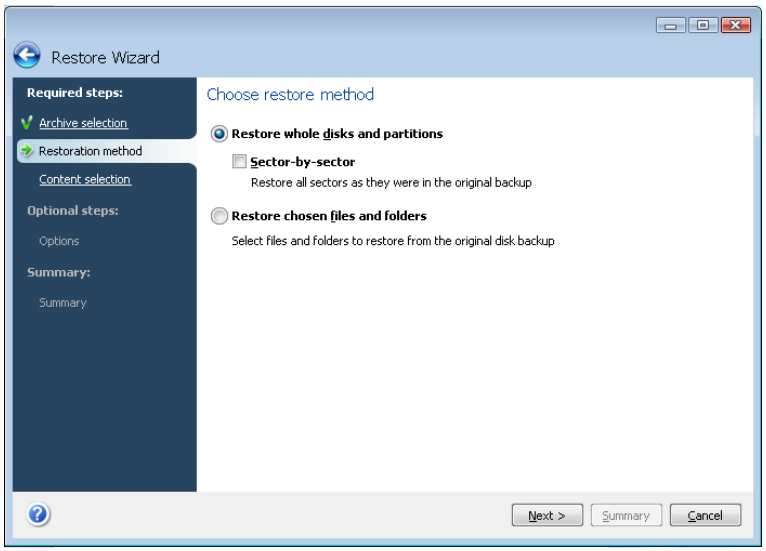
If the archive was protected with a password, Acronis True Image Home will ask for it. The partitions layout and the **Next** button will be unavailable until you enter the correct password.

2. If you are going to restore data from an archive containing incremental backups, Acronis True Image Home will enable selecting one of the successive incremental backups by its creation date/time. Thus, you can roll back the disk/partition state to a certain date.

To restore data from an incremental backup, you must have all previous backup files and the initial full backup. If any of the successive backups are missing, restoration is not possible. To restore data from a differential backup, you must have the initial full backup as well.

6.3.3 Restoration method selection

Select what you want to restore:



Restore whole disks and partitions

Having chosen a disk and partition recovery type, you may need to select the following option.

Sector-by-sector

The program will restore both used and unused sectors of disks or partitions. This option will appear only when you choose to restore a sector-by-sector backup.

Restore chosen files or folders

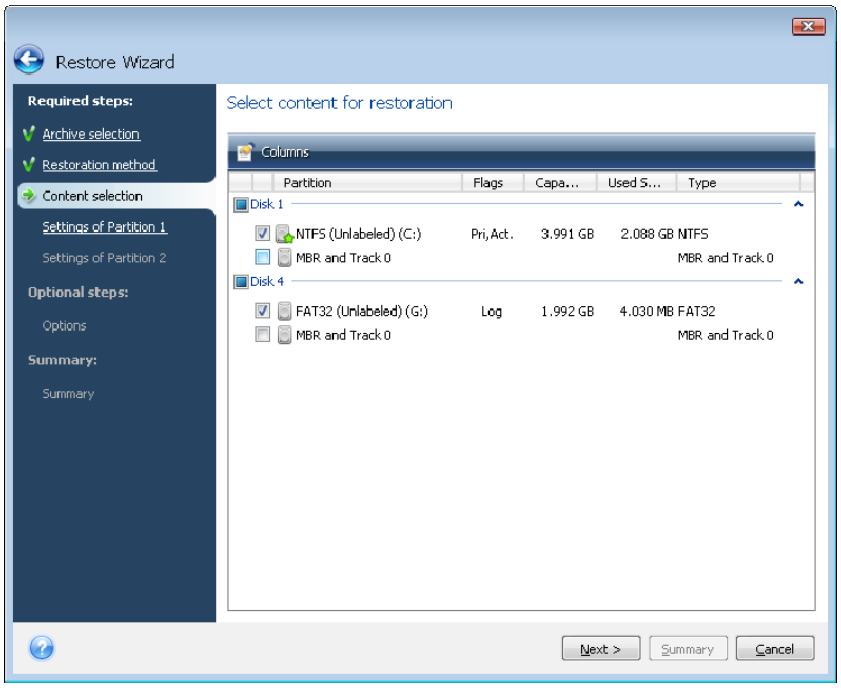
If you are not going to recover the system, but only want to repair damaged files, select **Restore chosen files or folders**. With this selection, you will be further asked to select where to restore selected folders/files (original or new location), choose files/folders to be restored, and so on. These steps look like those in file archive restore. However, watch your selection: if you are going to restore files instead of a disk/partition, unselect the unnecessary folders. Otherwise you will restore a lot of excess files. Then you will be able to go directly to the Restoration Summary screen (*6.3.10 Restoration summary and executing restoration*).

You can restore files from disk/partition images only if they have the FAT or NTFS file systems.

6.3.4 Selecting a disk/partition to restore

The selected archive file can contain images of several partitions or even disks. Select which disk/partition to restore.

During a single session, you can restore several partitions or disks, one by one, by selecting one disk and setting its parameters first and then repeating these actions for every partition or disk to be restored.



Disk and partition images contain a copy of track 0 along with the MBR (master boot record). It appears in this window in a separate line. You can choose whether to restore MBR and track 0 by selecting the corresponding box. Restore the MBR if it is critical to your system booting.

When MBR restoration is chosen, there will be the "Restore disk signature" box in the bottom left corner at the next step. Restoring disk signature may be desirable due to the following reasons:

1) Acronis True Image Home creates scheduled tasks using the signature of the source hard disk. If you restore the same disk signature, you don't need to re-create or edit the tasks created previously.

2) Some installed applications use disk signature for licensing and other purposes.

3) If you use Windows Restore Points, they will be lost when the disk signature is not restored.

4) In addition, restoring disk signature allows to restore VSS snapshots used by Windows Vista's "Previous Versions" feature.

If the box is unselected, Acronis True Image Home generates a new disk signature for the restored drive. This may be needed when you use an image backup not for disaster recovery but for cloning your Windows Vista hard drive to another one. Trying to boot Windows after

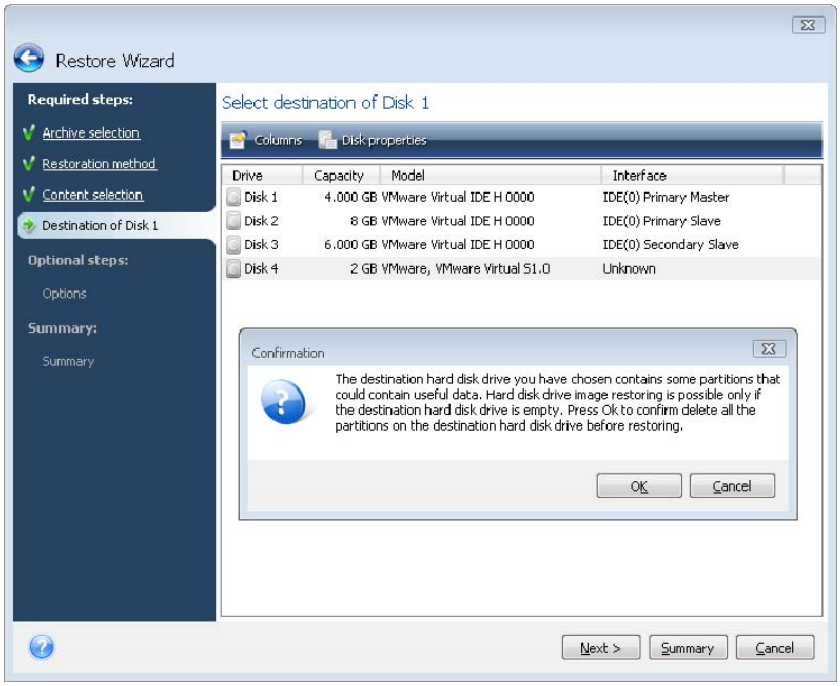
cloning with both drives connected will result in a problem. During Windows booting its loader checks the disk signatures of all of the connected drives, and if it finds two identical disk signatures, the loader changes the signature of the second disk, which would be the clone disk. Once this happens, the clone disk would not be able to boot up independently of the original disk, because the MountedDevices fields in the clone's registry reference the disk signature of the original disk, which will not be available if the original disk is disconnected.

6.3.5 Selecting a target disk/partition

1. Select a target disk or partition where you want to restore the selected image. You can restore data to its initial location, to another disk/partition or to an unallocated space. The target partition should be at least the same size as the uncompressed image data.

All the data stored on the target partition will be replaced by the image data, so be careful and watch for non-backed-up data that you might need.

2. When restoring an entire disk, the program will analyze the target disk structure to see whether the disk is free.



If there are partitions on the target disk, you will be prompted by the confirmation window stating that the destination disk contains partitions, perhaps with useful data.

You will have to select between:

- **OK** – all existing partitions will be deleted and all their data will be lost.
- **Cancel** – no existing partition will be deleted, discontinuing the recovery operation. You will then have to cancel the operation or select another disk.

Note that no real changes or data destruction will be performed at this time! For now, the program will just map out the procedure. All changes will be implemented only when you click **Proceed** in the wizard's **Summary** window.

6.3.6 Changing the restored partition type

When restoring a partition, you can change its type, though it is not required in most cases.

To illustrate why you might need to do this, let's imagine that both the operating system and data were stored on the same primary partition on a damaged disk.

If you are restoring a system partition to the new (or the same) disk and want to load the operating system from it, you will select **Active**.

Acronis True Image Home automatically corrects boot information during restore of the system partition to make it bootable even if it was not restored to the original partition (or disk).

If you restore a system partition to another hard disk with its own partitions and OS, most likely you will need only the data. In this case, you can restore the partition as **Logical** to access the data only.

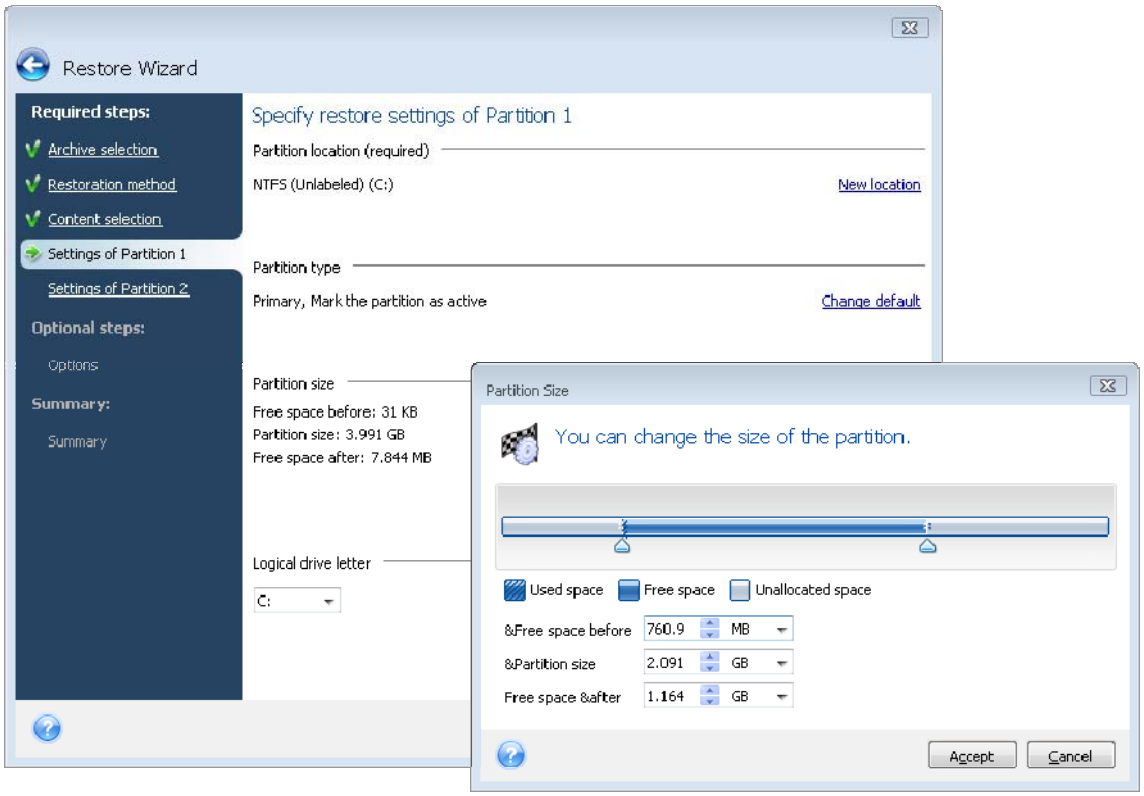
By default, the original partition type is selected.

Selecting **Active** for a partition without an installed operating system could prevent your computer from booting.

6.3.7 Changing the restored partition size and location

You can resize and relocate a partition by dragging it or its borders with a mouse on the horizontal bar on the screen or by entering corresponding values into the appropriate fields.

Using this feature, you can redistribute the disk space among partitions being restored. In this case, you will have to restore the partition to be reduced first.



These changes might be useful if you are going to copy your hard disk to a new high-capacity one by creating its image and restoring it to a new disk with larger partitions.

6.3.8 Assigning a letter to the restored partition

Acronis True Image Home will assign an unused letter to a restored partition. You can select the desired letter from a drop-down list or let the program assign a letter automatically by selecting the **Auto** setting.

You should not assign letters to partitions inaccessible to Windows, such as to those other than FAT and NTFS.

6.3.9 Setting restore options

Select the options for the restoration process (that is, restoration process priority, etc.). The settings will be applied only to the current restore task. Or, you can edit the default options. See *6.4 Setting restore options* for more information.

6.3.10 Restoration summary and executing restoration

At the final step, the restoration summary is displayed. Up to this point, you can make changes in the created task by choosing the step you want to change and editing its settings. If you click **Cancel**, no changes will be made to disk(s). Clicking **Proceed** will launch the task execution.

The task progress will be shown in a special window. You can stop the procedure by clicking **Cancel**. However, it is critical to note that the target partition will be deleted and its space unallocated – the same result you will get if the restoration is unsuccessful. To recover the "lost" partition, you will have to restore it from the image again.

6.4 Setting restore options

6.4.1 Files to preserve during restoration

This option is not applicable to restoration of disks and partitions from images.

By default, the program will not overwrite any files and folders, thus giving the files on the hard disk unconditional priority over the archived files.

Selecting the **Overwrite existing files** checkbox will give the archived files unconditional priority over the files on the hard disk.

You can set default filters for the specific types of files you wish to preserve during archive restoration. For example, you may want hidden and system files and folders, newer files and folders, as well as files matching selected criteria not to be overwritten by the archive files.

While specifying the criteria, you can use the common Windows wildcard characters. For example, to preserve all files with extension .exe, add ***.exe**. **My???.exe** will preserve all .exe files with names consisting of five symbols and starting with "my".

6.4.2 Pre/post commands

You can specify commands or batch files to be automatically executed before and after the restore procedure. Click **Edit** to open the **Edit Command** window where you can easily input the command, its arguments and working directory or browse folders to find a batch file.

Please note that interactive commands, i.e. commands that require user input, are not supported.

Unselecting the **Do not perform operations until the commands execution is complete** box, selected by default, will permit the restore procedure to run concurrently with your commands execution.

If you want the restore to be performed even if your command fails, uncheck the **Abort the operation if the user command fails** box (checked by default).

You can test execution of the command you created by clicking the **Test command** button.

Please, keep in mind that when restoring the system partition to the original place your post command will not be executed because recovery of the system partition requires a reboot, resulting in loss of the command. Such a command will also be lost if the program requests a reboot during any other restore operation.

6.4.3 Restoration priority

The preset is **Low**.

The priority of any process running in a system determines the amount of CPU usage and system resources allocated to that process. Decreasing the restoration priority will free more resources for other CPU tasks. Raising restoration priority may speed up the restore process as it takes resources from other currently running processes. The effect will depend on total CPU usage and other factors.

6.4.4 File-level security settings

The preset is **Restore files with their security settings**.

If the file security settings were preserved during backup (see *5.4.7 File-level security settings*), you can choose whether to restore them or let the files inherit the security settings of the folder where they will be restored.

This option is effective only when restoring files from file/folder archives.

6.4.5 Additional settings

1. You can choose whether to restore the file date and time from the archive or assign the files the current date and time. By default the current date and time will be assigned.

2. Before data is restored from the archive, Acronis True Image Home can check its integrity. If you suspect that the archive might have been corrupted, select **Validate backup archive before restoration**.

You must have all incremental and differential backups belonging to the archive and the initial full backup to check archive data integrity. If any backups are missing, the validation is not possible.

3. Having restored a disk/partition from an image, Acronis True Image Home can check the integrity of the file system. To do so, select **Check file system after restoration**.

Limitations on use of this option:

- Check of the file system is available only when restoring disk/partitions using FAT16/32 and NTFS file systems.
- The file system will not be checked if a reboot is required during restoration, for example, when restoring the system partition to its original place.

Chapter 7 Try&Decide

The Try&Decide feature allows creating a secure, controlled temporary workspace on your computer without requiring you to install special virtualization software. You can perform various system operations not worrying that you might damage your operating system, programs or data.

After making virtual changes, you may apply them to your original system. If you make changes that you want to keep, you might want to commit those changes to the system. Among the operations you may attempt with this feature is to open mail attachments from unknown senders or visit websites that might contain potentially troublesome content.

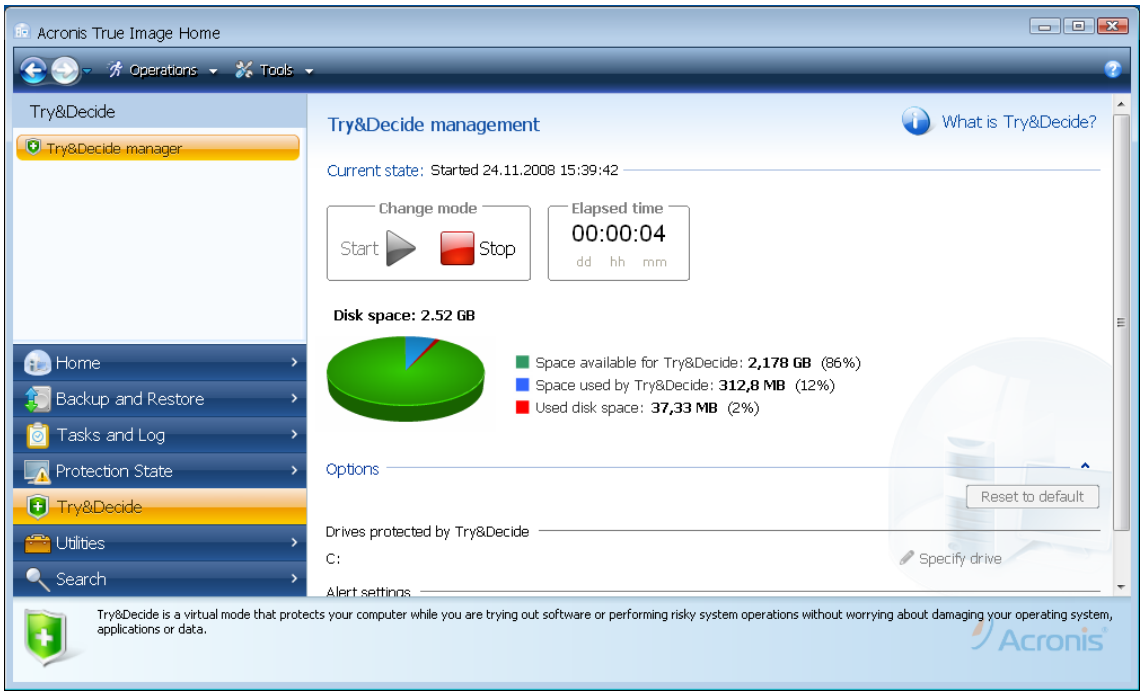
For example, if you visit a website or open an email attachment that puts a virus on your temporary duplicate, you can simply destroy the duplicate and no harm will be done – the virus will not appear on your machine.

It is important to remember that if you download e-mail from a POP mail server, create new files or edit existing documents while in the Try&Decide mode and then decide to discard your changes, those files, document changes, and mail will no longer exist. If you use POP email, make sure to change the settings in your e-mail to leave your mail on the server *before* you activate the Try&Decide mode. This way, you can always retrieve your email again. Similarly, save new files and/or edited documents to a drive not protected by Try&Decide.

After starting Try&Decide mode you can safely install any system updates, drivers and applications without worrying about what might happen to your system. If anything goes wrong, you can simply discard the changes made in the Try&Decide mode.

One of the best features of Try&Decide is that it isolates your "real" operating system from changes to the temporary operating system duplicate made by updates. Should you find any kind of incompatibility, you can easily revert your system to the initial state, which was not changed when the update was applied.

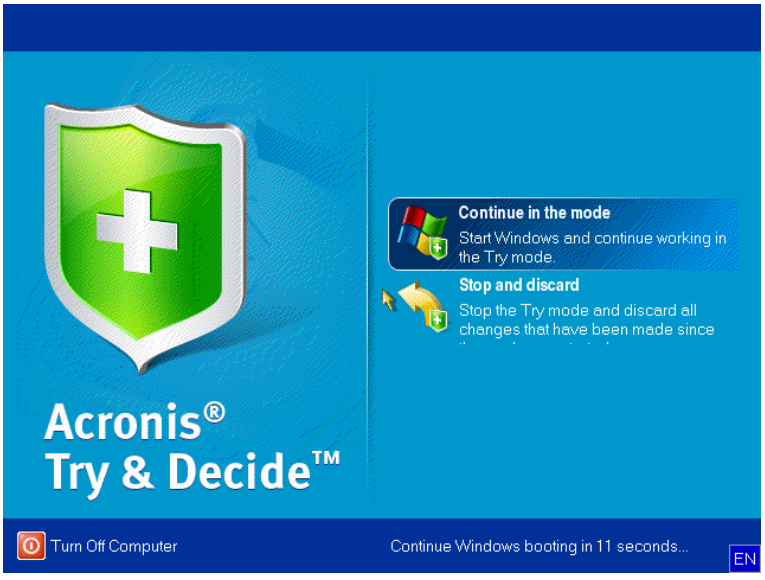
Because of this, you can safely install system updates when they appear. When Windows Update informs you that updates for the system and Microsoft applications are ready for installing, turn on the Try&Decide mode and then proceed to install the updates. If you encounter any sort of problem, discard the changes and leave your real operating system and applications untouched.



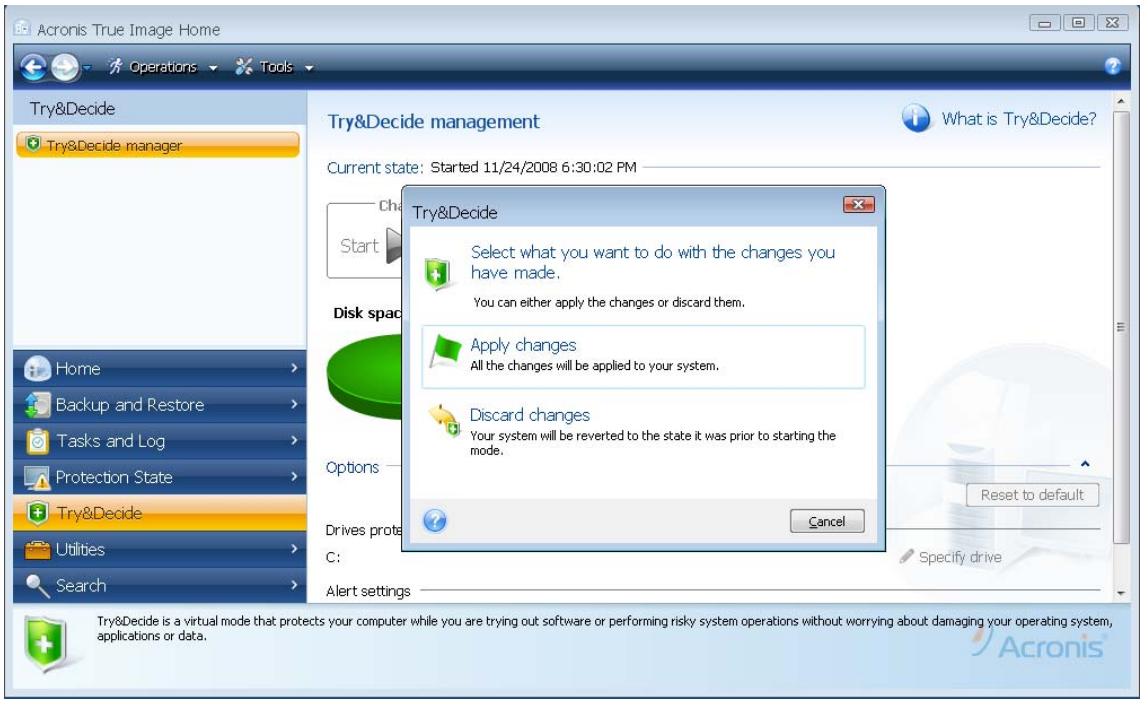
You can leave the Try&Decide mode turned on as long as you like (may be days on end, however in such a case applying changes may take a long time), since this mode "survives" across reboots of your operating system.

If you use Windows Vista, please, be aware that in the Try&Decide mode the program may use the free space in the Acronis Secure Zone quite intensively, even when your computer is idle. This is due to Windows Vista's housekeeping activities such as indexing that run in the background.

When your computer reboots for whatever reason while working in the Try&Decide mode, before booting of the operating system starts, you will be shown a dialog offering you two choices – stop the mode and discard changes or continue working in the mode. This will allow discarding the changes that have resulted in a system crash. On the other hand, if you reboot, for example, after installing an application, you can continue working in the Try&Decide mode after starting Windows.



The moment comes eventually when you decide to turn the mode off by clicking the **Stop** button. After clicking the button, the program will show a dialog where you should decide what to do with the changes to your system made in the Try&Decide mode - apply or discard:



Choosing **Apply changes** will allow you to keep the changes made to the system, and choosing **Discard changes** will return your system to the state it was in before turning on the Try&Decide mode.

Please note that while working in the Try&Decide mode you will experience slowing down of the system performance. Furthermore, the process of applying changes could take considerable time.

Please be aware that the Try&Decide cannot track changes in disk partitions, so you will be unable to use the Try&Decide mode for virtual operations with partitions such as resizing partitions or changing their layout. In addition, you must not use the Try&Decide mode and disk defragmentation or disk error checking utilities at the same time, because this can irreparably corrupt the file system, as well as make the system disk unbootable.

Acronis True Image Home will track changes until the Acronis Secure Zone is almost full. Then the program will alert you that the time has come to make a decision on whether to apply or discard the changes made so far. If you choose to not heed the alert message, the program will automatically restart the system when the zone is full, discarding the changes in the process of rebooting. At that point, all changes will be lost.

When the Try&Decide mode is started, you won't be able to use the previously activated Acronis Startup Recovery Manager.

If you have chosen **Discard Changes** and rebooted the computer with multiple operating systems installed, you won't be able to boot other operating systems, except the one used for working in the Try&Decide mode. The second reboot will restore the original MBR and make other operating systems bootable.

7.1 Using Try&Decide

Now let's see how to use this feature. First of all, you should decide for yourself which part of your system you want to protect and set the Try&Decide options correspondingly. Those options also provide other settings for the Try&Decide mode.

7.1.2. Try&Decide options

You can configure Try&Decide options as required.

- **Partition protected by T&D** – specify the partition you want to protect from unauthorized changes during a Try&Decide session. By default, T&D protects Disk C, though you may choose to protect any other partition in your system.
- **Alert settings** – specify whether Try&Decide should alert you when it uses up all the space allotted for saving virtual changes and after a specified time period has passed. By default all alerts are On.

7.2 Try&Decide usage examples

The Try&Decide feature can help you in a variety of ways; here are some examples:

There are cases when the installation of antivirus software cripples functionality of some applications; in fact, some programs might even refuse to start after antivirus installation. The Try&Decide feature can help you to avoid such a problem. Here's how:

1. Select an antivirus program and download a trial version.

2. Turn on the Try&Decide mode.

3. Install the antivirus software.

4. Try to work with the applications installed on your computer performing your usual tasks.

5. If everything works without any snags, you can be reasonably sure that there will be no incompatibility problems and can buy the antivirus software.

6. If you encounter any problems, discard the changes in your system and try antivirus software from another vendor. The new attempt might turn out to be successful.

Here's another example: You have accidentally deleted some files and then emptied the Recycle Bin. Then you have remembered that the deleted files contained important data and now you are going to try to undelete them using an undelete software program. However, sometimes you may do something wrong while trying to recover deleted files, making things worse than before trying to recover them. Here's one way you could try to recover the lost files:

1. Turn on the Try&Decide mode.

2. Launch the file undelete utility.

3. After the utility scans your disk in search of the deleted file or folder entries, it will present you the deleted entries it has found (if any) and offer you the opportunity to save whatever it is able to recover. There is always a chance that you might pick the wrong file and while recovering it the utility may overwrite the very file you are trying to recover. If not for Try&Decide, this error would be fatal and the file would be lost irretrievably.

4. But now you can simply discard the changes made in the Try&Decide mode and make one more attempt to recover the files after turning on the Try&Decide mode again. Such attempts can be repeated until you recover the files or until you are sure that you have done your best to recover them.

One more benefit of the Try&Decide feature. Now you can let your children use your computer without worrying that they may inadvertently harm the operating system or mess up your business documents.

We assume that your kid has the Limited user account type.

1. Turn on the Try&Decide mode. Making any changes to the Try&Decide options or turning off the Try&Decide mode will require administrator authority.

2. Log off and then log on using your kid's account.

3. Let your kid use the computer. When your kid is through with gaming or Internet surfing or when you think that it is time for the kid to go to bed, return the system to the state it was in before your kid started using the computer. To do so, log on and discard the changes made during the Try&Decide session.

It is well known that the "Add or Remove Programs" component of the Windows Control Panel cannot give a complete guarantee of cleanly uninstalling applications. This is because most applications do not provide enough information for it to be able to uninstall them without a trace. So almost every time you install a trial program and then remove it, you have some garbage left on your computer and after a while Windows may get slower. Even use of special uninstaller utilities cannot guarantee complete uninstallation. The Try&Decide feature, however, will ensure complete and perfect uninstallation of any software quickly and easily. Here's how:

1. Turn on the Try&Decide mode.

2. Install the software application you want to evaluate.

3. Try using the application.

4. When you want to uninstall it, just discard all the changes made to your computer in the Try&Decide mode.

This may come in handy not only for those who, for example, like to play a lot of games but for professional software testers as well – to use on their testing machines.

Chapter 8. Scheduling tasks

Acronis True Image Home allows you to schedule periodic backup and validation tasks. Doing so will give you peace of mind, knowing that your data is safe.

You can create more than one independently scheduled task. For example, you can back up your current project daily and back up the system disk once a week.

One consideration in choosing a backup schedule is media management. For example, if you're backing up to a recordable DVD, you must be prepared to insert a blank disc whenever the schedule runs. On the other hand, if you schedule backups to run when you're not around, you must always think ahead and make sure the drive has the necessary media ready. If, on the other hand, you're backing up to a hard disk or network device that can stay connected all the time, this problem is less likely to occur.

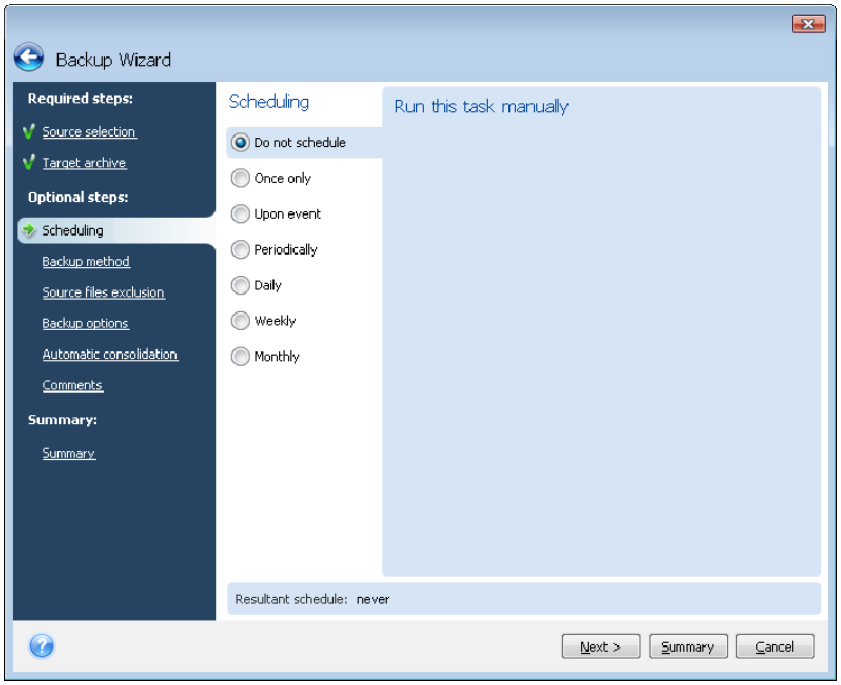
If you are performing a scheduled backup task to a USB flash drive, the backup process will begin automatically when the device is plugged in, but only when a scheduled backup has been missed. The USB flash drive must be the same as the one used for all previous backups; if you plug in another flash drive, the backup process won't start.

8.1 Creating scheduled tasks

You can schedule a new task in the **Backup Wizard** or **Validate Wizard** in the **Scheduling** step. It is also possible to create a scheduled task by clicking **Create Backup Task** or **Create Validation Task** on the toolbar of the **Manage Tasks and Log** screen.

If the backup archive you want to validate is protected with a password, Acronis True Image Home will ask for it.

1. Perform task running scheduling. Select one of the following scheduling options:



- **Once only** – the task will be executed once at the specified time and day
- **Upon event** – the task will be executed on an event to be selected in the right pane:

- **Periodically** – the task will be executed periodically with a frequency to be specified in the **Run this task periodically** pane, where you specify the time between runs for the task being scheduled.
- **Daily** – the task will be executed once a day or once every several days
- **Weekly** – the task will be executed once a week or once every several weeks on the selected day
- **Monthly** – the task will be executed once a month on the selected day

To postpone a scheduled task until the next time the user is idle, select the **Run when the user is idle** box. The task will automatically start when you are idle (not using the mouse and the keyboard) for the number of minutes specified in the **Wait** setting of the screen saver or when you log off. Once the task has started, it will be completed because task execution cannot be interrupted by the user. However, you can work on the computer while the task is running.

If the computer is off when the scheduled time comes, the task won't be performed, but you can force the missed task to run at the next system startup by selecting the **If missed, run the task at startup** box.

If you schedule a task for performing backup to a USB flash drive, one more checkbox appears on the scheduling screen – **If missed, run the task when device is attached**. Selecting this box will let you perform a missed backup when the USB flash drive is attached if it was disconnected at the scheduled time. If you want the missed task to be performed only when the same device is attached, select the **Run task only if the current device is attached** box. Otherwise the missed task will run when any USB flash drive is attached.

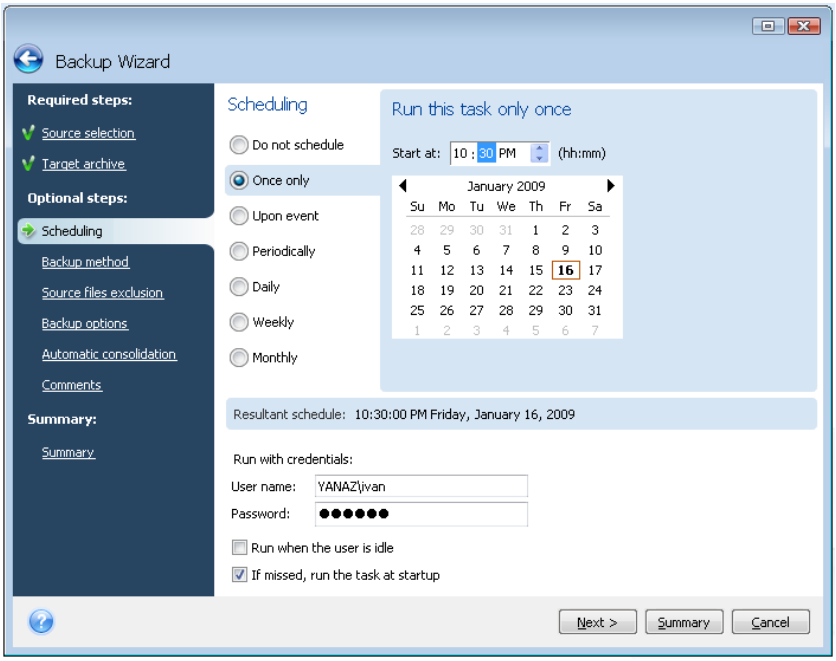
2. Specify the task start time and other schedule parameters, according to the selected periodicity (see 8.1.1 - 8.1.5).

3. Next you will have to specify the name of the user who owns the task to be executed; otherwise no scheduled execution will be available.

Enter the user name (or leave the name of the logged on user). Enter the password.

8.1.1 Setting up once only execution

If you choose once only execution, set the start time. Then set the date on which to execute the task using the provided calendar:

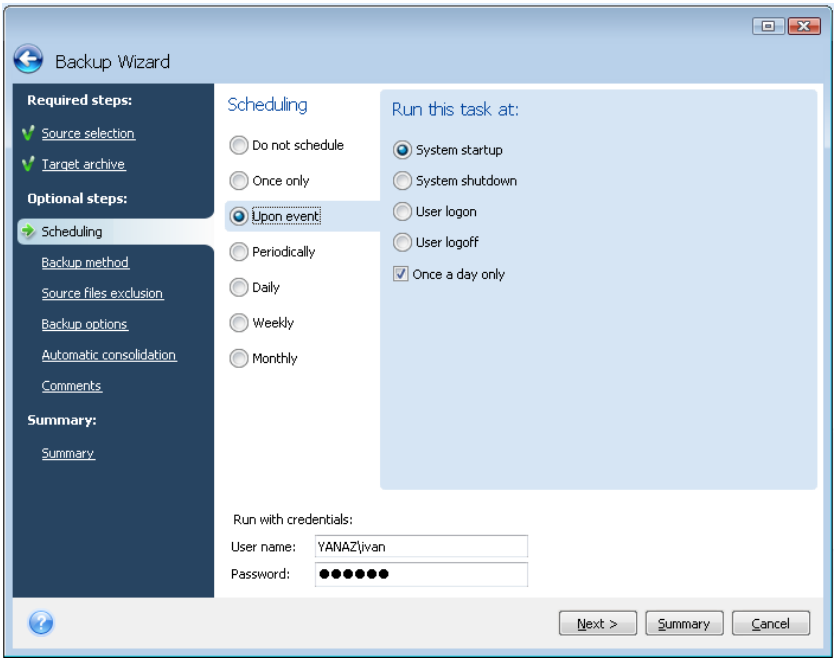


8.1.2 Setting up upon event execution

If you choose the upon event execution option, set the event upon which to execute the task:

- **System startup** – the task will be executed at every OS startup
- **System shutdown** – the task will be executed before every system shutdown or reboot
- **User logon** – the task will be executed each time the current user logs on to the OS
- **User logoff** – the task will be executed each time the current user logs off of the OS.

If you want to run a task only at the first occurrence of the event on the current day, select the **Once a day only** box.

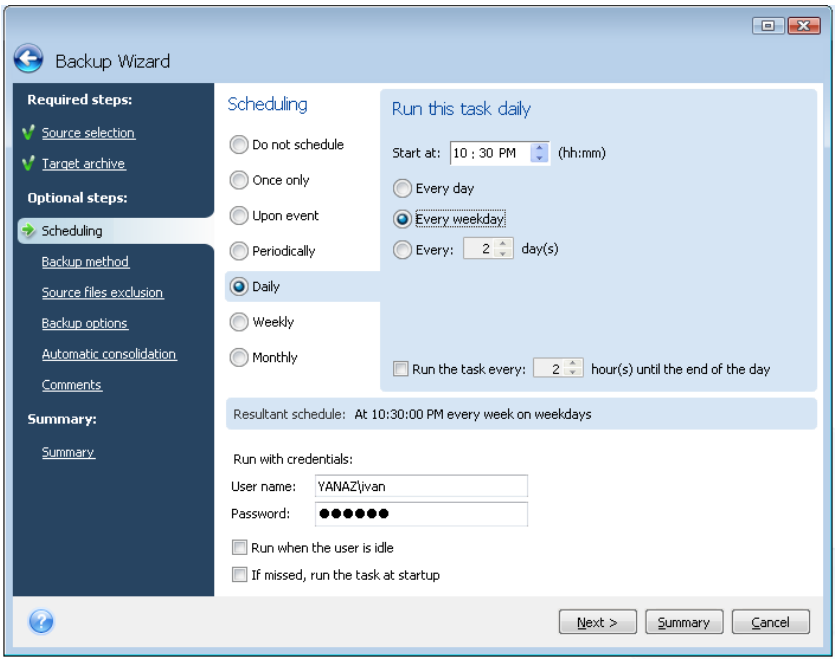


8.1.3 Setting up daily execution

If you choose daily execution, set the Start time and days on which you want to execute the task:

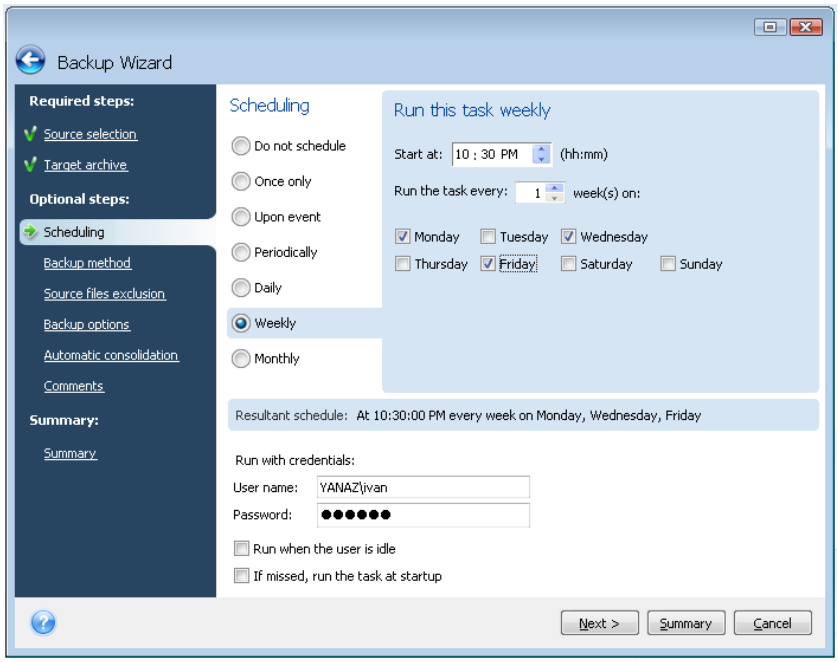
- **Every day**
- **Every weekday**
- **Every x days** – once every several days (specify the interval).

If you want the task to be repeated several times per day, select **Run the task every x hour(s) until the end of the day** box and specify the interval in hours.



8.1.4 Setting up weekly execution

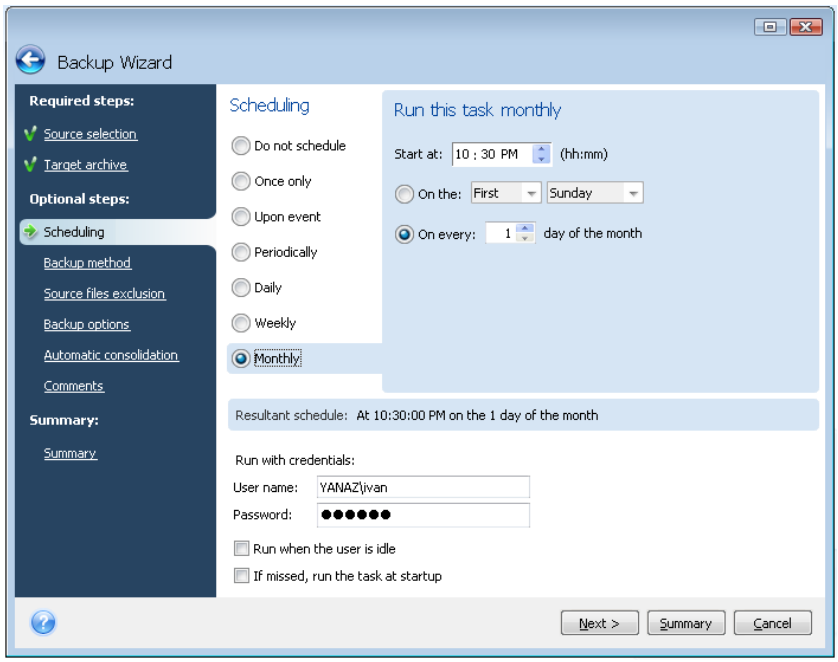
If you choose weekly execution, set the Start time, specify the task execution periodicity in the **Run the task every x week(s) on:** box (every week, every two weeks, etc.) and select the days on which to execute the task.



8.1.5 Setting up monthly execution

If you select monthly execution, set the Start time and days on which to execute the task:

- **On the <specify a day>** – on the specified day (e.g. on second Tuesday or fourth Friday); select this from the drop-down lists.
- **On every x day of the month** – on the specified date



8.2 Managing scheduled tasks

To manage the scheduled tasks, click **Tasks and Log** on the sidebar and you will go to the **Manage Tasks and Log** screen with the **Scheduled tasks** tab selected by default in the right pane. The tab displays all scheduled tasks along with their name, status, schedule, last run time, last result, and owner. To view the other task details, mouse over their names.

By default you see only your own tasks, but you have the option to view or manage tasks of other users. To do so, select **Tools -> Options -> Task options** from the main program menu. Then choose **Filter** and unselect the **Show only tasks created by a current user** box.

You can change the task parameters by editing. This is performed in the same way as creation, however, the earlier selected options will be set, so you only have to enter the changes. To edit a task, select it and click **Edit** on the toolbar.

To delete a task with confirmation, select it and click **Delete** on the toolbar.

To rename a task, select it, click **Rename** on the toolbar and enter the new task name.

You can also start execution of a scheduled task at any moment by clicking **Start** on the toolbar.

In addition, all the above actions can be chosen from a shortcut menu that you open by right-clicking on a selected scheduled task.

The same operations are available for unscheduled tasks listed on the **Unscheduled tasks** tab. If while editing an unscheduled task you set up any of the scheduling options, that task moves from the **Unscheduled tasks** tab to the **Scheduled tasks** tab.

Chapter 9. Managing Acronis Secure Zone

The Acronis Secure Zone is a special partition for storing archives on the same computer that created the archive. The Acronis Secure Zone is a required component for using the Acronis Startup Recovery Manager. For more information about these functions see *3.3 Acronis Secure Zone, 3.4 Acronis Startup Recovery Manager*.

When you select **Tools -> Manage Acronis Secure Zone** in the main menu, the program searches for the zone on all local drives. If a zone is found, the wizard will offer to manage it (resize or change the password) or delete it. If there is no zone, you'll be prompted to create it.

If the Acronis Secure Zone is password-protected, the correct password must be entered before any operation can take place.

9.1 Creating Acronis Secure Zone

The Acronis Secure Zone can be located on any internal disk. It is created using unallocated space, if available, or at the expense of free space on a partition. Partition resizing may require a reboot.

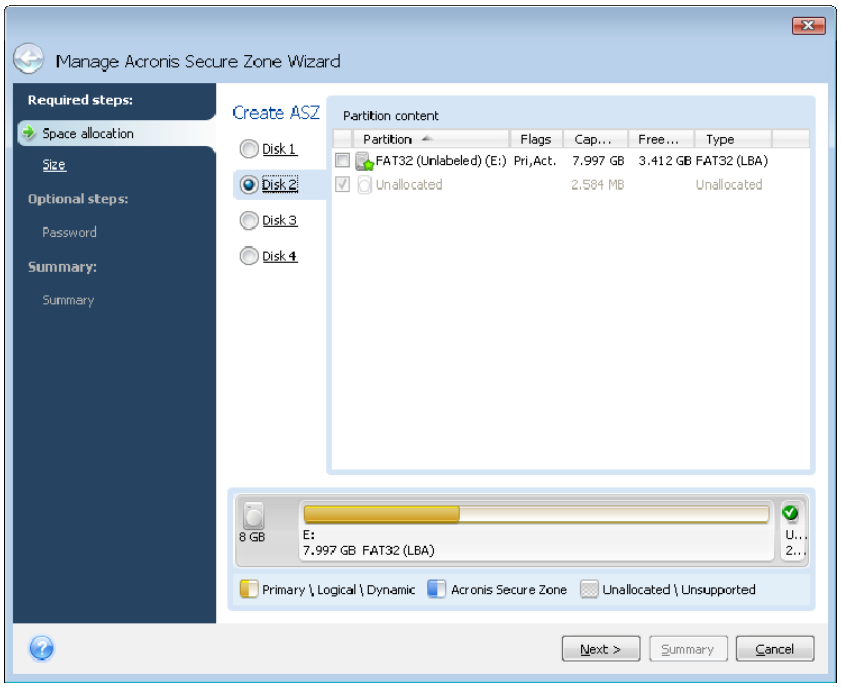
We do not recommend creating the Acronis Secure Zone on external media (USB drives, etc.), because this may lead to problems with computer booting if that external storage is disconnected.

A computer can have only one secure zone. To create a zone on another disk, you must first delete the existing zone.

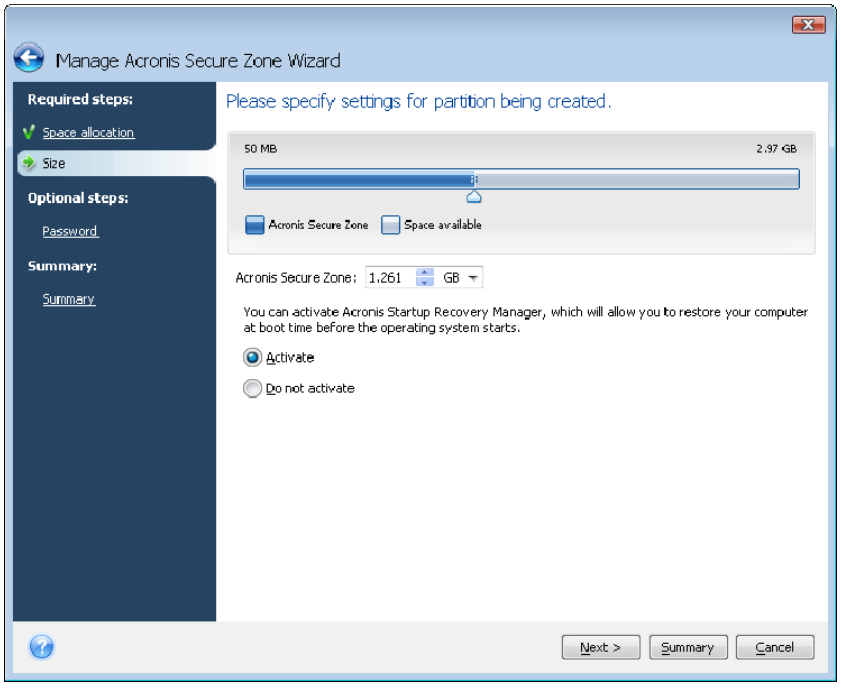
1. Before creating the zone, you need to estimate its size. To do so, start a backup and select all data you are going to copy into it. At the **Backup Options** step set the compression level. You will see the estimated full backup size (for disk/partition backup) or the approximate compression ratio (for file-level backup) with which you can calculate the estimated full backup size. Multiply this by 1.5 to be able to create incremental or differential backups. Remember that the *average* compression rate is 2:1, so you can use this as a guide as well to create a zone. Let's say you have a hard disk with 10GB of programs and data. Under normal conditions, that will compress down to approximately 5GB. As a result, you might want to make the total size 7.5GB.

2. If there are several disks installed, select one on which to create Acronis Secure Zone.

3. Select the partitions from whose space the zone will be created.



4. In the next window, enter the Acronis Secure Zone size or drag the slider to select any size between the minimum and maximum ones.



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 the zone, the program will first use the unallocated space. If there is not enough unallocated space, the selected partitions will be decreased. Partition resizing may require a reboot.

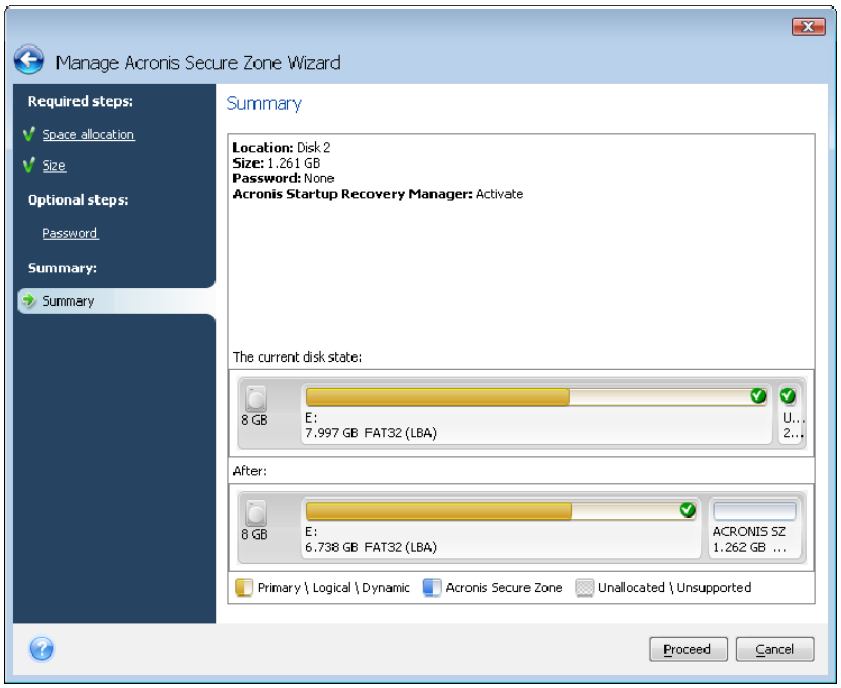
Reducing a system partition to the minimum size might prevent your operating system from booting.

5. You can set a password to restrict access to the zone. The program will ask for the password at any operation relating to it, such as data backup and recovery, mounting images or validating archives on the zone, rescue boot with the F11 key, resizing and deleting the zone.

Acronis True Image Home 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 zone will be reset.

6. After this, you will be prompted to activate Acronis Startup Recovery Manager, which will enable you to start Acronis True Image Home at boot time by pressing the F11 key. Or, you can activate this feature later from the main program window.

7. Then you will see a list of operations to be performed on the partitions (disks).

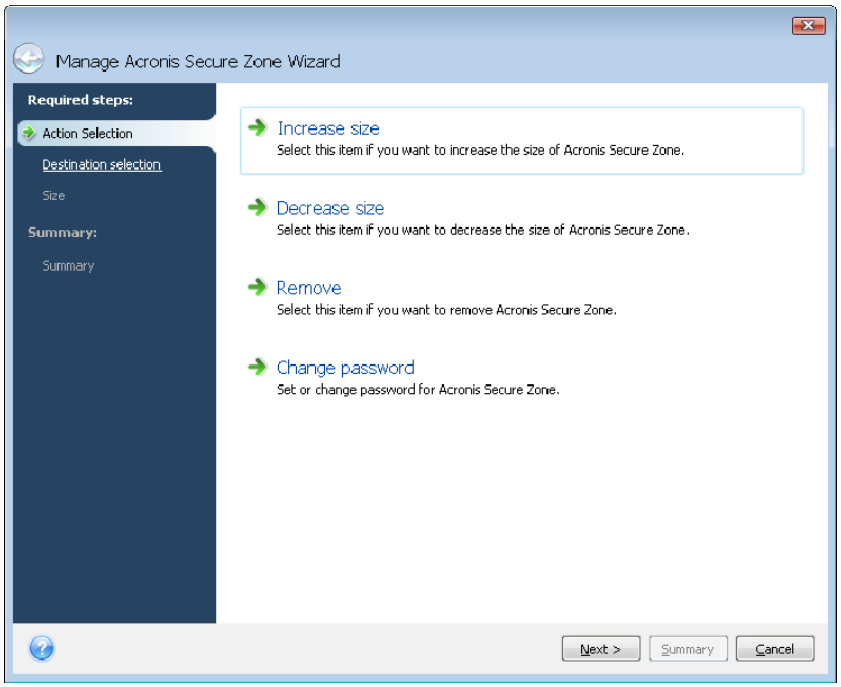


After you click **Proceed**, Acronis True Image Home will start creating the zone. Progress will be reflected in a special window. If necessary, you can stop zone creation by clicking **Cancel**. However, the procedure will be canceled only after the current operation is finished.

Acronis Secure Zone creation might take several minutes or more. Please wait until the whole procedure is finished.

9.2 Resizing Acronis Secure Zone

1. If you want to resize the Acronis Secure Zone, select **Tools -> Manage Acronis Secure Zone** in the main menu.



2. Select to increase or decrease the zone size. You might need to increase it to provide more space for archives. The opposite situation may arise if any partition lacks free space.

3. Select partitions from which free space will be used to increase Acronis Secure Zone or that will receive free space after the zone is reduced.

4. Enter the new size of the zone or drag the slider to select the size.

When increasing the Acronis Secure Zone, the program will first use unallocated space. If there is not enough unallocated space, the selected partitions will be decreased. Resizing of the partitions may require a reboot.

When reducing the zone, any unallocated space, if the hard disk has any, will be allocated to the selected partitions along with the space freed from the zone. Thus, no unallocated space will remain on the disk.

5. Next you will see a list of briefly described operations to be performed on partitions (disks).

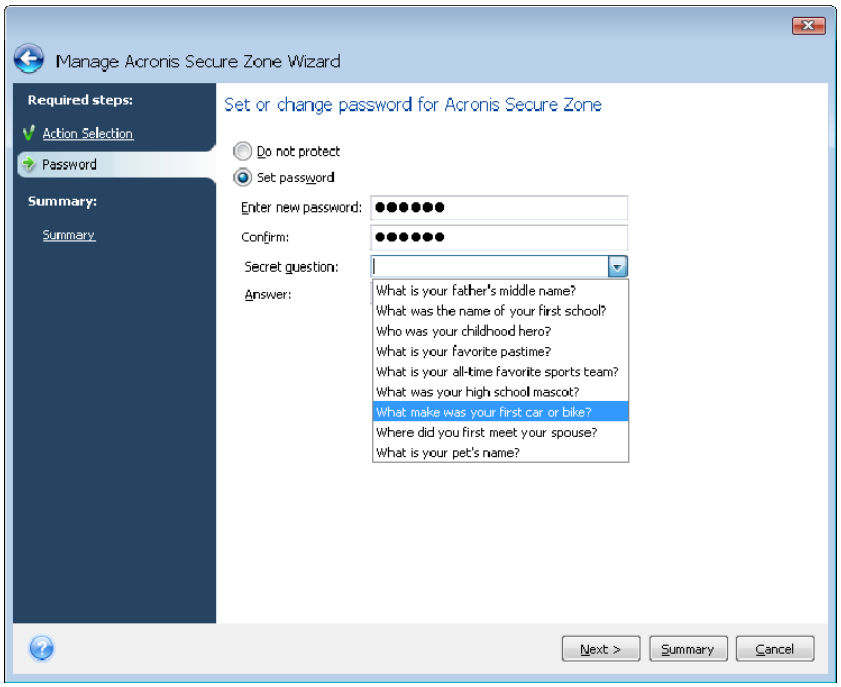
After you click **Proceed**, Acronis True Image Home will start resizing the zone. Progress will be reflected in a special window. If necessary, you can stop the procedure by clicking **Cancel**. However, the procedure will be canceled only after the current operation is finished.

Zone resizing can take several minutes or longer. Please wait until the whole procedure is finished.

9.3 Changing password for Acronis Secure Zone

1. If you want to change the password for the Acronis Secure Zone, select **Tools -> Manage Acronis Secure Zone** in the main menu.

2. Select **Change password.**



3. Enter the new password and confirm it or select **Do not use password protection**. You can also select a secret question that will be asked in case you forget the password.

4. To perform the password change operation, click **Proceed** in the final wizard window.

9.4 Deleting Acronis Secure Zone

1. If you want to remove the Acronis Secure Zone, select **Tools -> Manage Acronis Secure Zone** in the main menu and then choose **Remove Acronis Secure Zone**.

2. Select the partitions to which you want to add the space freed from the zone. If you select several partitions, the space will be distributed proportionally to each partition.

3. Next, you will see a list of briefly described operations to be performed on partitions (disks).

After you click **Proceed**, Acronis True Image Home will start deleting the zone. Progress will be reflected in the opened window. If necessary, you can stop the procedure by clicking **Cancel**. However, the procedure will be canceled only after the current operation is finished.

Zone deletion might take several minutes or more. Please wait until the whole procedure is finished.

Acronis Secure Zone deletion will automatically destroy all backups stored in the zone and disable the Acronis Startup Recovery Manager.

Chapter 10. Creating bootable media

You can run Acronis True Image Home from an emergency boot disk 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 archive by imaging the disk one sector at a time. To do so, you will need bootable media that has a copy of the standalone Acronis True Image Home version installed on it.

If you purchased the boxed product, you already have a bootable CD, because the installation CD itself is bootable in addition to serving as the program installation disk.

If you purchased Acronis True Image Home on the Web or as a download from a retailer, you can create bootable media using the Bootable Media Builder. For this, you will need a blank CD-R/RW, a blank DVD±R/RW or any other media from which your computer can boot, such as a Zip drive.

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

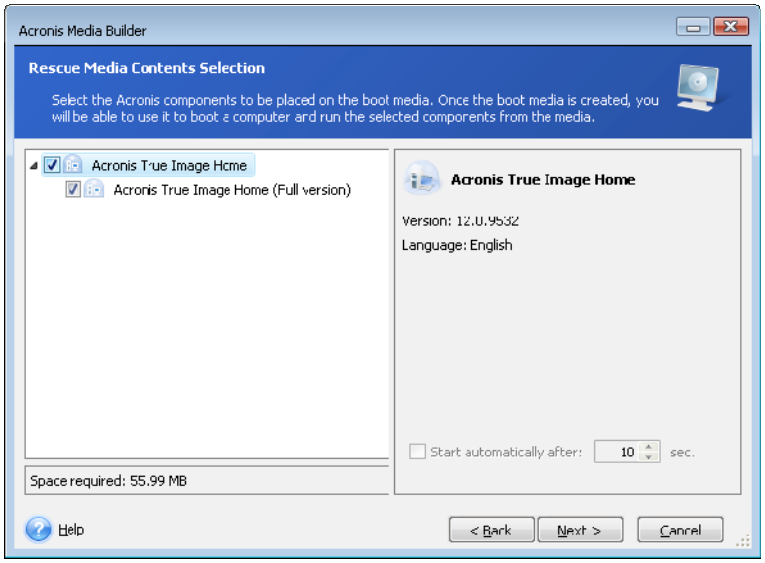
If you have other Acronis products, such as Acronis Disk Director Suite, installed on your computer, you can include standalone versions of these programs on the same bootable disk as well.

If you have chosen not to install the Bootable Media Builder during Acronis True Image Home installation, you will not be able to use this feature.

When booting from the Rescue Media, you cannot perform backups to disks or partitions with Ext2/Ext3, ReiserFS, and Linux SWAP file systems.

1. Choose **Create Bootable Rescue Media** in the **Tools** menu. You can also run the Bootable Rescue Media Builder without loading Acronis True Image Home by choosing **Programs -> Acronis -> Acronis True Image Home -> Bootable Rescue Media Builder** from the **Start menu**.

2. Select which components of Acronis programs you want to place on the bootable media.



Acronis True Image Home offers the following component:

- **Acronis True Image Home full version**

Includes support of USB, PC Card (formerly PCMCIA) and SCSI interfaces along with the storage devices connected via them, and therefore is strongly recommended.

In the next window 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.). All the available startup parameters are listed in *Appendix D. Startup Parameters*. 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.

If you purchased the boxed product, the installation CD contains an installation file for installing **Acronis True Image Home** safe version and an Acronis True Image Home plug-in for the well-known **Bart PE** utility. The safe version does not include USB, PC Card, or SCSI drivers. Recommended for use on rare occasions where problems running the full version occur. After installation **Acronis True Image Home safe version** will appear as one of the components to be offered by **Acronis Media Builder** for placing on the bootable media and you will be able to add **Acronis True Image Home** safe version when creating your bootable rescue media.

Bart PE (Bart Preinstalled Environment) is a bootable Windows CD/DVD created from the original Windows XP or Windows Server 2003 installation/setup CD. Applications are installed into Bart PE in the form of plug-ins and Acronis True Image Home plug-in can be included into the Bart PE plug-in tab. Booting from the Bart PE CD/DVD with the included Acronis True Image Home plug-in, will allow you to work in a well-known Windows environment and use practically all Acronis True Image Home functionality for recovering your system from a disaster. For more information on the Bart PE visit the Bart PE homepage at http://www.nu2.nu/pebuilder/

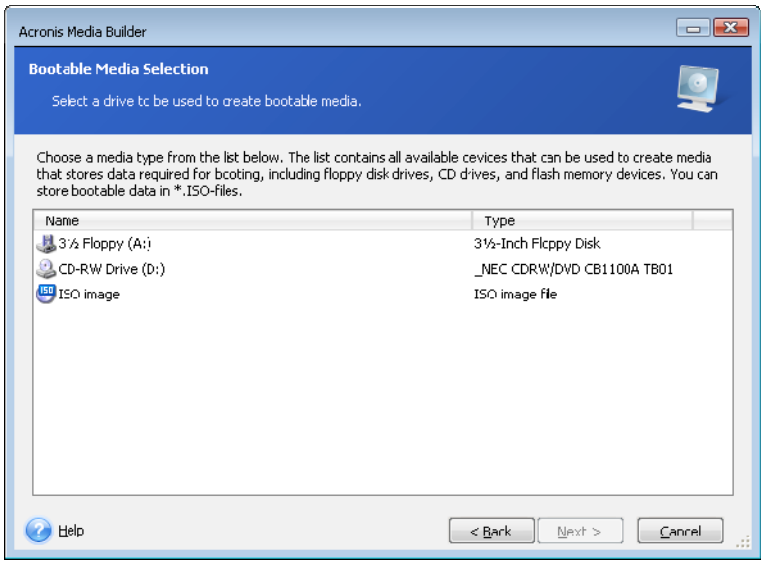
By the way, you can download that installation file from the Acronis website.

You may opt for automatic start of the bootable media creation. In this case select the **Start automatically after X seconds** box and specify the number of seconds (maximum 100 seconds).

To find out more about components of other Acronis products, see their respective user guides.

3. Select the type of bootable media (CD-R/RW, DVD±R/RW or 3.5” diskettes) to create. If your BIOS has this feature, you can create other bootable media such as removable USB flash drives. You can also choose to create a bootable disk ISO image.

When using 3.5” diskettes, you will only be able to write one component at a time (for example, the full version of Acronis True Image Home) on a set of diskettes. To write another component, start Bootable Media Builder again.



4. If you are creating a CD, DVD or any removable media, insert a blank disc so the program can determine its capacity. If you choose to create a bootable disc ISO image, specify the ISO file name and the folder in which to place it.

5. Next, the program will estimate how many blank diskettes are required (in case you have not chosen ISO or CD/DVD) and give you time to prepare them. When you are finished, click **Proceed**.

After you create a boot disc, mark it and keep it in a safe place.

Please keep in mind that the backups created by the later program version may be incompatible with the previous program versions. Due to this reason, we strongly recommend that you create a new bootable media after each Acronis True Image Home upgrade. One more thing you should remember – when booting from the rescue media and using a standalone version of Acronis True Image Home, you cannot recover files and folders encrypted with use of the encryption feature available in Windows XP and Windows Vista operating systems. For more information see *5.4.7 File-level security settings*. On the other hand, backup archives encrypted using the Acronis True Image Home encryption feature can be recovered.

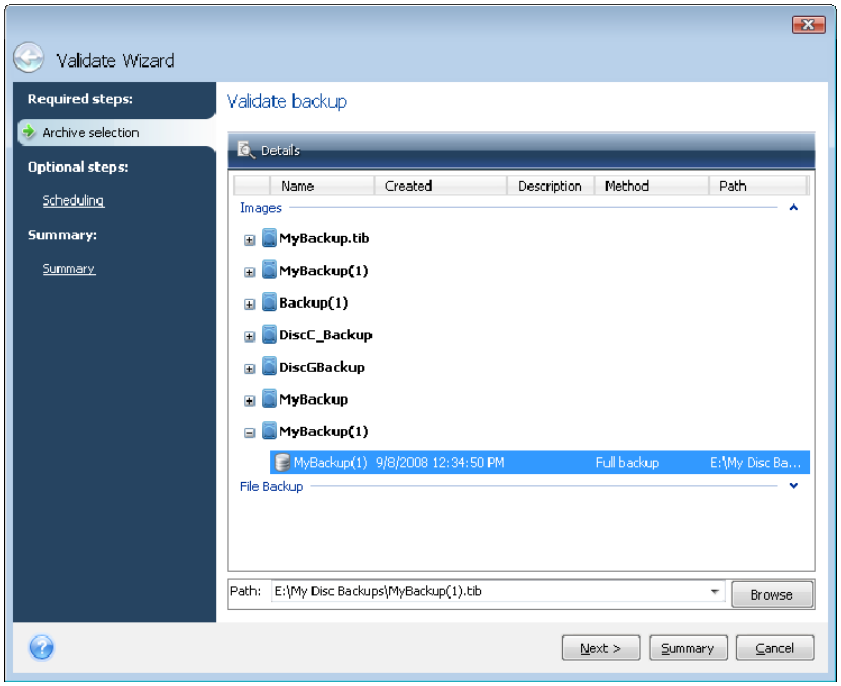
Chapter 11. Other operations

11.1 Validating backup archives

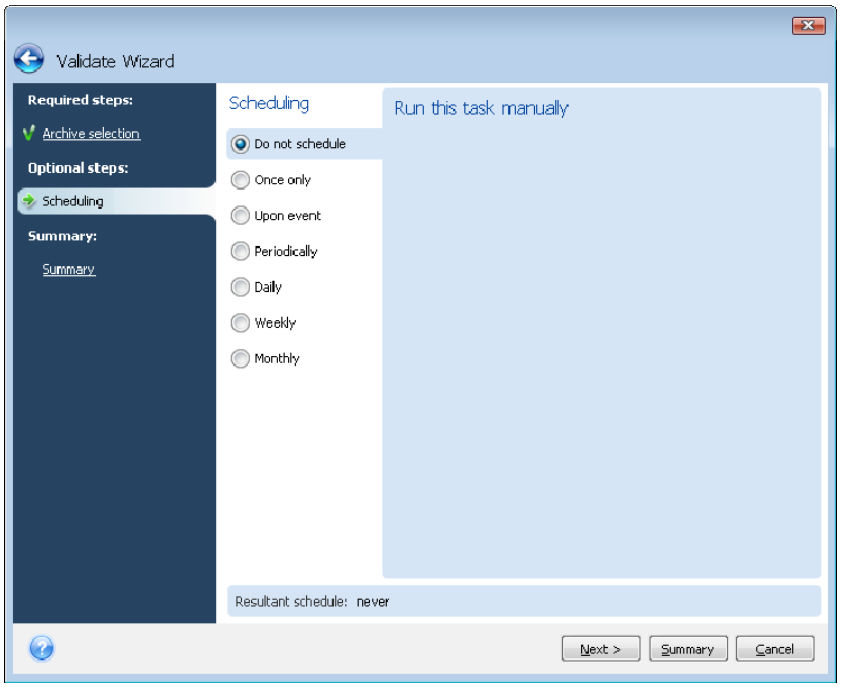
You can check the integrity of your backups to be certain that your archives are not damaged. You may perform such validations using the **Validate Wizard**.

1. To start the **Validate Wizard**, choose **Operations -> Validate Backup Archive** from the main program menu.

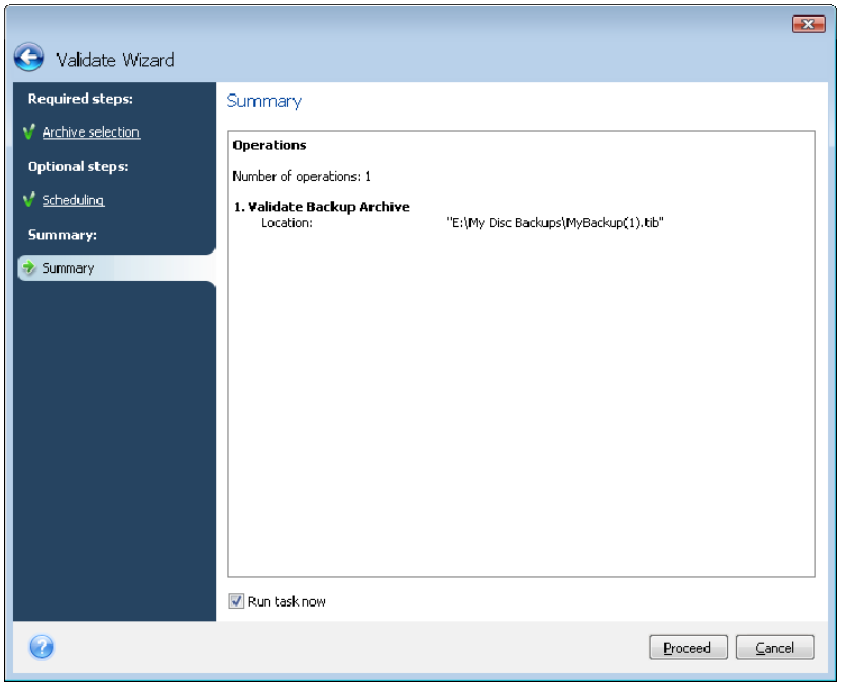
2. Select the archive to validate. Click **Next** to continue. If the selected archive is protected with a password, Acronis True Image Home will ask for the password in a dialog box. The **Next** button will be disabled until you enter the correct password.



3. After entering the correct password you will be taken to the Scheduling step, where you can schedule validation of the backup or leave the default setting **Do not schedule**.



4. Clicking **Proceed** in the summary window will launch the validation procedure if you leave the **Run task now** box selected. If you have decided to validate the backup archive on schedule, the **Run task now** box will be unselected by default and the validation will proceed according to the schedule you set, though you can also validate the backup right away by selecting this box. After the validation is complete, you will see the results window. You can cancel validation by clicking **Cancel**.



To check archive data integrity you must have all incremental and differential backups belonging to the archive and the initial full backup. If any of the successive backups are missing, validation is not possible.

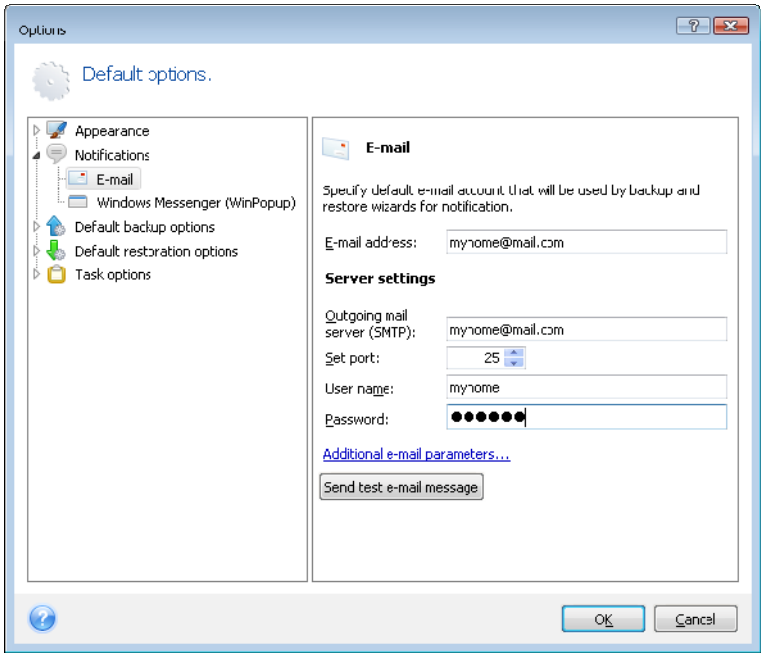
11.2 Operation results notification

Sometimes a backup or restore procedure can last for 30 minutes or more. Acronis True Image Home can notify you when it is finished using the WinPopup service or 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**.

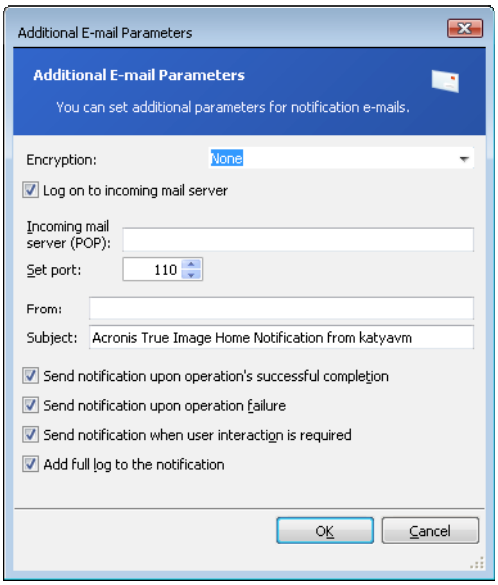
11.2.1 Email notification

To set up e-mail notification, select **Tools -> Options -> Notifications -> E-mail**:



Provide the email address to which notifications will be sent as well as the outgoing SMTP server name and port. A user name and a password might also be needed if the SMTP server requires user authentication.

To set up the additional e-mail parameters, click **Additional e-mail parameters...**



If the outgoing SMTP server requires logging on to an incoming mail server before it allows sending outgoing messages, enter the necessary information for the incoming mail server.

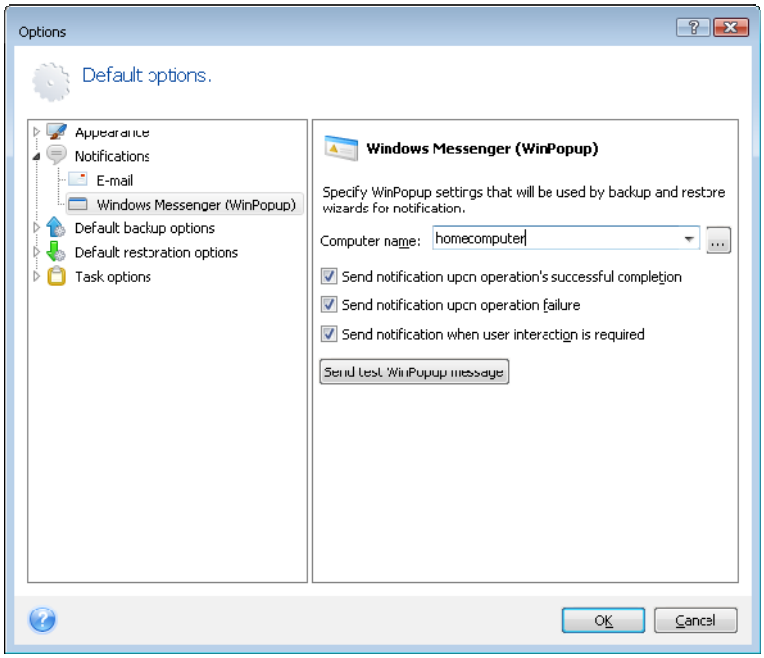
At the bottom of this window you can choose whether you want to get notifications:

- when the operation is completed successfully (check **Add full log to the notification** to add the full operation log to the message)
- if the operation failed (check **Add full log to the notification** to add the full operation log to the message)
- during the operation when user interaction is required

After setting up e-mail notifications, you can send a test mail message by clicking the appropriate button.

11.2.2 WinPopup notification

To set up WinPopup notification, select **Tools -> Options -> Notifications -> Windows Messenger (WinPopup)**:



Provide the name of the computer to which notifications will be sent.

At the bottom of this window you can choose whether you want to get notifications:

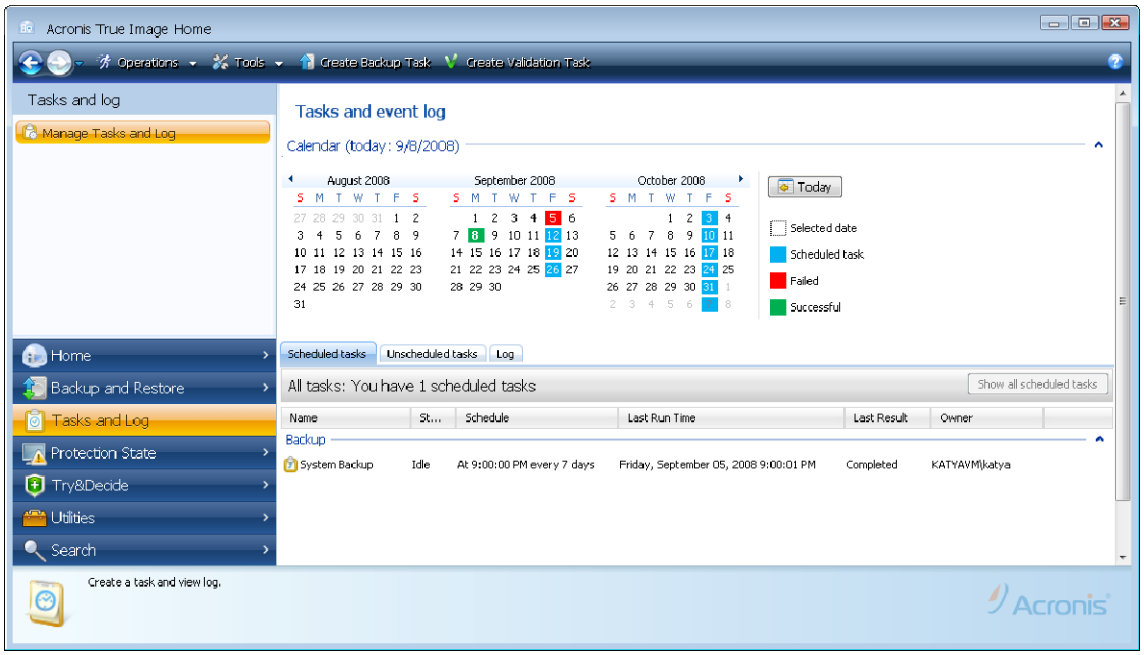
- when the operation is completed successfully
- when the operation failed
- during the operation when user interaction is required

11.3 Viewing Tasks and Logs

Acronis True Image Home has a Tasks and Log screen that allows you to view its working logs and scheduled tasks. The logs can provide information about scheduled backup or validation task results, including reasons for failure, if any.

To open the Tasks and Log screen, click **Tasks and Log** on the sidebar. By default, the screen opens with the **Scheduled Tasks** tab selected. The tab shows all scheduled tasks (if any). Selecting the **Unscheduled Tasks** tab will show all tasks that have been configured

after choosing **Do not schedule** at the Scheduling step in the Backup or Validation wizard, regardless of whether they have been completed or not.



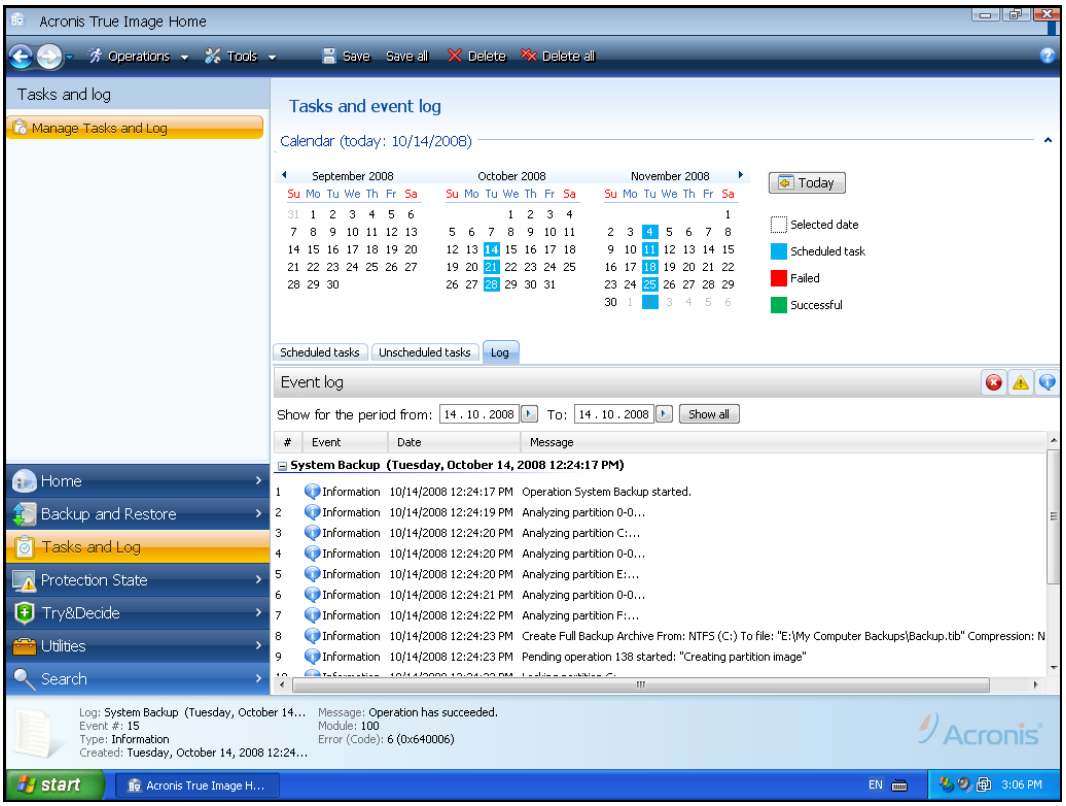
The color marks in the calendar show information about the days with scheduled tasks, tasks completed with errors, and successfully completed tasks. The current day is highlighted in bold font. Clicking a day marked with a scheduled task shows a task(s) scheduled for this date.

The buttons with the left and right arrows at the sides of the calendar allow you to browse the months being shown in the calendar. If you have gone several months back or forward, clicking the **Today** button will quickly return you to the current month and date.

Clicking any day in the past takes you to the **Log** tab and shows logs for the selected date. If there are no logs for that date, an appropriate message appears.

To view logs, you can just click on the **Log** tab.

When the **Log** tab is selected, the upper pane shows the calendar, while the lower one shows logs' contents.



To view the logs for a specific period, select the period by clicking the right arrow buttons in the **From:** and **To:** fields of the **Show for the period** area. Clicking the arrow in the **From:** field opens a pop-up calendar where you can set the start day of the period by double-clicking the appropriate day number. Then set the end day using the same procedure for the **To:** field. You can change months and years in the pop-up calendars using the left and right arrows in the month name area. In addition, you can enter the desired period start and end dates directly in the fields. If you would like to see all the logs, click the **Show all** button.

To delete a log entry, select it and click the **Delete** button on the toolbar. To delete all log entries, click the **Delete all** button. You can also save a log entry to file by clicking the **Save** button. To save all logs to file, click **Save all**.

If any step shown in logs was terminated by an error, the corresponding log will be marked with a red circle with a white cross inside.

The three buttons to the right control message filters: the white cross in the red circle filters error messages, the exclamation mark in a yellow triangle filters warnings, and the “i” in the blue circle filters information messages.

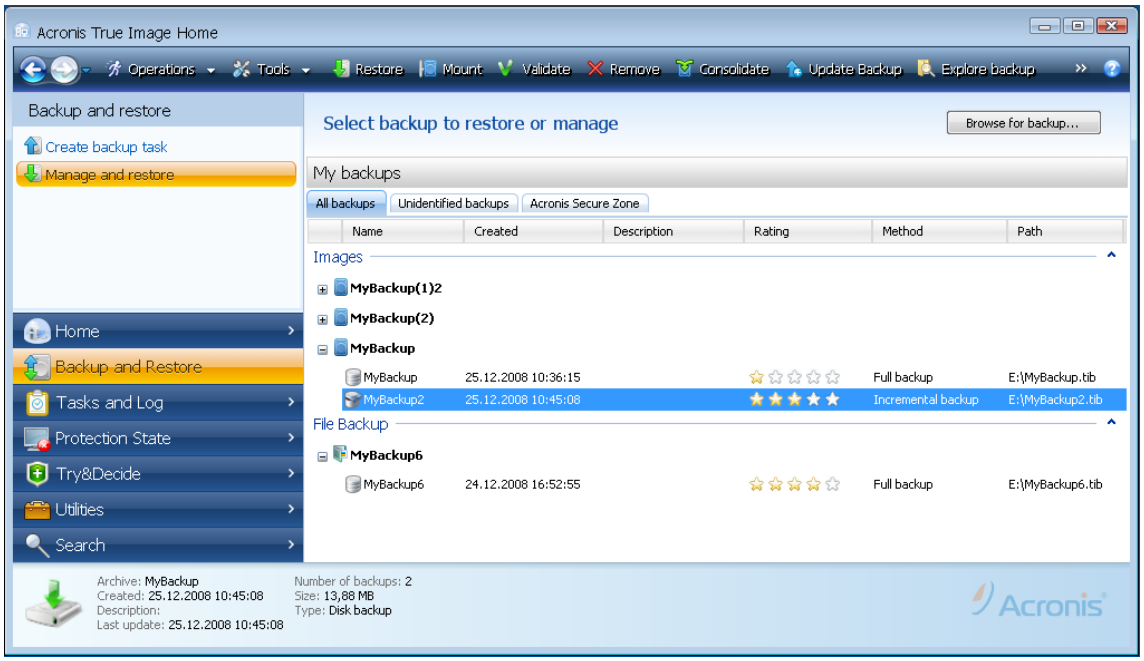
To view the details of the current step better, you can hide the calendar by clicking the **Up** arrow at the top right of the calendar pane. This will enlarge the logs area. To view the calendar again, click the **Down** arrow at the top right of the calendar pane.

Clicking a day marked with a scheduled task takes you to the **Scheduled tasks** tab with the task details shown. Clicking any day in the future also takes you to the **Scheduled tasks** tab.

11.4 Managing backup archives

After a while you may wish (or be forced) to manage your backup archives, for example, in order to free some space for new backups by removing the oldest backups or those you no longer need. Since now Acronis True Image Home stores information about the backup

archives in a metadata information database, you must manage backup archives (e.g. delete some of them) by using the program's tools and not Windows Explorer. To manage your backup archives, go to the **Manage and restore** screen by clicking **Manage and Restore** on the Welcome screen or selecting **Backup and Restore -> Manage and Restore** on the sidebar.



The toolbar on the screen provides for the following operations with backups (these operations can also be selected through a shortcut menu opened by right-clicking on a desired backup):

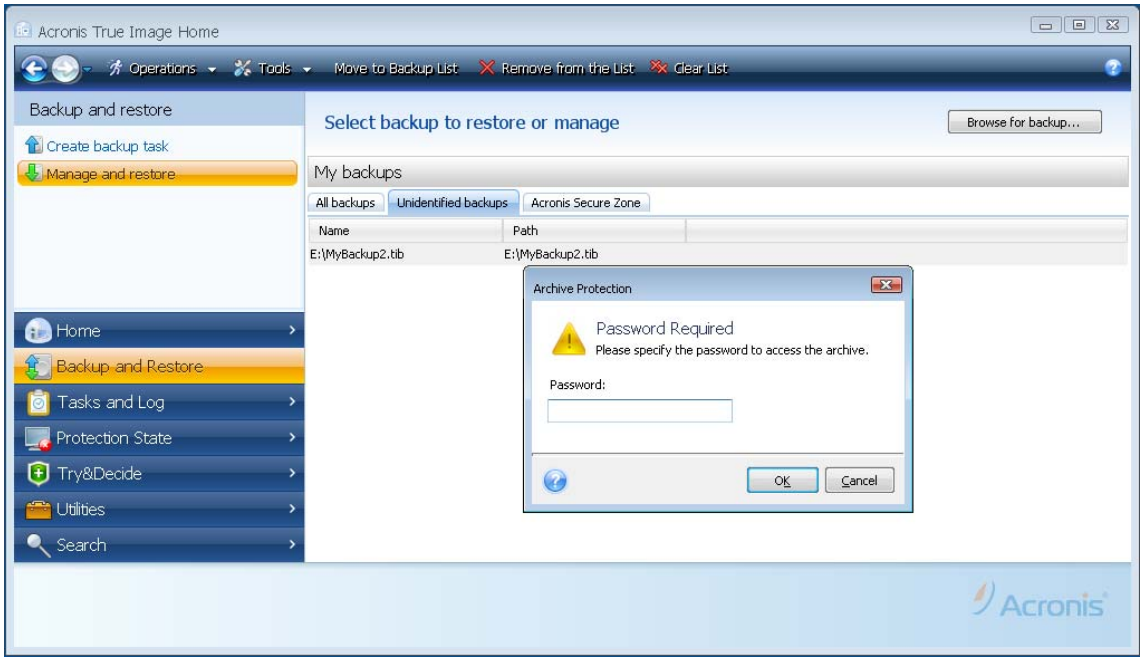
- **Restore** - see *Chapter 6. Restoring backup data*;
- **Mount** (only for the images) - *see 12.3 Mounting an image*;
- **Validate** - see *11.1 Validating backup archives*;
- **Remove** - see *11.6 Removing backup archives*;
- **Consolidate** - see *11.5 Consolidating backups*;
- **Update backup** - adding an incremental or differential backup to an existing backup archive without creating a new backup task;
- **Explore backup** - see *Chapter 12. Exploring archives and mounting images*.

Selecting the **All backups** tab allows you to manage backup archives stored on all local storage media and network resources except the Acronis Secure Zone, which has its own tab.

You cannot explore backups stored in the Acronis Secure Zone.

There is one more tab - **Unidentified backups**, which is usually empty. If you are upgrading an earlier version of Acronis True Image Home, this tab may show a list of password-protected backups created by that earlier version. During the first start the current version of the program scans all your local hard disks and if it finds any previous Acronis True Image Home backups, they are added to the database storing the metadata information about backups and to the list on the **All backups** tab. You will be able to

manage those backups as well as restore the data they contain. When scanning reveals any password-protected backup archives, Acronis True Image Home cannot determine their parameters, because earlier versions of Acronis True Image Home did not maintain a metadata information database, so it shows only their names and paths. If you know the password for a particular backup archive, click **Move to Backup List** on the toolbar. Acronis True Image Home will ask you to enter the password.



After you enter the correct password and click **OK** the program will move the backup archive to the **All backups** tab. If you do not remember the password for a backup, click **Remove from the List** on the toolbar and this backup will be removed. To remove all password-protected backups from this tab, click **Clear list**.

If you uninstall and then re-install Acronis True Image Home, your password-protected backup archives will appear on the **Unidentified backups** tab, because the metadata information database will be deleted. Updating Acronis True Image Home without uninstallation will not affect the metadata information database, so after updating this tab will remain empty.

11.5 Consolidating backups

There are two kinds of backup consolidation procedures in Acronis True Image Home: automatic consolidation and file name-based consolidation. In the case of automatic consolidation, the program uses the rules set for backup archives. After creating a backup, the program checks the backup archive for quota violations, such as exceeding a preset maximum number of gigabytes set aside for backups and, if any limitation is exceeded, consolidates the oldest backups. It will combine the first full backup with the next incremental one into one full backup which will be dated the latter backup date. Then, if necessary, this backup will be combined with the next, until the occupied storage space (or number of backups) decreases to the preset limit. Thus, the archive integrity will not be affected, despite the fact that the oldest backups will be deleted.

The actual number of backups created can exceed the **Maximum number of backups** by one. This enables the program to detect the fact of exceeding the number quota and start consolidation. Backup will be prohibited until the consolidation finishes.

The file name-based consolidation allows deleting the backups that you do not need anymore from any archive while maintaining the archive consistency. You can delete from an archive, if need be, the base full backup. The program will create another full backup in place of the oldest remaining backup. The two kinds of backup procedures have the following difference:

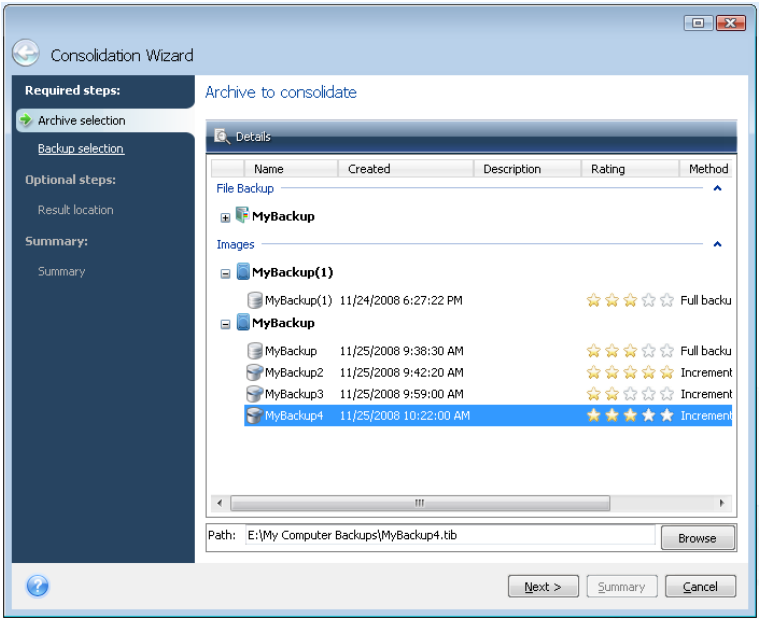
Automatic consolidation only can consolidate two backups in one. File name-based consolidation keeps whichever backups you choose and deletes any backups that are not selected.

The current Acronis True Image Home version does not support consolidation of backup archives created in the zip format.

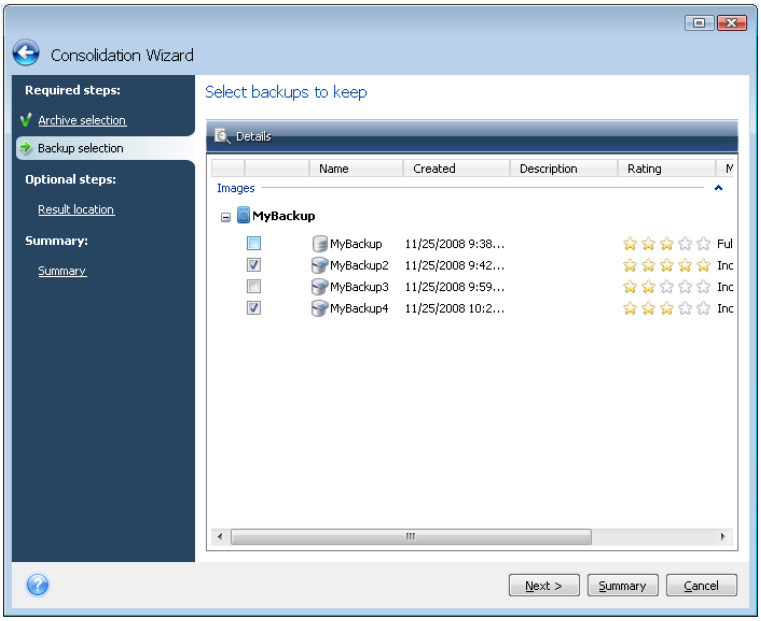
To consolidate backups in an archive:

1. Launch the **Backup Consolidation Wizard** by choosing **Operations -> Consolidate Archive** in the main program menu or select **Backup and Restore -> Manage and Restore** on the sidebar and then click **Consolidate**.

2. Select the archive for consolidation.

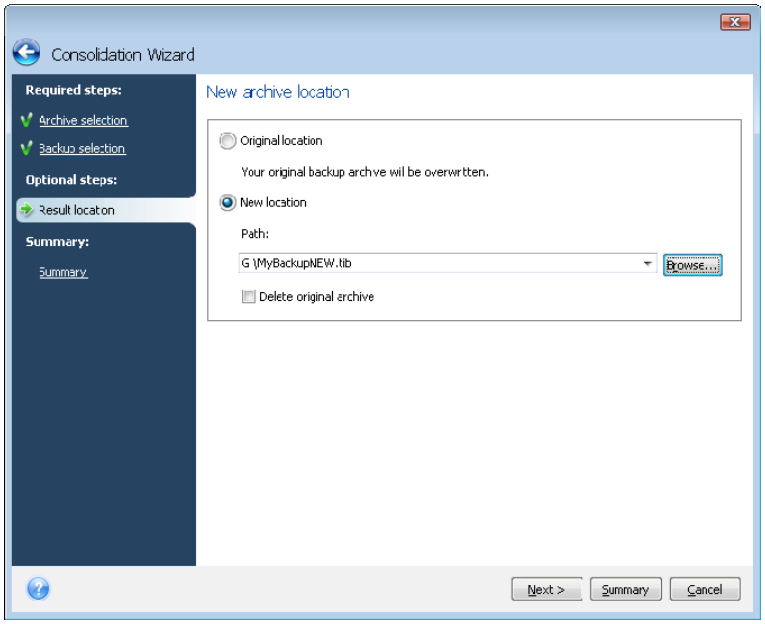


3. The program displays a list of backups belonging to the selected archive with their creation date and time. The upper backup is the full backup; the rest are incremental backups. Select the backups you want to *keep*.



4. Choose the location and name for the archive copy. By default, the program suggests the same location and the original backup archive will be overwritten. But you can choose a new location and in such a case the source archive will stay as is, unless you choose to delete it by selecting the **Delete original archive** box. This requires more disk space, but ensures security of the archive in case the consolidation fails because of power failure or lack of disk space.

You cannot choose another location when consolidating backups in an archive located in the Acronis Secure Zone.

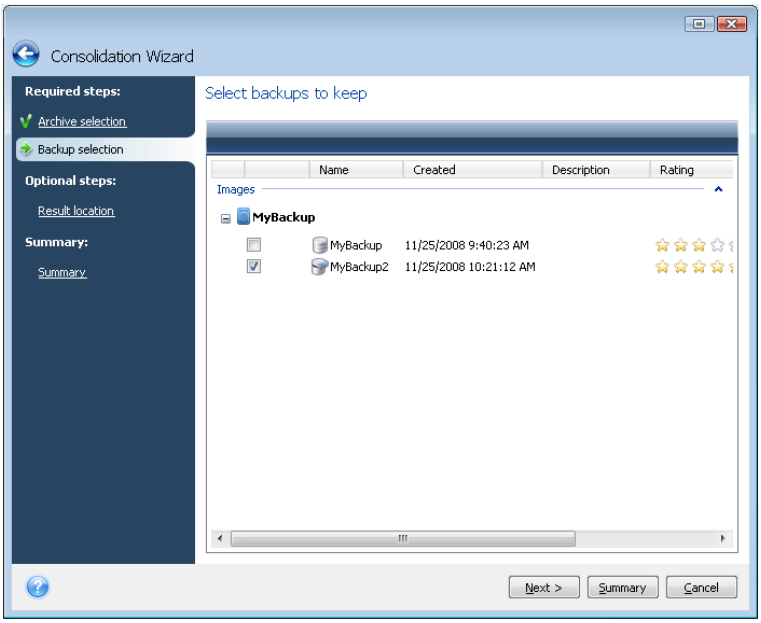


5. The program displays the summary window. Click **Proceed** to start consolidation.

In our example, when consolidation is complete, disk G will contain two new archives MyBackup and MyBackup2.

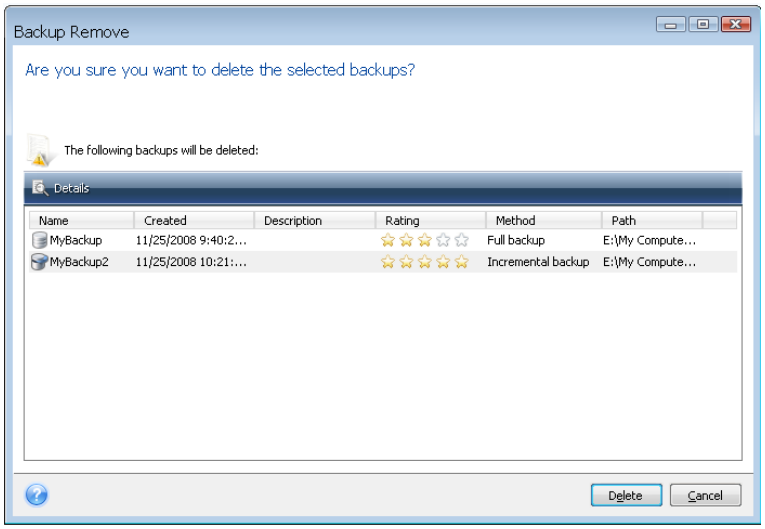
MyBackup is a full backup containing data as of November 25, 2008, 9:40:23 AM. MyBackup2 is an incremental backup containing data as of November 25, 2008, 10:21:12

AM. You can make sure of this by starting the consolidation wizard again, selecting the archive MyBackup and proceeding to the next window.



11.6 Removing backup archives

You may want to remove backups and backup archives you no longer need. Because Acronis True Image Home stores information on the backup archives in a metadata information database, deleting unneeded archive files using Windows Explorer will not delete information about these archives from the database and Acronis True Image Home will consider that they still exist. This will result in errors when the program tries to perform operations on the backups that no longer exist. So you must only remove obsolete backups and backup archives using the tool provided by Acronis True Image Home. To remove the entire backup archive, select it and click **Remove** on the toolbar or right-click on the full backup of the backup archive and choose **Remove** in the shortcut menu. To remove an incremental or a differential backup, select it and click **Remove** on the toolbar or right-click on the selected backup and choose **Remove** in the shortcut menu. In this case all other successive incremental and differential backups created later than the selected incremental or differential backup will be also deleted. The following screen appears:



If you click **Delete**, the program will remove the backup archive from its metadata information database as well as from the hard disk.

Chapter 12. Exploring archives and mounting images

Acronis True Image Home offers two kinds of archive contents management: mounting for images and exploring for both images and file-level archives.

Exploring images and file-level archives lets you view their contents and copy the selected files to a hard disk. To explore a backup archive, double-click on the corresponding tib file. You can also right-click on the file and choose **Explore** in the shortcut menu.

Mounting images as virtual drives lets you access them as though they were physical drives. Such an ability means that:

- a new disk with its own letter will appear in the drives list
- using Windows Explorer and other file managers, you can view the image contents as if they were located on a physical disk or partition
- you will be able to use the virtual disk in the same way as the real one: open, save, copy, move, create, delete files or folders. If necessary, the image can be mounted in read-only mode.

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

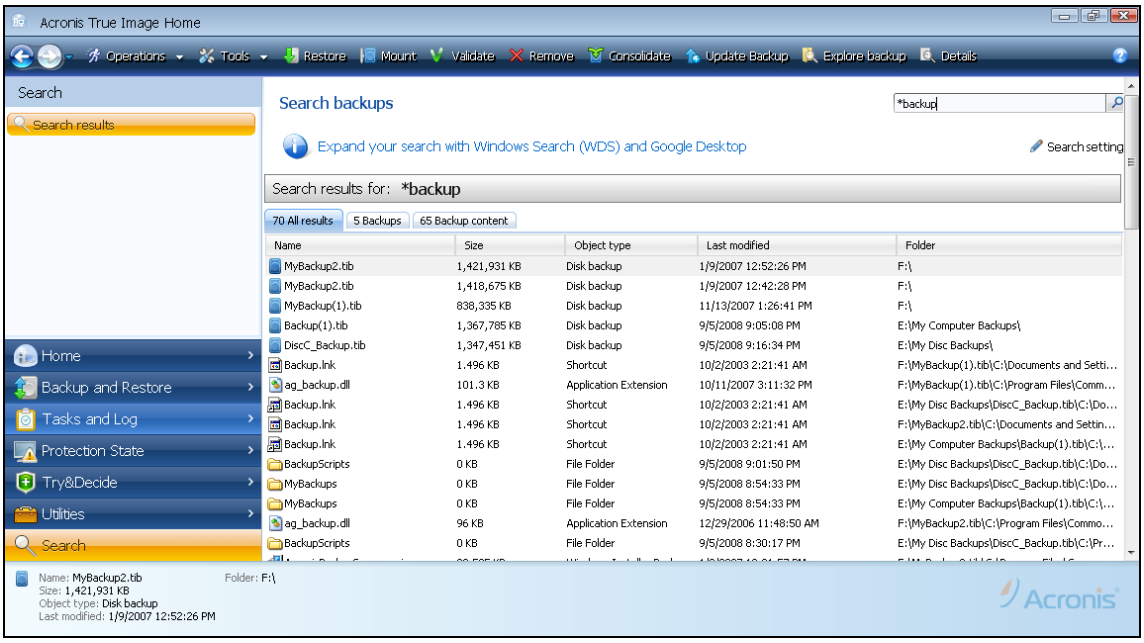
Please keep in mind that, though both file archives and disk/partition images have a default ".tib" extension, only **images** can be mounted. If you want to view file archive contents, use the Explore operation. The following is a brief summary of the Explore vs Mount operation:

	Explore	**Mount**
Archive type	File-level, disk or partition image	Partition image
Assigning a letter	No	Yes
Archive modification	No	Yes (in R/W mode)
Files extraction	Yes	Yes

12.1 Searching

In addition to the ability to explore backup archives, Acronis True Image Home now provides search for tib and zip archives themselves, for files in tib archives only, as well as offering full-text search in help topics and in the comments to archives made during the archive's creation. This facilitates searching of the information you need for using Acronis True Image Home and for restoring files from your backup archives. Here's how you can search the data you need.

1. Enter a search string into the Search field at the top right of the Acronis True Image Home window and then click the magnifying glass icon. You will be taken to the **Search Results** window. The search results are output in the corresponding tabs of the window and all search results are shown on the **All results** tab.



2. By default the search is performed in all the sources where Acronis True Image Home can search information. You can select an information source of interest by choosing the appropriate tab among **Backups** and **Backup content**.

- The **Backups** tab shows the results of the search for tib and zip archives by archive filename. Double-clicking on a filename opens the corresponding archive in Windows Explorer where you can explore the archive contents. You can validate or restore the archive by right-clicking on its filename and choosing the appropriate item in the shortcut menu. In addition, you can use the **Restore**, **Mount** (for image backups), **Validate**, **Remove**, and **Consolidate** buttons for tib archives, and **Restore**, **Validate**, and **Remove** buttons for zip archives, that appear on the toolbar after selecting an archive on the **Backups** tab.
- The **Backup content** tab shows results of searches for files and folders in tib archives. Double-clicking on a filename opens the file. You can restore the file by right-clicking on its filename and choosing Restore in the shortcut menu. This shortcut menu also enables you to open the file or the parent folder that contains that file.

To help you better understand the search results, here is some information on the algorithms used by the Search feature.

1. When searching files in tib archives you can type all or part of the filename and use the common Windows wildcard characters. For example, to find all batch files in the archives, type "*.bat". Typing my???.exe will allow you to find all .exe files with names consisting of five symbols and starting with "my". By the way, search is case-insensitive, i.e. "Backup" and "backup" is the same search string. Furthermore, the search stops after the program finds 100 files corresponding to a search criterion you have typed. If the search results do not contain the file you need, you will have to refine the search criterion.

Please note that Acronis True Image Home does not search files in encrypted and password-protected tib archives as well as in the password protected Acronis Secure Zone. In addition, the program does not search files in zip backup archives created by Acronis True Image Home.

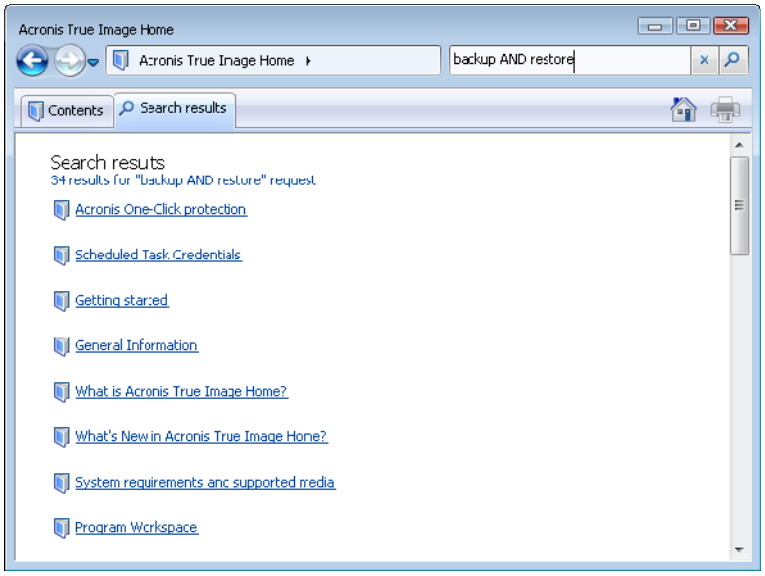
When a file is included in several backups and it has not been modified, the search results will show it only once in the oldest backup file. If such a file has been changed, the search results will show all backup files containing *differing* versions of the file.

2. Search in the Help topics and comments to backup archives is carried out differently. First of all, you cannot use "*" and "?" as Windows wildcard characters. As in this case the program uses full text search, it will just find all occurrences of these characters in the Help topics (if any). The full text search uses the following rules:

- Search criteria consist of words separated by space character(s) or by a logical operator: "AND", "OR", "NOT" (please, take note of the upper case).
- Only one logical operator is allowed (the first one that occurs in a search string), otherwise they are ignored and interpreted as search words.
- All space-separated words must be in a topic for successful match.

The **Backups** tab (as well as the **All results** tab) shows the archive files whose comments satisfy the search criterion. Double-clicking on an archive opens it for exploring.

Search in the Help topics is performed after opening the **Help** by pressing the **F1** key or clicking the help icon in any Acronis True Image Home window and entering a search string in the Search field. Clicking on a found help topic title opens the corresponding Help topic.



12.2 Google Desktop and Windows Search integration

Acronis True Image Home has plug-ins for Google Desktop and Windows Search (WDS). If you use any of these search engines on your computer, then during the first start after installation Acronis True Image Home will detect the search engine you use and will install an appropriate plug-in for indexing your tib backup archives. Indexing of backups will speed up searches in the backup archives. After such indexing you will be able to search archives content by entering a file name into the Google Desktop or Windows Search deskbar query field without opening Acronis True Image Home. The search results will be shown in a browser window. Using the search results you can:

- Select any file and open it for viewing and/or save that file back to the file system anywhere (not in the archive) or where it was before
- See in which archive a given file is stored and restore that archive

Google Desktop has a "Quick Find" window. This window is filled with the most relevant results from your computer. The results change as you type, so you can quickly get to what you want on your computer. Windows Search provides similar functionality.

In addition to indexing the files in backup archives by their names, the Google Desktop and Windows Search provide Acronis True Image Home with the ability to perform full-text indexing of many files in tib archives, so you will be able to use this feature and perform searches of the files' content.

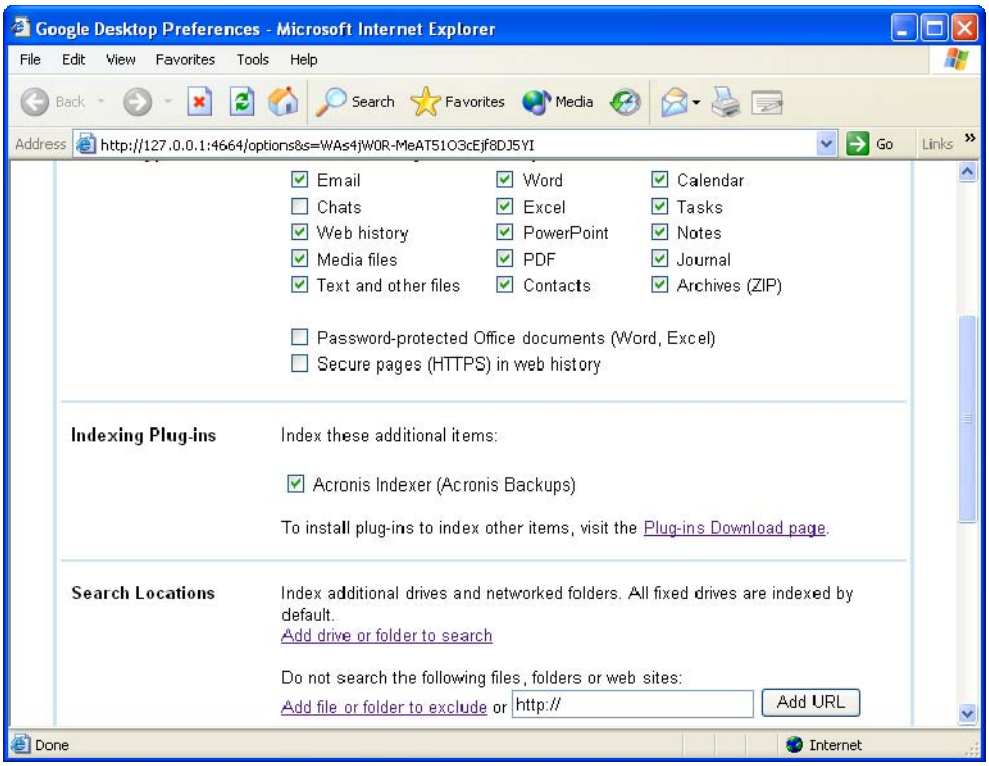
Full-text indexing of files in backup archives is provided only for the file types recognizable by Google Desktop and Windows Search. They recognize text files, Microsoft Office files, all Microsoft Office Outlook, and Microsoft Outlook Express items, and more.

The contents of password-protected tib backup archives or archives protected by a password and encryption, as well as the System State and My E-mail backup archives will not be indexed, though Google Desktop and Windows Search provide search for the tib files themselves and in the comments to such archives. Furthermore, Google Desktop and Windows Search have no access to the Acronis Secure Zone, so these search engines will be unable to search and index archives in the zone.

Suppose you have Google Desktop installed and want to use it for searching files in tib archives. To get such an ability:

1. During the first start of Acronis True Image Home, Google Desktop will display a confirmation window. Click **OK** to install the plug-in.

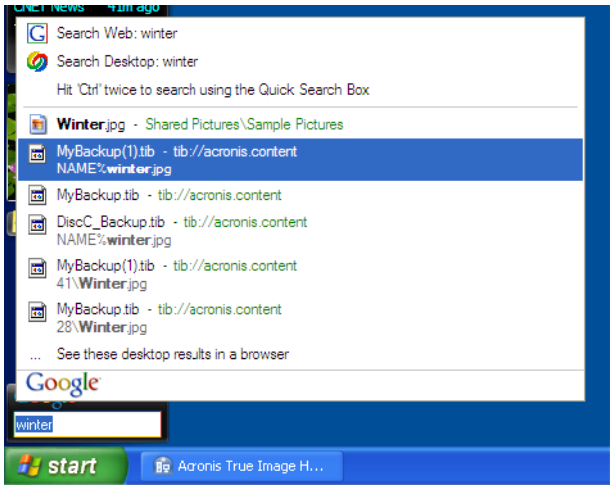
2. Verify that the plug-in is installed. Right-click on the Google Desktop icon in your system tray and select **Options** in the context menu. Google Desktop opens the **Preferences** window in your browser. Make sure that **Acronis Indexer (Acronis Backups)** is selected in the **Indexing Plug-ins** area.



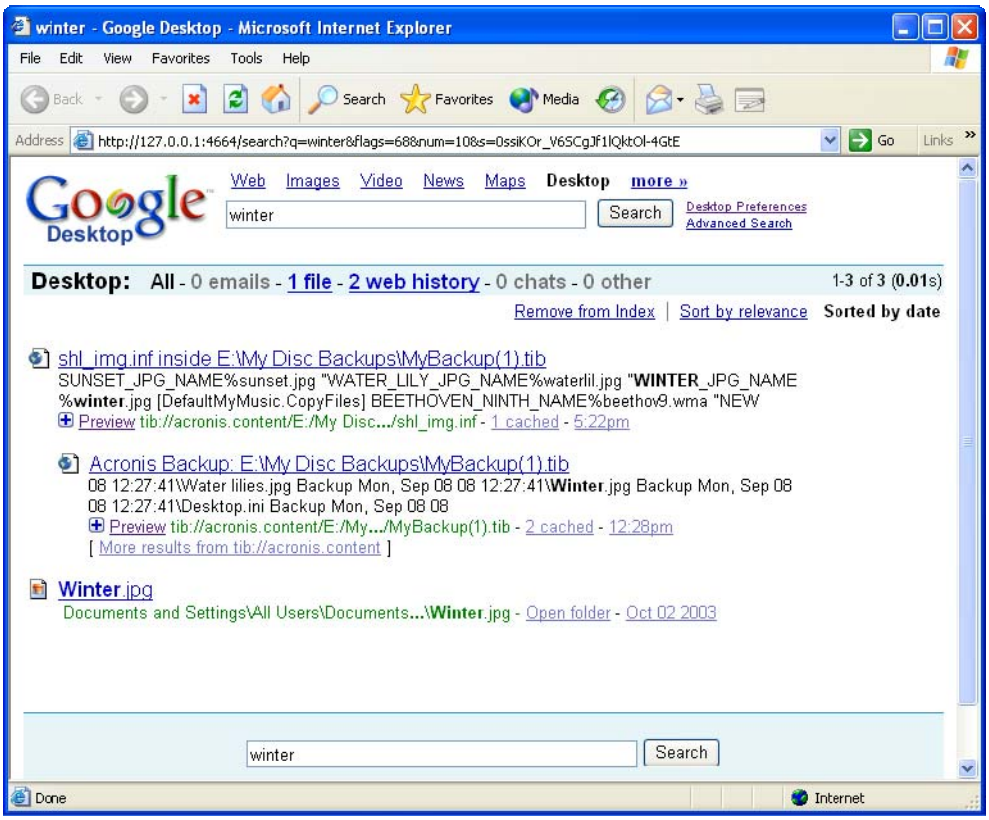
3. Right-click on the Google Desktop icon in your system tray once more and select **Indexing -> Re-Index**. Click **Yes** in the confirmation window that appears. Google Desktop will add all the new content to the existing index.

Give Google Desktop some time for indexing all tib files on your computer's hard disks and adding the indexing information to its index database. The required time depends on the number of tib archives and the number of files they contain.

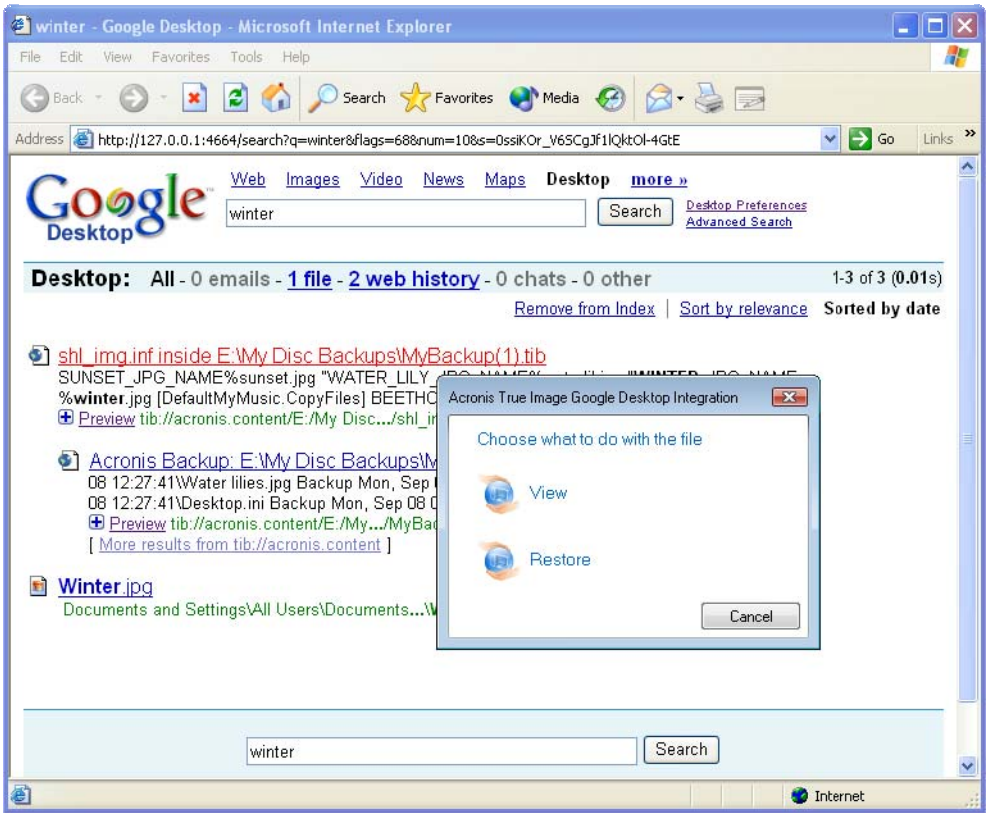
After, for example an hour, check whether Google Desktop has indexed the tib archives by entering in its query field the name of a file which you know for sure that you backed up. If Google Desktop has completed indexing, it will show you the tib archives where it has found the file.



If you want to see all the search results, click the "See all N results in a browser" and you will see something like the screen shot below.



Clicking in the browser window on a line related to the desired file version opens a small dialog with just two options: **View** and **Restore**.



Choosing **View** starts the application associated with this file type and opens the file. Choosing **Restore** starts Acronis True Image Home and you can then restore the file to a desired location.

Google Desktop also provides for searching files in zip backup archives, created by Acronis True Image Home, though you cannot open or restore files from zip archives by clicking on a line with a filename in the browser window. To restore files found in zip backup archives by Google Desktop, use Acronis True Image Home's Restore feature.

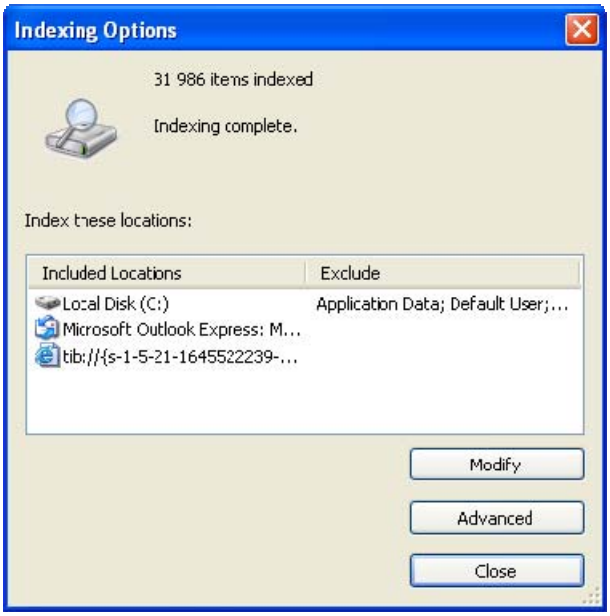
The following information may be of interest to you if you use any edition of Windows Vista that has built-in Desktop Search functionality or Windows Desktop Search 3.0 or later and wish to enable Windows Search support for tib files.

Windows Search does not support indexing of zip files content.

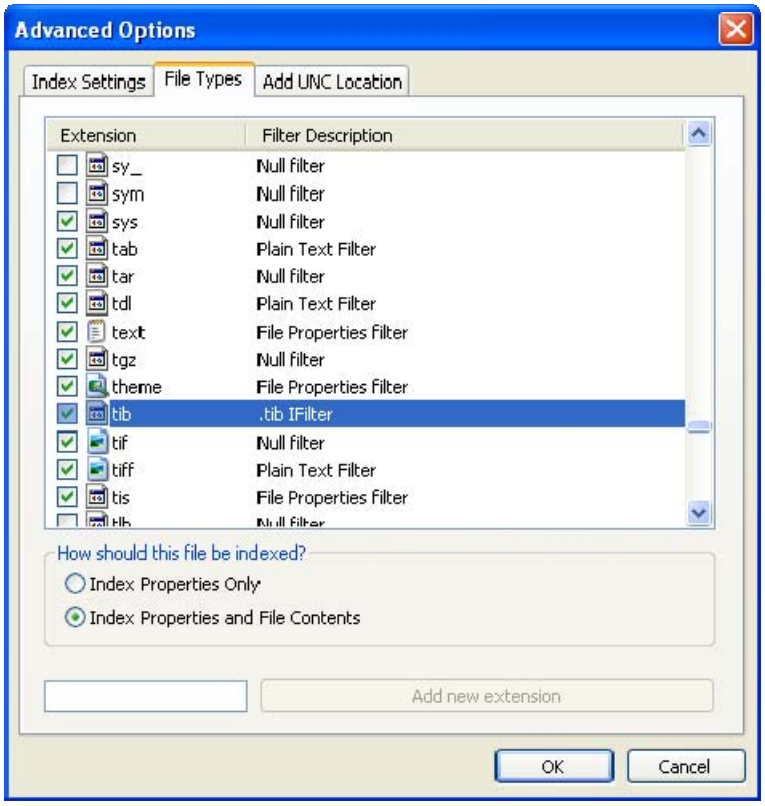
To use Windows Search support:

1. Verify that the tib support is enabled. Right-click on the Windows Search icon in your system tray and select **Windows Search Options...** in the context menu. The following window appears. Make sure that the "tib:///" item is present in the Included Locations list.

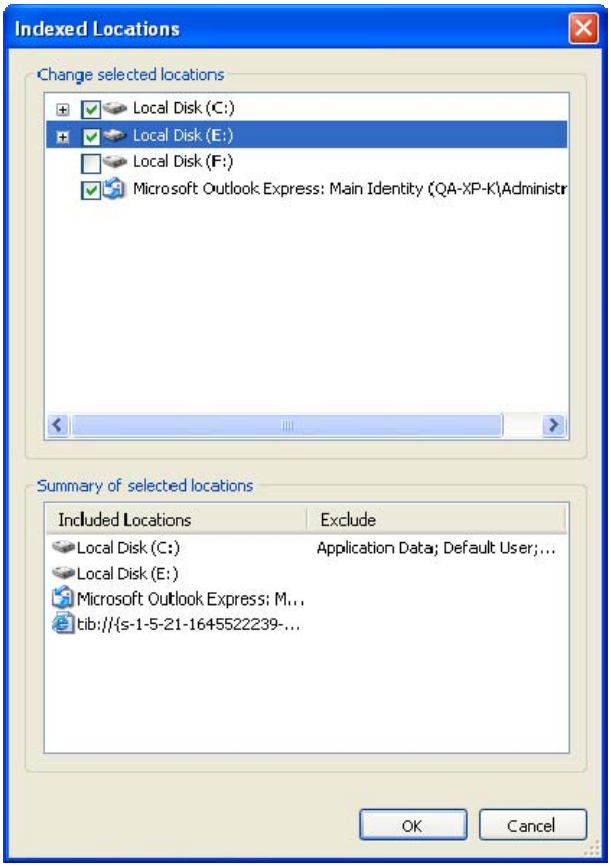
To open the Indexing Options window in Windows Vista, open the Control Panel and then double-click the **Indexing Options** icon. The Windows Vista indexing options have some differences in content and appearance, though most of the following information is applicable to Windows Vista as well.



2. Click **Advanced**, select the **File Types** tab and then make sure that the **tib** extension is selected and ".tib IFilter" is shown in the Filter Description field. **Select Index Properties and File Contents**.

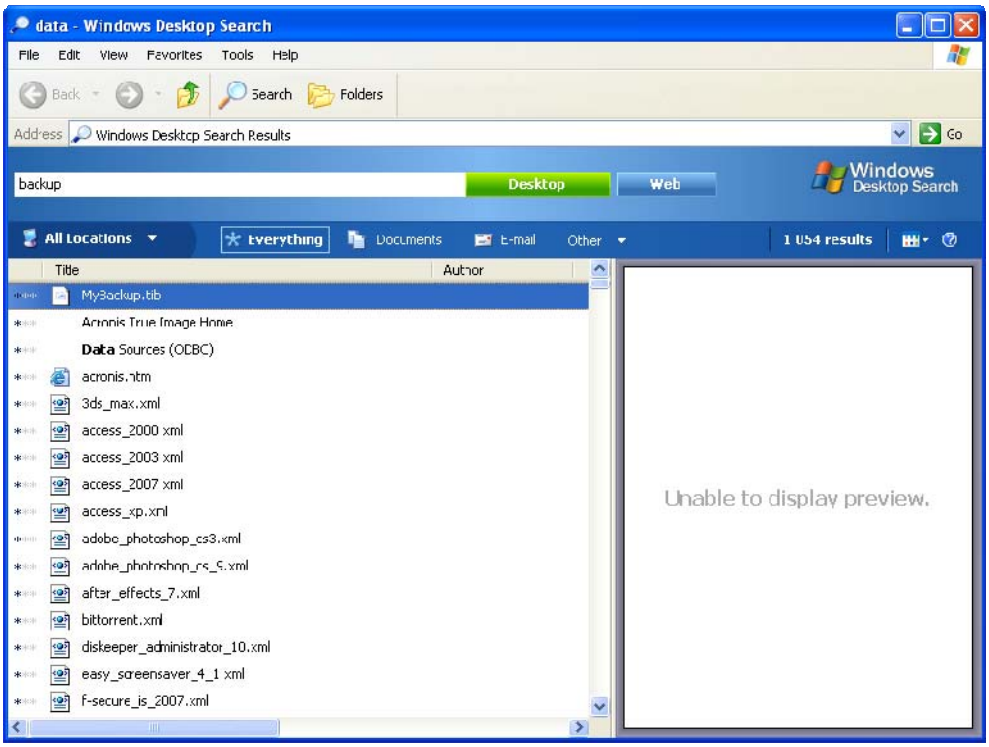


3. Click **OK** and while the **Indexing Options** window is open, check that the disks where you store your tib backup archives are shown in the "Included Locations" list. If the list does not contain those disks, the tib files will not be indexed. To include the disks, click **Modify** and select them in the window that appears.

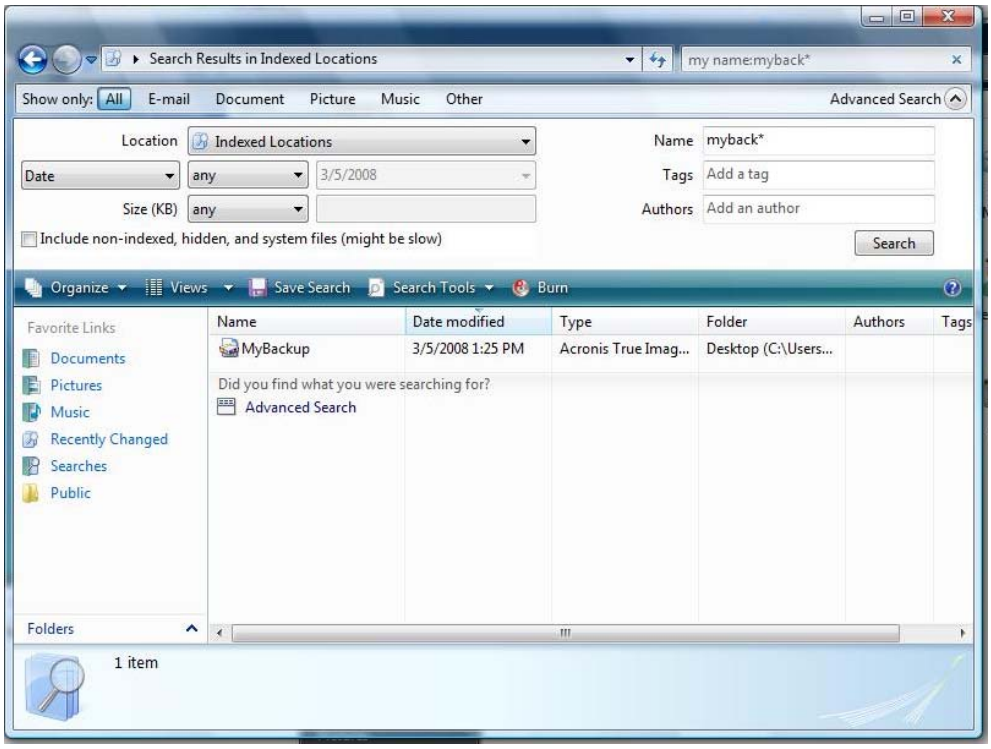


If you store backups on a network share, Windows Search can index them too. You just have to add the share to the Indexed Locations list by typing the appropriate UNC path after selecting the **Add UNC Location** tab of **Advanced Options**.

Give Windows Search some time for indexing all tib files on your computer's hard disks and adding the indexing information to its index database. The required time depends on the number of tib archives and the number of files they contain. After completing the indexing, the Desktop Search will be able to search files in tib backup archives. The search engines in WDS and Windows Vista have similar functionalities, though search results are presented somewhat differently:



Windows Search results



Windows Vista search results

12.3 Mounting an image

1. Start the **Mount Wizard** by selecting **Operations -> Mount Image** in the main program menu or by right-clicking on an image archive and selecting **Mount** in the Windows Explorer shortcut menu.

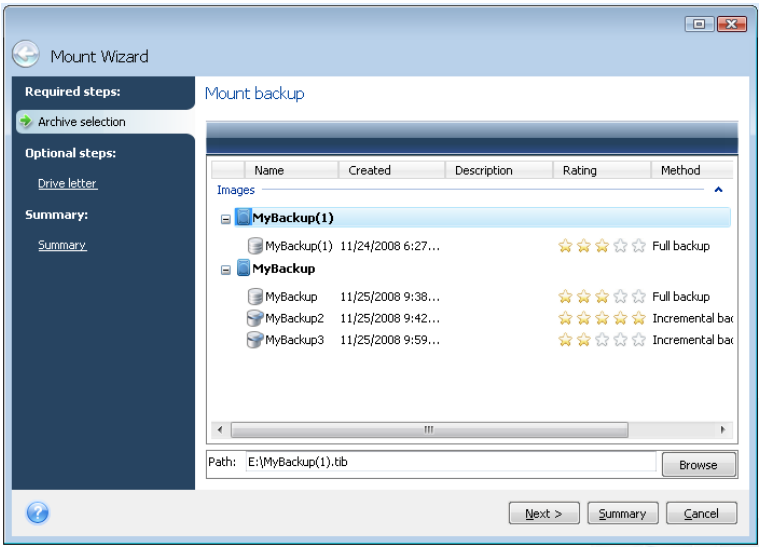
2. Select the archive for mounting.

If you selected an archive containing incremental images, you can select one of the successive incremental images (also called "slices") by its creation date/time. Thus, you can explore the data state at a certain moment.

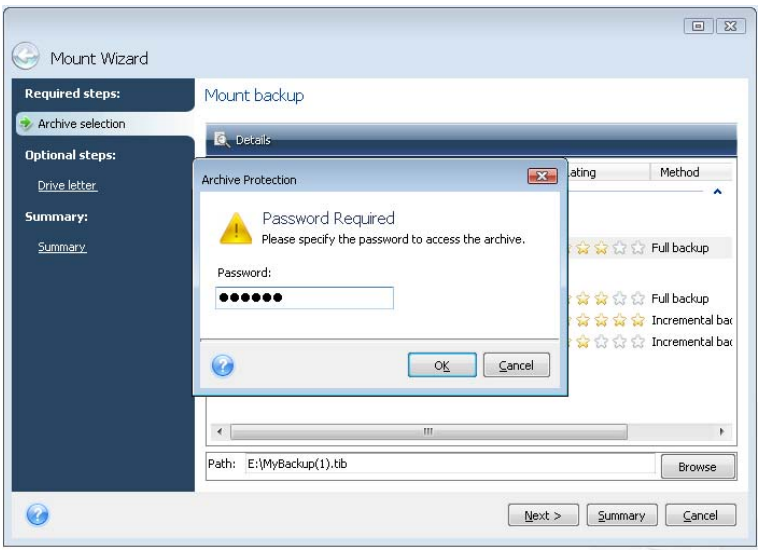
To mount an incremental image, you must have all previous images and the initial full image. If any of the successive images are missing, mounting is not possible. By default the program will mount the latest incremental image.

To mount a differential image, you must have the initial full image as well.

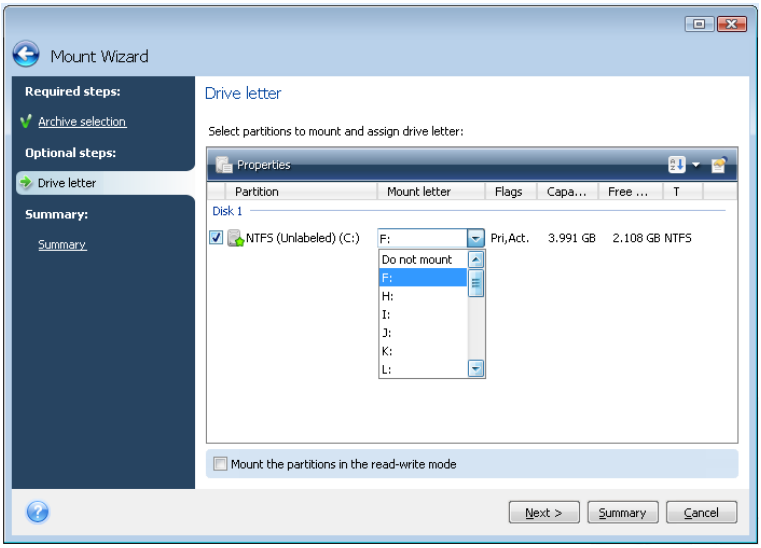
3. Select a partition to mount as a virtual disk. (Note that you cannot mount an image of the entire disk except in the case when the disk consists of one partition.)



If you added a comment to the archive, it will be displayed in the Description column. If the archive was protected with a password, Acronis True Image Home will ask for the password in a dialog box. Neither the partitions layout will be shown, nor will the **Next** button be enabled until you enter the correct password.

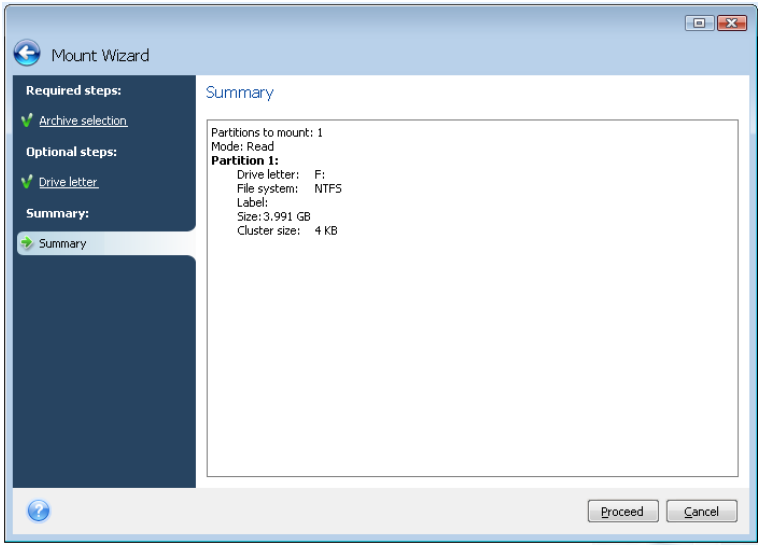


You can also select a letter to be assigned to the virtual disk from the **Mount letter** drop-down list. If you do not want to mount the virtual drive, select **Do not mount** in the list.



4. If you select the **Mount the partitions in the read-write mode** box, the program assumes that the mounted image will be modified and creates an incremental archive file to capture the changes. It is strongly recommended that you list the forthcoming changes in the Comments section to this file. For you to be able to make comments, the optional **Comments** step appears in the wizard.

5. The program displays a summary containing a single operation. Click **Proceed** to connect the selected partition image as a virtual disk.



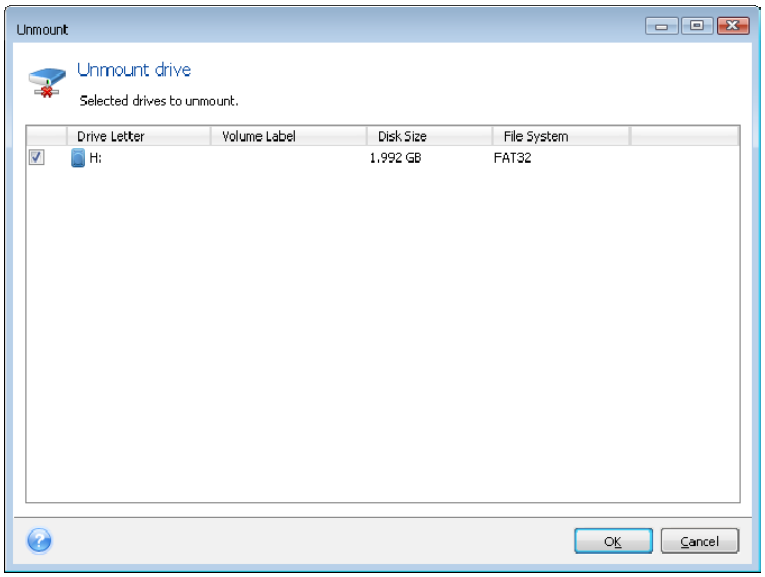
6. After the image is connected, the program will run Windows Explorer, showing its contents. Now you can work with files or folders as if they were located on a real disk.

You can connect multiple partition images. If you want to connect another partition image, repeat the procedure.

12.4 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. If you do not unmount the disk, it will disappear after your computer is turned off.

To disconnect the virtual disk, choose **Operations -> Unmount Image**, select the disk to unmount and click **OK**.



You can also do this in Windows Explorer by right-clicking on the disk icon and choosing **Unmount**.

Chapter 13. Transferring the system to a new disk

13.1 General information

Sooner or later, most computer users find that their hard disk is too small. If you just don't have space for more data, you can add another disk just for data storage as described in the following chapter.

However, you might find that your hard disk does not have enough space for the operating system and installed applications, preventing you from updating your software or installing new applications. In this case, you have to transfer the system to a higher-capacity hard disk.

To transfer the system, you must first install the disk in the computer (see details in the *Appendix B. Hard disks and BIOS setup*). If your computer doesn't have a bay for another hard disk, you can temporarily install it in place of your CD drive or use a USB 2.0 connection to the external target disk. If that is not possible, you can clone a hard disk by creating a disk image and restoring it to a new hard disk with larger partitions.

There are two transfer modes available: automatic and manual.

In the automatic mode, you will only have to take a few simple actions to transfer all the data, including partitions, folders and files, to a new disk, making it bootable if the original disk was bootable.

There will be only one difference between these disks – partitions on the newer disk will be larger. Everything else, including the installed operating systems, data, disk labels, settings, software and everything else on the disk, will remain the same.

This is the only result available in the automatic mode. The program can only duplicate the original disk layout to the new one. To obtain a different result, you will have to answer additional questions about cloning parameters.

The manual mode will provide more data transfer flexibility.

1. You will be able to select the method of partition and data transfer:

- as is
- new disk space is proportionally distributed between the old disk partitions
- new disk space is distributed manually

2. You will also be able to select operations to perform on the old disk:

- leave partitions (and data!) on the old disk
- remove all information from the old disk
- create new partitions on the old disk (and remove all the old information)

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 using the appropriate operating system tools.

13.2 Security

Please note the following: if the power goes out or you accidentally press **RESET** during the transfer, the procedure will be incomplete and you will have to partition and format or clone the hard disk again.

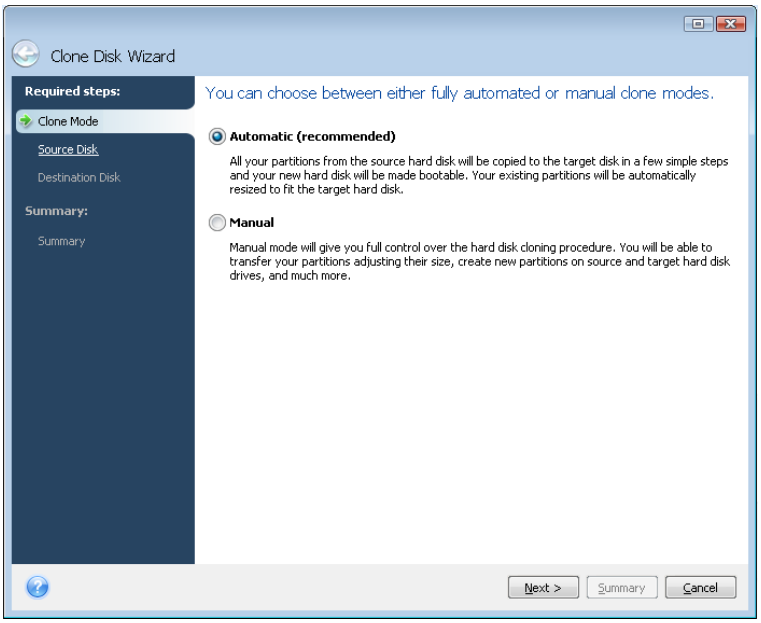
No data will be lost because the original disk is only being read (no partitions are changed or resized).

Nevertheless, we do not recommend that you delete data from the old disk until you are sure it is correctly transferred to the new disk, the computer boots up from it and all applications work.

13.3 Executing transfers

13.3.1 Selecting Clone mode

You will see the **Clone Mode** window just after the welcome window.

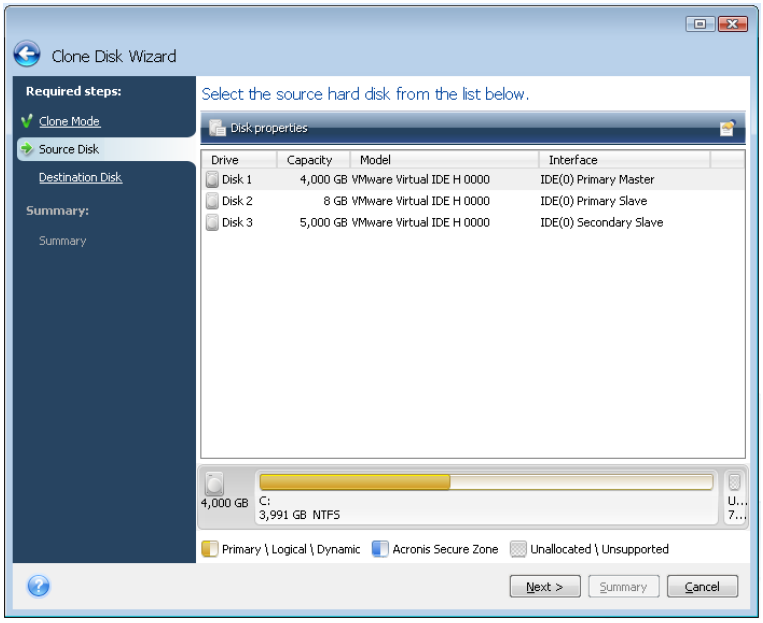


We recommend using automatic mode in most cases. The manual mode can be useful if you need to change the disk partition layout.

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 a case, the next steps will be bypassed and you will be taken to the cloning Summary screen.

13.3.2 Selecting source disk

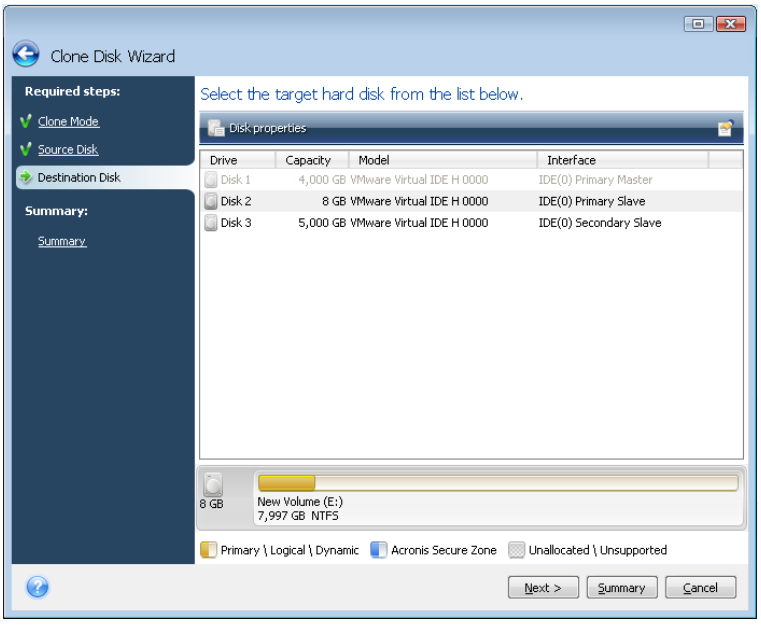
If the program finds several partitioned disks, it will ask you which one is the source (i.e. the older data disk).



You can determine the source and destination using the information provided in this window (disk number, capacity, label, partition, and file system information).

13.3.3 Selecting destination disk

After you select the source disk, you have to select the destination where the disk information will be copied.

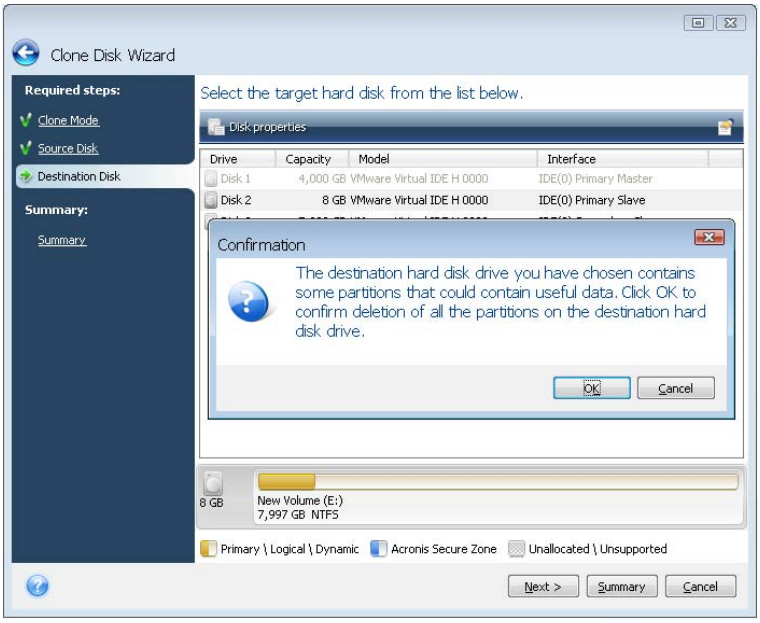


The previously selected source becomes grayed-out and disabled for selection.

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

13.3.4 Partitioned destination disk

At this point, the program checks to see if the destination disk is free. If not, you will be prompted by the Conformation window stating that the destination disk contains partitions, perhaps with useful data.



To confirm deletion of the partitions, click **OK**.

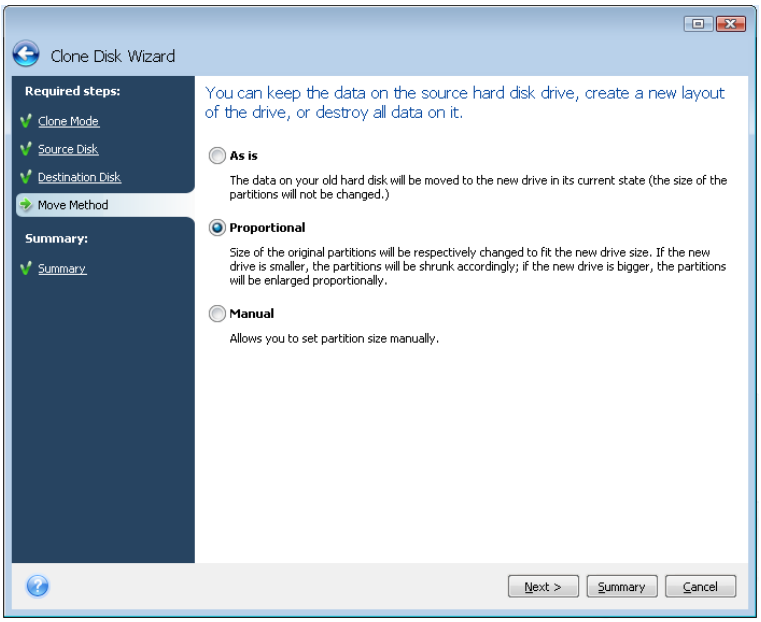
Note that no real changes or data destruction will be performed at this time! For now, the program will just map out cloning. All changes will be implemented only when you click **Proceed.**

If you selected the automatic mode, the program will not ask you anything else and will take you to the cloning summary window.

13.3.5 Selecting partition transfer method

When you select the manual cloning mode, Acronis True Image Home will offer you the following data move methods:

- **As is**
- **Proportional** – the new disk space will be proportionally distributed among cloned partitions
- **Manual** – you will specify the new size and other parameters yourself



If you elect to transfer information "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. Afterwards, you will be able to use the unallocated space to create new partitions or to enlarge the existing partitions with special tools, such as Acronis Disk Director Suite.

As a rule, "as is" transfers are not recommended as they leave a lot of unallocated space on the new disk. Using the "as is" method, Acronis True Image Home transfers unsupported and damaged file systems.

If you transfer data proportionally, each partition will be enlarged, according to the proportion of the old and new disk capacities.

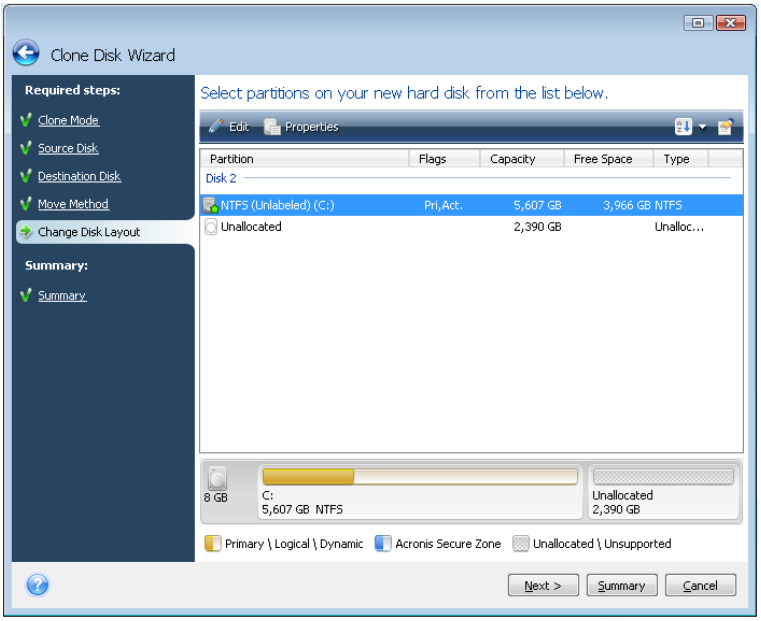
FAT16 partitions are enlarged less than others, as they have a 4GB size limit.

Depending on the selected combination, you will proceed to either the cloning summary window, or the Change disk layout step (see below).

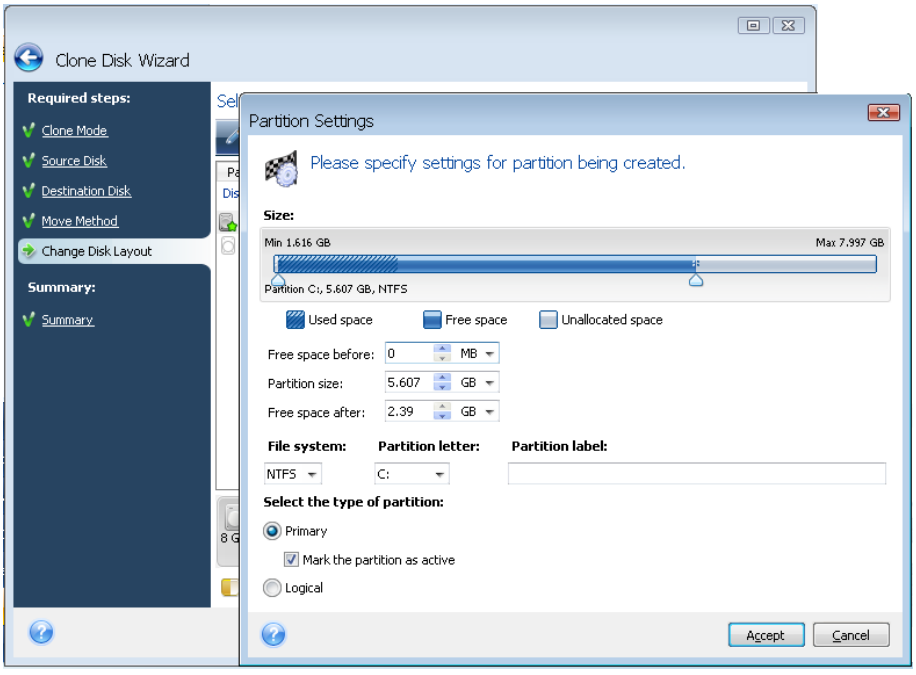
13.3.6 Cloning with manual partitioning

The manual transfer method enables you to resize partitions on the new disk. By default, the program resizes them proportionally. In the next window, you will see the new disk layout.

Along with the hard disk number, you will see disk capacity, label, partition, and file system information. Different partition types, including primary, logical, and unallocated space are marked with different colors.



First, select a partition to resize and click **Edit** on the toolbar. This will open the Partition Settings window, where you can resize and relocate the partition.



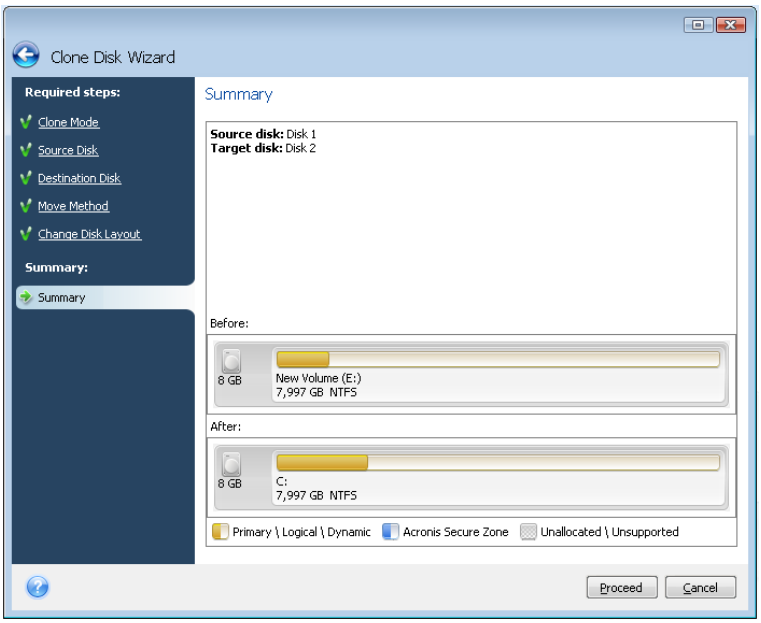
You can do this by entering values in the **Free space before, Partition size, Free space after** fields, by dragging partition borders or the partition itself.

If the cursor turns into two vertical lines with left and right arrows, it is pointed at the partition border and you can drag it to enlarge or reduce the partition's size. If the cursor turns into four arrows, it is pointed at the partition, so you can move it to the left or right (if there's unallocated space near it).

Having provided the new location and size, click **Accept**. You will be taken back to the Change disk layout window. You might have to perform some more resizing and relocation before you get the layout you need.

13.3.7 Cloning summary

The cloning summary window graphically (as rectangles) illustrates information about the source disk (partitions and unallocated space) and the destination disk layout. Along with the disk number, some additional information is provided: disk capacity, label, partition and file system information. Partition types — primary, logical and unallocated space — are marked with different colors.



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. After the clone process finishes you will be offered an option to shut down the computer by pressing any key. This enables you to change the position of master/slave jumpers and remove one of the hard drives.

Cloning a non-system disk or a disk containing an operating system, but one that is not currently active, will proceed without the need to reboot. After you click **Proceed**, Acronis True Image Home will start cloning the old disk to the new disk, indicating the progress in a special window. You can stop this procedure by clicking **Cancel**. In that case, you will have to repartition and format the new disk or repeat the cloning procedure. After the cloning operation is complete, you will see the results message.

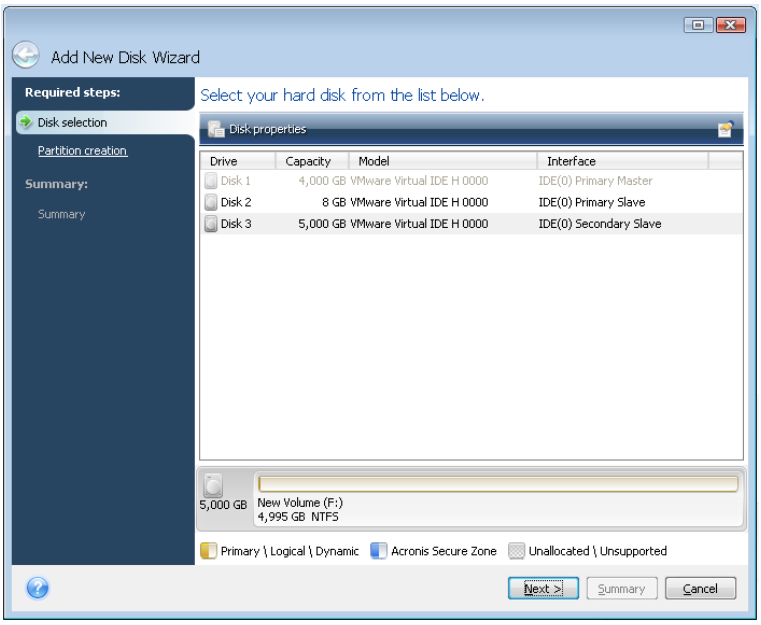
Chapter 14. Adding a new hard disk

If you don't have enough space for your data, you can either replace the old disk with a new higher-capacity one (data transfers to new disks are described in the previous chapter), or add a new disk only to store data, leaving the system on the old disk. If the computer has a bay for another disk, it would be easier to add a data disk drive than to clone a system drive.

To add a new disk, you must first install it in your computer.

14.1 Selecting a hard disk

Select the disk that you've added to the computer.



If there are any partitions on the new disk, you will be shown a warning window. For you to be able to add the disk, they must be deleted first, so click **OK** to continue.

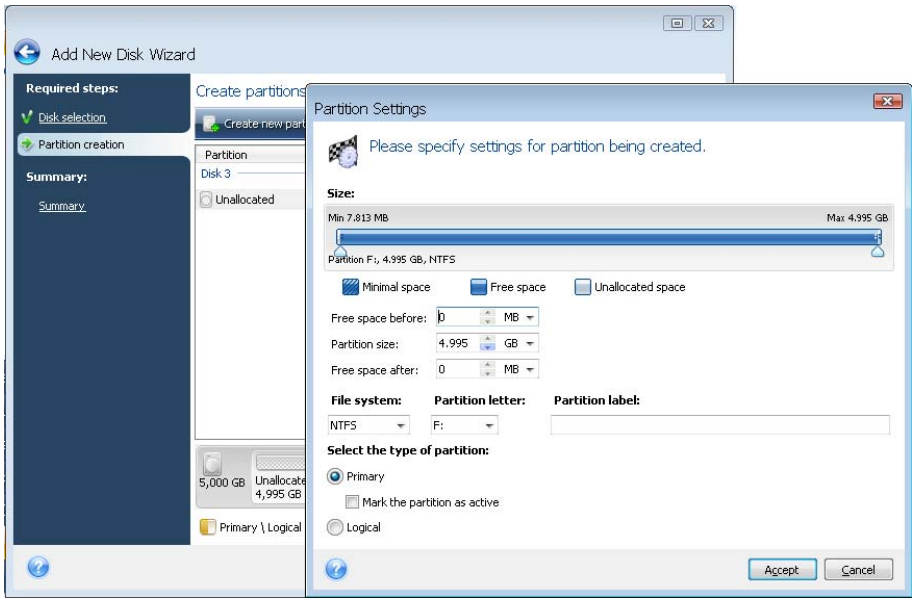
14.2 Creating new partitions

Next you will see the current partition layout. Initially, all disk space will be unallocated. This will change after you add new partitions.

To create a partition, click **Create new partition** and set the new partition location and size. You can do this both by entering values in the **Free space before, Partition size, Free space after** fields, and by dragging partition borders or the partition itself.

If the cursor turns into two vertical lines with left and right arrows, it is pointed at the partition border and you can drag it to enlarge or reduce the partition size. If the cursor turns into four arrows, it is pointed at the partition, so you can move it to the left or right (if there is unallocated space near it).

Select a file system for the new partition. You may select a partition letter of your choice (or leave the default one) and input a label for the new partition in the corresponding field. Finally, select a partition type.

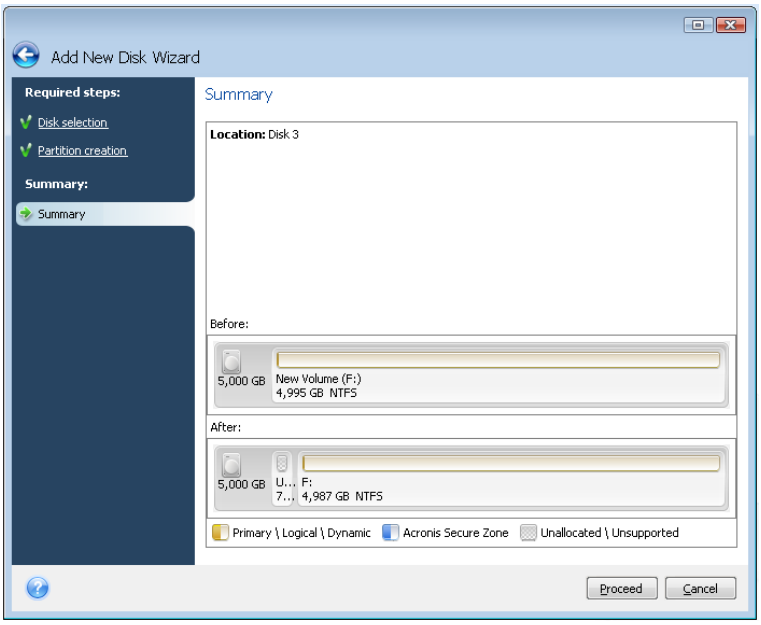


Click the **Accept** button and you will be taken back to the Partition Creation screen. Check the resulting partition's settings and start creating another partition by clicking **Create new partition** again. You can also edit the new partition's settings by clicking **Edit** on the toolbar or delete it by clicking **Delete**.

If you allocate all unallocated space on the disk to the new partition, the **Create new partition** button disappears.

14.3 Disk add summary

Clicking **Next** after creating a desired partition layout takes you to the disk add summary. The disk add summary contains a list of operations to be performed on disks.



After you click **Proceed**, Acronis True Image Home will start creating new partition(s), indicating the progress in a special window. You can stop this procedure by clicking **Cancel**. You will then have to repartition and format the new disk or repeat the disk add procedure.

Chapter 15. Security and Privacy Tools

Acronis True Image Home includes tools for secure destruction of data on an entire hard disk drive, individual partitions, as well as for erasing individual files and eliminating user system activity traces.

These tools ensure the security of your confidential information, as well as maintain your privacy when you work with a PC, because they clean-up the evidence showing your actions (records in various system files) that you don't even know about. This could include user names and passwords.

If you need to:

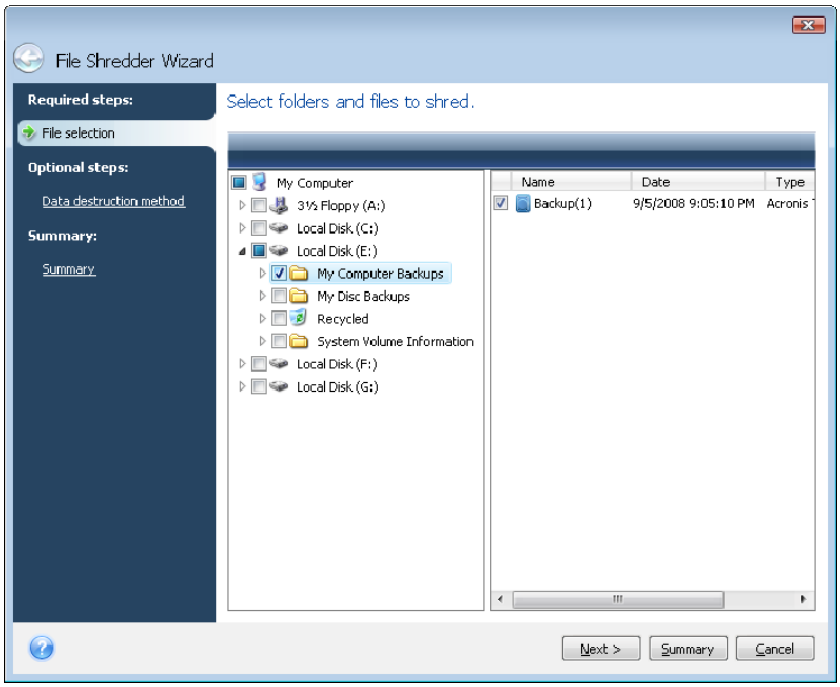
- securely destroy files or folders you select, run **File Shredder**.
- securely destroy data on selected partitions and/or disks so it can't be recovered, run **Acronis DriveCleanser**.
- clean up Windows components (folders, files, registry sections, etc.) related to general system tasks which are capable of retaining user PC activity evidence, run **System Clean-up**.

15.1 Using File Shredder

The **File Shredder** enables quick selection of files and folders to destroy them permanently.

To run the folders/files shredder, select **Tools -> File Shredder** in the main program menu. This starts **File Shredder Data Destruction Wizard**, which will guide you through the steps required for permanently destroying the selected files and folders.

1. First select the files and/or folders you wish to destroy.



2. On the next wizard's step select the desired data destruction method. By default the program will use the Fast method (see ***Appendix C. Hard Disk Wiping*** methods of this manual). You can also choose one of the other preset data destruction methods from the drop-down list.

3. To permanently destroy the selected files using the desired method, click **Proceed** in the next window.

15.2 Acronis DriveCleanser

Many operating systems do not provide users with secure data destruction tools, so deleted files can be restored easily by using simple applications. Even a complete disk reformat can not guarantee you permanent confidential data destruction.

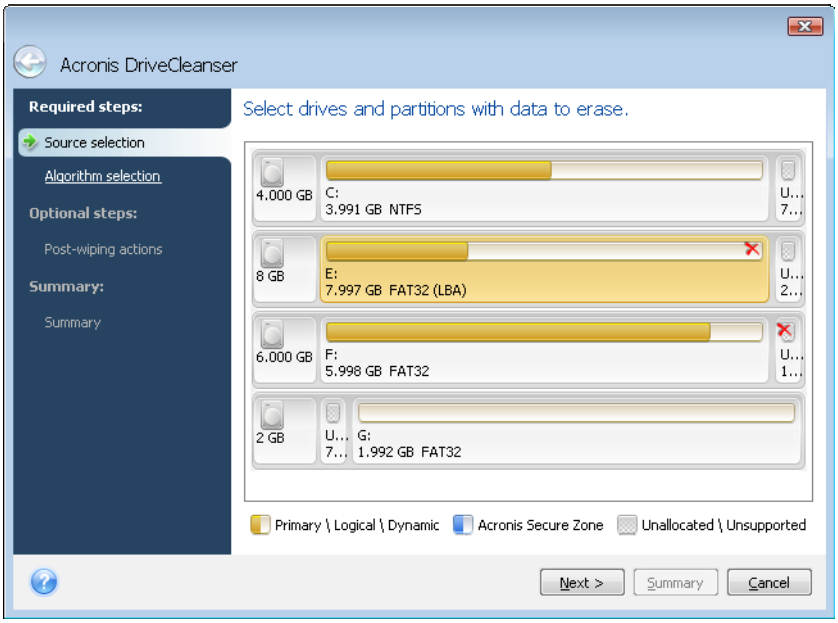
Acronis DriveCleanser solves this problem with guaranteed and permanent data destruction on selected hard disks and/or partitions. It allows you to select from a number of data destruction methods depending on the importance of your confidential information.

To start Acronis DriveCleanser, select **Tools -> Acronis DriveCleanser** in the main program menu. Acronis DriveCleanser allows you to do the following:

- clean up selected hard disks or partitions using preset methods;
- create and execute custom user methods of hard disk clean-up.

Acronis DriveCleanser is based on a **wizard** that **scripts** all hard disk operations, so no data destruction is performed until you click **Proceed** in the wizard's Summary window. At any moment, you can return to the previous steps to select other disks, partitions or data destruction methods.

First, you must select the hard disk partitions where you want to destroy data.



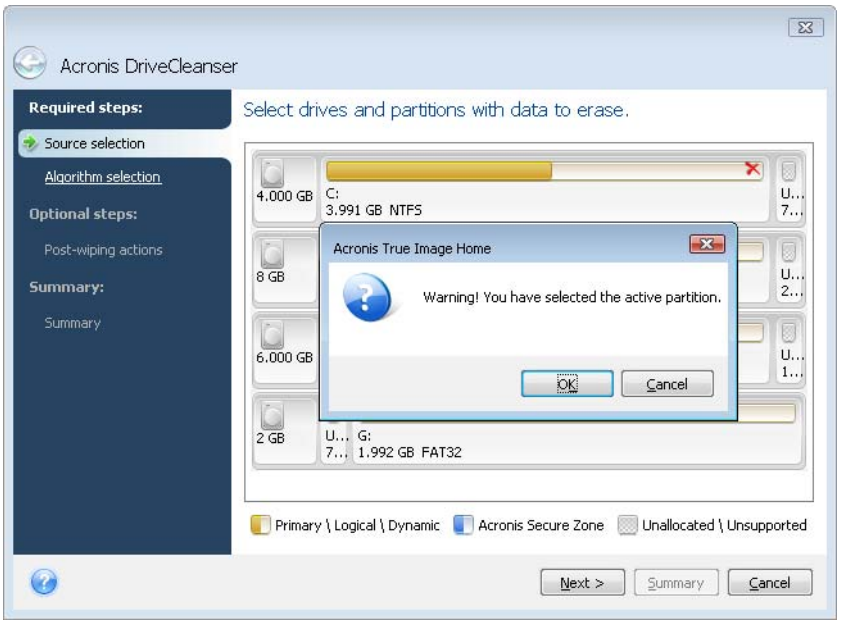
To select a partition, click the corresponding rectangle. You will see a red mark in the upper right corner indicating that the partition is selected.

You can select an entire hard disk or several disks for data destruction. To do this, click the rectangle corresponding to the hard disk (with a device icon, disk number and capacity).

You can select at one time several partitions located on different hard disks or on several disks.

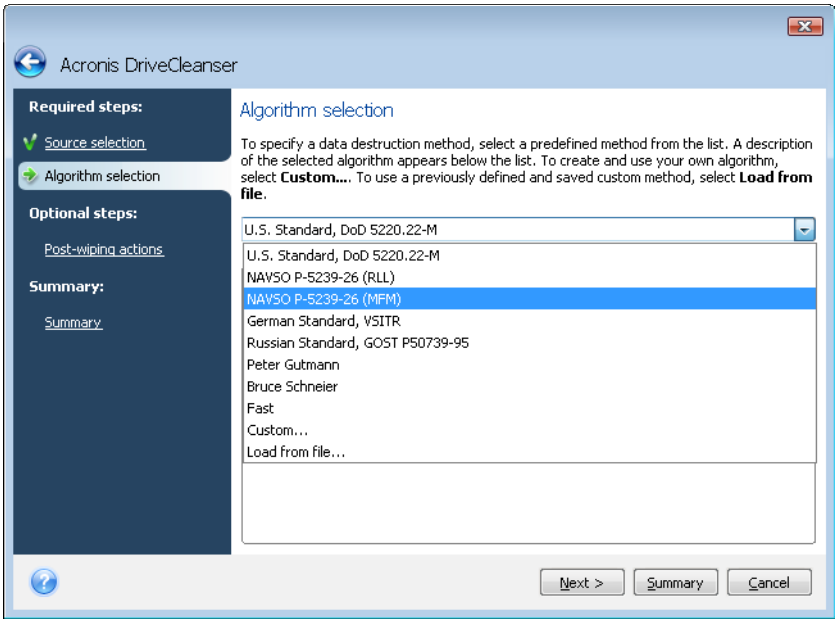
Click **Next** to continue.

If the disks and/or partitions you have selected include the system disk or partition, you will see a warning window.



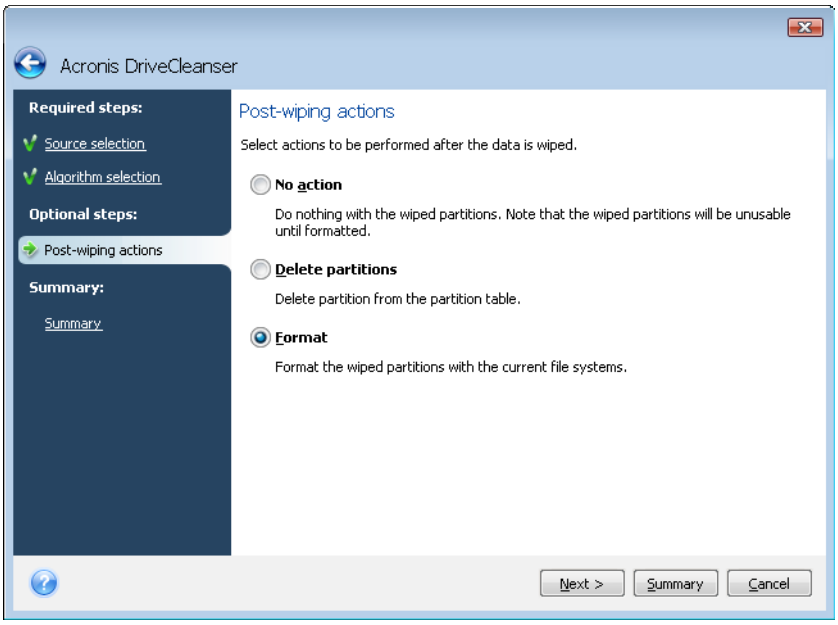
Be careful, because clicking OK in this warning window and then Proceed in the Summary window will result in wiping the system partition containing your Windows operating system.

Acronis DriveCleanser utilizes a number of the most popular data destruction methods described in detail in ***Appendix C. Hard Disk Wiping*** methods of this manual. If you want to create a custom data destruction algorithm, choose **Custom...** and go to *15.3 Creating custom algorithms of data destruction*.



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 choices:

- **Leave partition(s) as is** — just destroy data using the method selected below
- **Delete partition(s)** — destroy data and delete partition
- **Format** — destroy data and format partition (default)

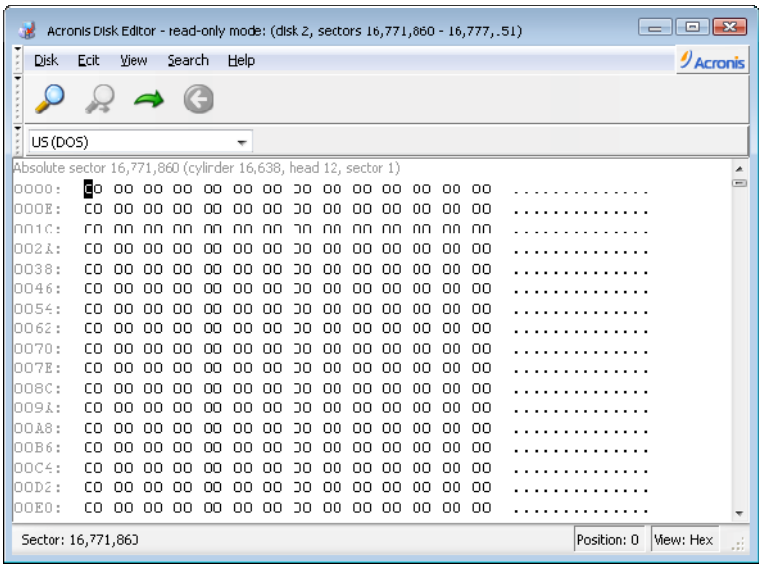


In this example, the switch is set to **Format**. This will allow you to see the results of partition and data destruction, along with the reformatting of the partition.

After you select a post-wiping action and click **Next**, Acronis DriveCleanser will display the data destruction task summary. Up to this point, you can make changes in the created task. Clicking **Proceed** will launch the task execution. Acronis DriveCleanser will perform all actions necessary for destroying the contents of the selected partition or disk. After this is done, you will see a message indicating the successful data destruction.

Acronis DriveCleanser offers you another useful capability — to estimate the results of executing a data destruction method on a hard disk or partition. To view the state of your cleaned disks or partitions, choose **Utilities** in the lower part of the sidebar and then **Disk clean-up** in the upper part. The Acronis DriveCleanser area in the right pane contains the **View disks** link. Click on the link and then choose the partition whose cleaning results you wish to view. This opens an integrated **DiskViewer** hard disk browsing tool (a module of Acronis Disk Editor).

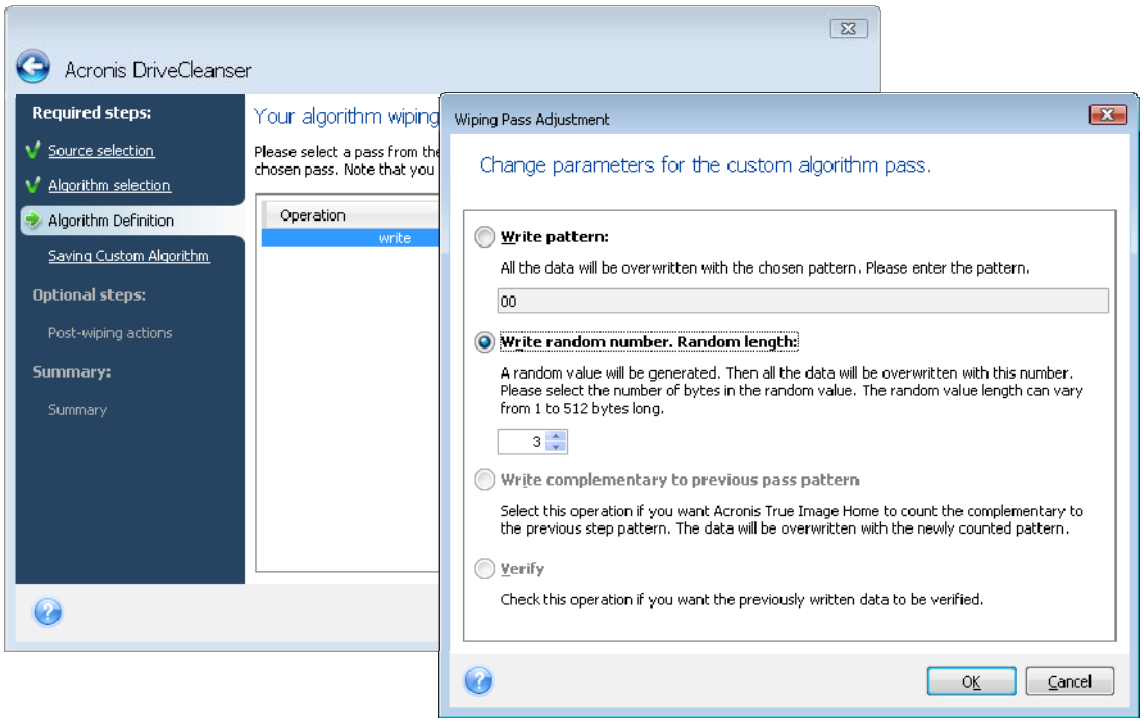
The aforementioned algorithms offer various levels of confidential data destruction. Thus the picture you might see on a disk or partition depends on the data destruction method. But what you actually see are disk sectors filled with either zeros or random symbols.



15.3 Creating custom algorithms of data destruction

Acronis DriveCleanser gives you the opportunity to create your own algorithms for wiping hard disks. Although the software includes several levels of data destruction, you can choose to create your own. This is recommended only for users familiar with the principles of data destruction used in secure disk wiping methods.

Creating a custom method of hard disk wiping is possible after choosing "**Custom...**" from the drop-down list in the **Algorithm Selection** window. In this case some new required steps appear in the DriveCleanser wizard and you will be able to create a data destruction algorithm matching your security requirements.



Having completed the creation, you can save the algorithm you created. This will be handy if you are going to use it again.

To save your algorithm, you need to give it a filename and show the path to the folder you want to store it in by selecting the folder from the tree shown in the left pane.

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

If you created and saved your algorithm for data destruction while working with Acronis DriveCleanser, you can use it later in the following way:

In the **Algorithm Selection** window, choose **Load from file...** from the drop-down list and select the file with custom data destruction algorithm parameters. By default, such files have a *.alg extension.

15.4 System Clean-up

The **System Clean-up** Wizard enables you to securely remove all traces of your PC actions stored by Windows.

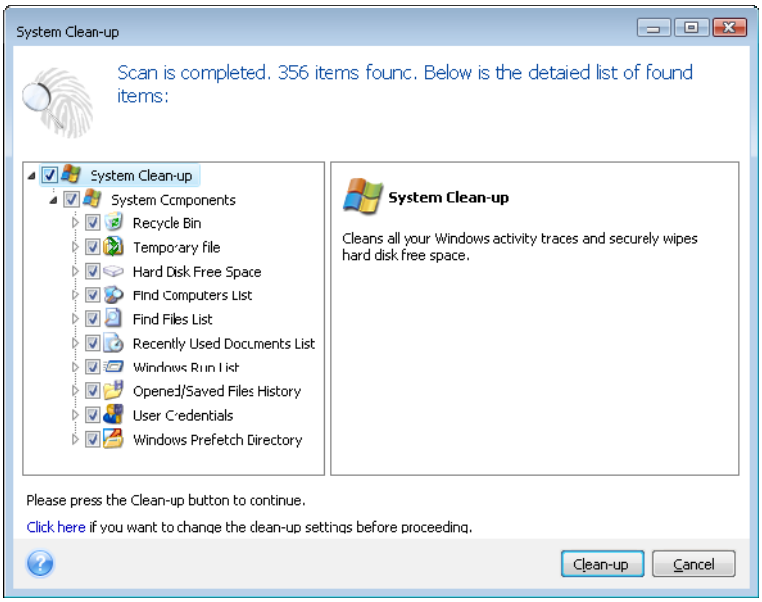
It can do the following operations:

- 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 does 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.

After you run the **wizard** by selecting **Tools -> System Clean-up** in the main program menu, 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.

15.5 System Clean-up Wizard settings

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.

To enable or disable any System Clean-up component, check or uncheck its **Enable this component** flag.

In the System Clean-up Wizard **Properties** window you can also set clean-up parameters for each system component. Some of these parameters apply to all components.

You can restore the default system clean-up settings by clicking the **Restore Defaults** button in the **Properties** window.

15.5.1 "Data Destruction Method" setting

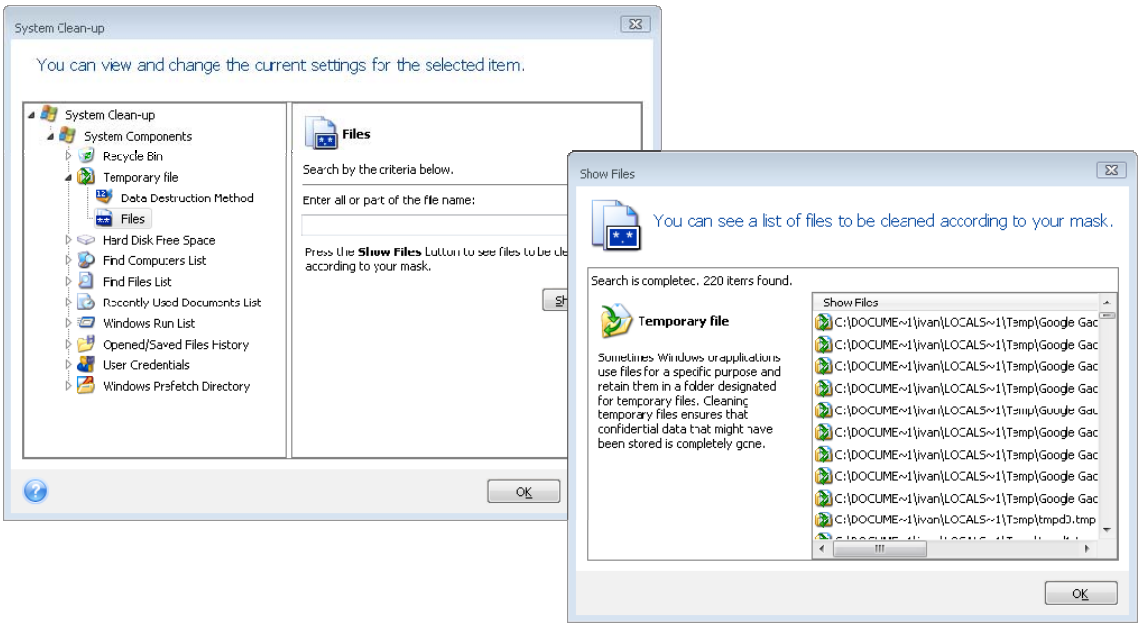
This setting defines the method of guaranteed data destruction to use for cleaning up a given component.

By default, all components that have this setting have it set to **Use common method**. You can change the common method by clicking the **Click to change this setting...** link and selecting a desired method from the drop-down list (see ***Appendix C. Hard Disk Wiping*** methods).

If you need to set a custom method of data destruction for a component, choose **Use custom method for this component** and then select the one you prefer from the drop-down list.

15.5.2 "Files" setting

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"

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 found files. These files will be cleaned.

15.5.3 "Computers" setting

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.

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.

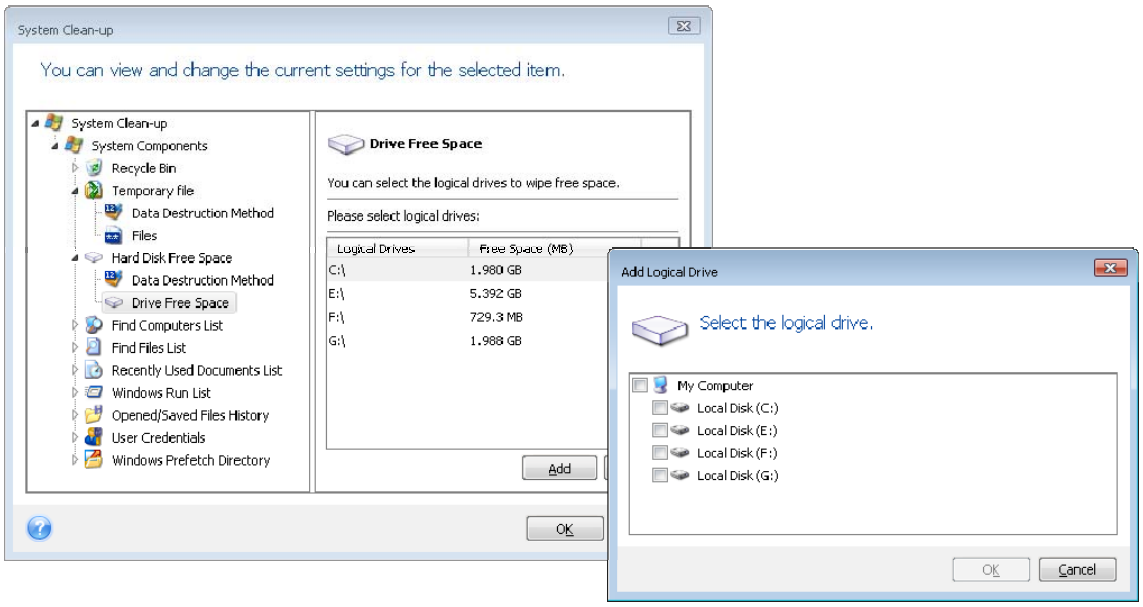
15.5.4 "Drive Free Space" setting

Here you can manually specify physical and/or logical drives to clean up free space on.

By default, the System Clean-up Wizard 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.



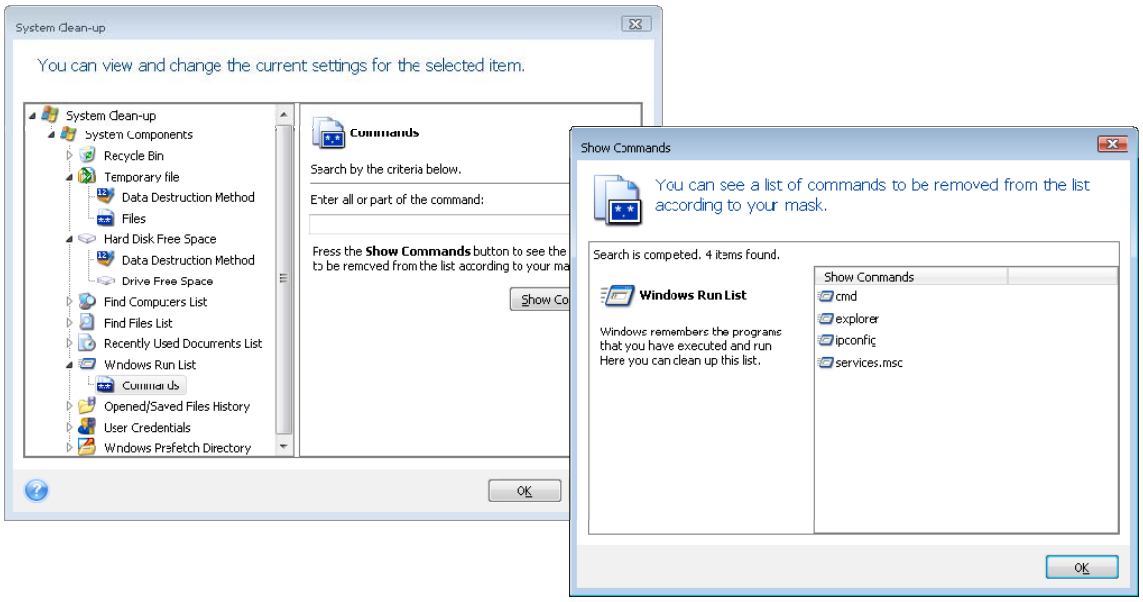
15.5.5 "Commands" setting

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.



15.5.6 "Network Places Filter" setting

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.

To see the list of network places for which the stored network user credentials will be wiped according to your filter, click **Show Network Places**.

15.6 Cleaning up separate system components

If you don't want to clean up all system components, you can clean components of your choice or an individual component separately.

In this case all global settings of the **System Clean-up Wizard** will be valid for individual components as well.

To clean up individual components, select them in the **System Components** section in the **System Clean-up** window and run the **System Clean-up Wizard**.

Appendix A. Partitions and file systems

A.1 Hard disk partitions

The mechanism that allows you to install several operating systems on a single PC or to carve up a single physical disk drive into multiple "logical" disk drives is called **partitioning**.

Partitioning is performed by special applications. In MS-DOS and Windows, these are FDISK and Disk Administrator.

Partitioning programs perform the following:

- create a primary partition
- create an extended partition that can be split into several logical disks
- set an active partition (applied to a single primary partition only)

Information about partitions on a hard disk is stored in a special disk area – in the 1st sector of cylinder 0, head 0, which is called the partition table. This sector is called the master boot record, or MBR.

A physical hard disk might contain up to four partitions. This limit is forced by the partition table that is suitable for four strings only. However, this does not mean you can have only four operating systems on your PC! Applications called disk managers support far more operating systems on disks. For example, Acronis OS Selector, a component of Acronis Disk Director Suite, enables you to install up to 100 operating systems!

A.2 File systems

An operating system gives the user the ability to work with data by supporting a certain type of **file system** on a partition.

All file systems are made of structures that are necessary to store and manage data. These structures are usually composed of operating system boot sectors, folders and files. File systems perform the following basic functions:

- track occupied and free disk space (and bad sectors, if any)
- support folders and file names
- track physical location of files on disks

Different operating systems use different file systems. Some operating systems are able to work with only one file system, while others can use several of them. Here are some of the most widely used file systems:

A.2.1 FAT16

The FAT16 file system is widely used by DOS (DR-DOS, MS-DOS, PC-DOS, PTS-DOS, etc.), Windows 98/Me, and Windows NT/2000/XP/Vista operating systems and is supported by most other systems.

The main features of FAT16 are the file allocation table (FAT) and clusters. FAT is the core of the file system. To increase data safety, it is possible to have several copies of the FAT (there are usually two of them) on a single disk. A cluster is a minimum data storage unit in the FAT16 file system. One cluster contains a fixed number of sectors. FAT stores information about what clusters are free, what clusters are bad, and also defines in which clusters files are stored.

The FAT16 file system has a 2GB limit that permits a maximum 65,507 clusters that are 32KB in size. (Windows NT/2000/XP/Vista support partitions up to 4GB with up to 64KB clusters). Usually the smallest cluster size is used to make the total cluster amount within the 65,507 range. The larger a partition, the larger its clusters.

Usually the larger the cluster size, the more disk space is wasted. A single byte of data could use up one cluster, whether the cluster size is 32KB or 64KB.

Like many other file systems, the FAT16 file system has a root folder. Unlike others, however, its root folder is stored in a special place and is limited in size (standard formatting produces a 512-item root folder).

Initially, FAT16 had limitations on file names. They could only be eight characters long, plus a dot, plus three characters of the name extension. However, long-name support in Windows 95 and Windows NT bypassed this limitation. The OS/2 operating system also supports long names, but does so in a different way.

A.2.2 FAT32

The FAT32 file system was introduced in Windows 95 OSR2. It is also supported by Windows 98/Me/2000/XP/Vista. FAT32 is an evolved version of FAT16. Its main differences from FAT16 are 28-bit cluster numbers and a more flexible root, whose size is unlimited. The reasons FAT32 appeared are the support of large hard disks (over 8GB in capacity) and the impossibility of implementing any more complex file system into MS-DOS, which is still the basis for Windows 98/Me.

The maximum FAT32 disk size is 2 terabytes (1 terabyte, or TB, is equal to 1024 gigabytes, or GB).

A.2.3 NTFS

NTFS is the main file system for Windows NT/2000/XP/Vista. Its structure is closed, so no other operating system is fully supported. The main structure of NTFS is the MFT (master file table). NTFS stores a copy of the critical part of the MFT to reduce the possibility of data damage and loss. All other NTFS data structures are special files. NTFS stands for NT File System.

Like FAT, NTFS uses clusters to store files, but cluster size does not depend on partition size. NTFS is a 64-bit file system. It uses unicode to store file names. It is also a journaling (failure-protected) file system, and supports compression and encryption.

Files in folders are indexed to speed up file search.

A.2.4 Linux Ext2

Ext2 is one of the main file systems for the Linux operating system. Ext2 is a 32-bit system. Its maximum size is 16TB. The main data structure that describes a file is an i–node. A place to store the table of all i-nodes has to be allocated in advance (during formatting).

A.2.5 Linux Ext3

Officially introduced with its version 7.2 of the Linux operating system, Ext3 is the Red Hat Linux journaling file system. It is forward and backward compatible with Linux ext2. It has multiple journaling modes and broad cross-platform compatibility in both 32- and 64-bit architectures.

A.2.6 Linux ReiserFS

ReiserFS was officially introduced to Linux in 2001. ReiserFS overcomes many Ext2 disadvantages. It is a 64-bit journaling file system that dynamically allocates space for data substructures.

Appendix B. Hard disks and BIOS setup

The appendices below provide you with extra information on how the hard disk is organized, how information is stored on disks, how disks should be installed in the computer and plugged into the motherboard, configuring disks with BIOS, partitions and file systems, and how operating systems interact with disks.

B.1 Installing hard disks in computers

B.1.1 Installing a hard disk, general scheme

To install a new IDE hard disk, you should do the following (**we will assume you have powered OFF your PC before you start!**)**:**

1. Configure the new hard disk as **slave** by properly installing jumpers on its controller board. Disk drives generally have a picture on the drive that shows the correct jumper settings.

2. Open your computer and insert the new hard disk into a 3.5'' or 5.25'' slot with special holders. Fasten down the disk with screws.

3. Plug the power cable into the hard disk (four-threaded: two black, yellow and red; there is only one way you can plug in this cable).

4. Plug the 40- or 80-thread flat data cable into sockets on the hard disk and on the motherboard (plugging rules are described below). The disk drive will have a designation on the connector or next to it that identifies Pin 1. The cable will have one red wire on the end that is designated for Pin 1. Make sure that you place the cable in the connector correctly. Many cables also are "keyed" so that they can only go in one way.

5. Turn your computer on and enter BIOS setup by pressing the keys that are displayed on the screen while the computer is booting.

6. Configure the installed hard disk by setting the parameters **type**, **cylinder**, **heads**, **sectors** and **mode** (or **translation mode**; these parameters are written on the hard disk case) or by using the IDE autodetection BIOS utility to configure the disk automatically.

7. Set the boot sequence to A:, C:, CD-ROM or some other, depending on where your copy of Acronis True Image Home is located. If you have a boot diskette, set the diskette to be the first; if it is on a CD, make the boot sequence start with CD-ROM.

8. Quit BIOS setup and save changes. Acronis True Image Home will automatically start after reboot.

9. Use Acronis True Image Home to configure hard disks by answering the wizard's questions.

10. After finishing the work, turn off the computer, set the jumper on the disk to the **master** position if you want to make the disk bootable (or leave it in **slave** position if the disk is installed as additional data storage).

B.1.2 Motherboard sockets, IDE cable, power cable

There are two slots on the motherboard to which the hard disks can be connected: **primary IDE** and **secondary IDE**.

Hard disks with an IDE (Integrated Drive Electronics) interface are connected to the motherboard via a 40- or 80-thread flat marked cable: one of the threads of the cable is red.

Two IDE hard disks can be connected to each of the sockets, i.e. there can be up to four hard disks of this type installed in the PC. (There are three plugs on each IDE cable: two for hard disks and one for the motherboard socket.)

As noted, IDE cable plugs are usually designed so that there is only one way to connect them to the sockets. Usually, one of the pinholes is filled on the cable plug, and one of the pins facing the filled hole is removed from the motherboard socket, so it becomes impossible to plug the cable in the wrong way.

In other cases, there is a jut on the plug on the cable, and an indentation in the socket of the hard disk and of the motherboard. This also ensures that there is only one way to connect the hard disk and the motherboard.

In the past, this design of plug did not exist, so there was an empirical rule: **the IDE cable is connected to the hard disk socket so that the marked thread is the closest to the power cable**, i.e. the marked thread connected to pin #1 of the socket. A similar rule was used for connecting cables with the motherboard.

Incorrect connection of the cable with either the hard disk or the motherboard does not necessarily damage the electronics of the disk or the motherboard. The hard disk is simply not detected or initialized by BIOS.

There are some models of hard disks, especially the older ones, for which incorrect connection damaged the electronics of the drive.

We will not describe all the types of hard disks. Currently the most widespread are those with IDE or SCSI interfaces. Unlike IDE hard disks, there can be from six to 14 SCSI hard disks installed in your PC. However, you need a special SCSI controller (called a host adapter) to connect them. SCSI hard disks are not usually used in personal computers (workstations), but are found mostly in servers.

Aside from an IDE cable, a four-thread power cable must be connected to the hard disks. There is only one way to plug in this cable.

B.1.3 Configuring hard disk drives, jumpers

A hard disk drive can be configured in a computer as **master** or as **slave**. The configuring is done using special connectors (called jumpers) on the hard disk drive.

The jumpers are either located on the electronic board of the hard disk or a special socket that provides for the connection of the hard disk and the motherboard.

There is usually a sticker on the drive that explains the markings. Typical markings are **DS**, **SP**, **CS** and **PK**.

Each jumper position corresponds to one hard disk(s) installation mode:

- **DS – master/factory default**
- **SP – slave (or no jumper required)**
- **CS – cable select for master/slave**: the purpose of the hard disk is determined by its physical position with respect to the motherboard
- **PK – jumper parking position**: the position where one can put the jumper if it is not necessary in the existing configuration

The hard disk with the jumper in **master** position is treated by the basic input/output system (BIOS) as bootable.

The jumpers on hard disks that are connected to the same cable can be in the **cable select for master/slave** position. In this case, BIOS will deem as "master", the disk that is connected to the IDE cable, which is closer to the motherboard than the other one.

Unfortunately, hard disk markings were never standardized. You might well find that markings on your hard disk differ from the ones described above. Moreover, for the old types of hard disks, their purpose could be defined by two jumpers instead of one. You should study the markings carefully before installing your hard disk in the computer.

It is not enough to physically connect the hard disk to the motherboard and set the jumpers properly for the hard disk to function — hard disks have to be properly configured with the motherboard BIOS.

B.2 BIOS

When you turn on your computer, you often see a number of short text messages before you see the splash screen of your operating system. These messages are from the POST (power-on self test) program that belongs to BIOS and is executed by the processor.

BIOS, or the basic input/output system, is a program that resides in the permanent memory chip (ROM or flash BIOS) on the motherboard of your computer and is its key element. The version of BIOS that you use "knows" all the peculiarities of all the components of the motherboard: processor, memory, integrated devices. BIOS versions are provided by the manufacturers of motherboards.

Main BIOS functions are:

- POST checking of processor, memory and I/O devices
- initial configuring of all software-manageable parts of the motherboard
- initialization of the operating system (OS) booting process

Among numerous components of the computer, initial configuration is necessary for the external memory subsystem that controls hard disk drives, floppy disk drives, CD-ROM drives, DVDs, and other devices.

B.2.1 Setup utility

BIOS has a built-in setup utility for initial computer configuration. To enter it, you have to press a certain key combination (**Del, F1**, **Ctrl+Alt+Esc**, **Ctrl+Esc**, or some other, depending on your BIOS) during the POST sequence that starts immediately after you turn your computer on. Usually the message with the required key combination is displayed during the startup testing. Pressing this combination takes you to the menu of the setup utility that is included in your BIOS.

The menu can differ in appearance, sets of items and their names, depending on the BIOS manufacturer. The most widely known BIOS makers for PC motherboards are Award/Phoenix and AMI. Moreover, while items in the standard setup menu are mostly the same for various BIOSes, items of the extended setup heavily depend on the computer and BIOS version.

Below we describe the general principles of initial hard disk configuration.

Large PC manufacturers like Dell and Hewlett-Packard produce motherboards themselves, and develop their own BIOS versions. You should always refer to the documentation that came with your computer for instructions on proper BIOS configuration.

B.2.2 Standard CMOS setup menu

Parameters in the standard CMOS setup menu usually define the geometry of the hard disk. The following parameters (and values) are available for each hard disk installed in your PC:

Parameter	Value	Purpose
Type	1-47, Not Installed, Auto	Type 0 or Not Installed is used when there is no hard disk installed (to uninstall it). Type 47 is reserved for user-defined parameters or for parameters detected by the IDE Auto detection utility. Auto value allows for automatic detection of IDE disk parameters during the boot sequence.
Cylinder (Cyl)	1-65535	The number of cylinders on a hard disk. For IDE disks, a logical number of cylinders are specified.
Heads (Hd)	1-16	The number of heads on a hard disk. For IDE disks, a logical number of heads are specified.
Sectors (Sec)	1-63	The number of sectors per track of a hard disk. For IDE disks, a logical number of sectors are specified.
Size (Capacity)	MBytes	The capacity of the disk in megabytes. It is calculated according to the following formula: Size=(Cyl x Hds x Sec x 512) / 1024 / 1024.
Mode (Translation Method)	Normal/ LBA/ Large/Auto	Method of translation of sector addresses.

For example, to demonstrate the main features of Acronis True Image Home, we used a Quantum™ Fireball™ TM1700A hard disk as one of the disks in our examples. Its parameters have the following values:

Parameter	Value
Type	Auto
Cylinder (Cyl)	827
Heads (Hd)	64
Sectors (Sec)	63
Mode	Auto
CHS	1707 MB
Maximum LBA Capacity	1707 MB

In BIOS setup, you can set the Type parameter to User Type HDD (user-defined type). In this case, you also have to specify the value of the translation mode parameter, which can be Auto/Normal/LBA/Large.

Translation mode is how sector addresses are translated. This parameter appeared because in BIOS versions, there were limitations to the maximum address capacity of disks, which is 504 MB (1024 cylinders x 16 heads x 63 sectors x 512 bytes). There are two ways to bypass this limitation: (1) switch from physical to logical sector addresses (LBA), (2) use mathematics to reduce the number of addressed sectors (cylinders) and increase the number of heads; this method is called Large Disk (Large). The simplest decision is to set the value of this parameter to Auto.

If there are several hard disks connected to your motherboard, but you do not want to use some of them at the moment, you have to set the Type of these disks to Not Installed.

Parameters of hard disks can be set manually with the help of information provided by the hard disk manufacturer on its case, but it is easier to use the IDE autodetection utility that is usually included in modern BIOS versions.

The utility is sometimes a separate BIOS menu item and is sometimes included in the standard CMOS setup menu.

Please note that in "Appendix B. Hard disks and BIOS setup", we have described the general details of the **physical** hard disk structure. Built-in IDE hard disk controls mask the physical disk structure. As a result, the BIOS of the motherboard "sees" **logical** cylinders, heads and sectors. We are not going to elaborate on this issue here, but knowing about this can sometimes be useful.

B.2.3 Arranging boot sequence, advanced CMOS setup menu

Aside from standard CMOS setup, the BIOS menu usually has an **advanced CMOS setup** item. Here you can adjust the **boot sequence**: C:; A:; CD-ROM:.

Please note that **boot sequence** management differs for various BIOS versions, e.g. for AMI BIOS, AWARDBIOS, and brand-name hardware manufacturers.

Several years ago, the operating system boot sequence was hard-coded into the BIOS. An operating system could be booted either from a diskette (drive A:), or from the hard disk C:. That was the sequence in which the BIOS queried external drives: if drive A: was ready, BIOS attempted to boot an operating system from a diskette. If the drive was not ready or there was no system area on the diskette, BIOS tried to boot an operating system from hard disk C:.

At present, BIOS allows booting operating systems not only from diskettes or hard disks, but also from CD-ROMs, DVDs, and other devices. If there are several hard disks installed in your computer labeled as C:, D:, E:, and F:, you can adjust the boot sequence so that an operating system is booted from, for example, disk E:. In this case, you have to set the boot sequence to look like E:, CD-ROM:, A:, C:, D:.

This does not mean that booting is done from the first disk in this list; it only means that the **first attempt** to boot an operating system is to boot it from this disk. There may be no operating system on disk E:, or it may be inactive. In this case, BIOS queries the next drive in the list. Errors can happen during booting, see B.2.4 "*Hard disk initialization errors*".

The BIOS numbers disks according to the order in which they are connected to IDE controllers (primary master, primary slave, secondary master, secondary slave); next go the SCSI hard disks.

This order is broken if you change the boot sequence in BIOS setup. If, for example, you specify that booting has to be done from hard disk E:, numbering starts with the hard disk that would be the third in usual circumstances (it is usually the secondary master).

After you have installed the hard disk in your computer and have configured it in BIOS, one can say that the PC (or the motherboard) "knows" about its existence and its main parameters. However, it is still not enough for an operating system to work with the hard disk. In addition, you have to create partitions on the new disk and format the partitions using Acronis True Image Home. See *Chapter 14. Adding a new hard disk*.

B.2.4 Hard disk initialization errors

Devices are usually initialized successfully, but sometimes errors can happen. Typical errors related to hard disks are reported by the following messages:

```
PRESS A KEY TO REBOOT
```

This error message is not directly related to errors during hard disk initialization. However, it appears, for example, when the boot program finds no operating system on the hard disk, or when the primary partition of the hard disk is not set as active.

```
DISK BOOT FAILURE,
INSERT SYSTEM DISK AND
PRESS ENTER
```

This message appears when the boot program finds no available boot device, be it a floppy or a hard disk, or a CD-ROM.

```
C: DRIVE ERROR
C: DRIVE FAILURE
ERROR ENCOUNTERED INITIALIZING HARD DRIVE
```

This message appears when it is not possible to access the C: disk. If the disk is known to be functional, the reason for this error message is probably incorrect settings/connections of:

- hard disk parameters in BIOS setup
- jumpers on the controller (master/slave)
- interface cables

It is also possible that the device is out of order, or the hard disk is not formatted.

B.3 Installing a SATA hard drive

Most recently manufactured PCs use the SATA interface for hard drives. In general, installing a SATA hard drive is easier than an IDE drive, as it is not necessary to configure master-slave jumpers. SATA drives use a thin interface cable with seven-pin keyed connectors. This improves airflow through the PC case. Power is supplied to SATA drives through 15-pin connectors. Some SATA drives also support legacy four-pin power connectors (Molex) — you can use a Molex or SATA connector but do not use both at the same time, because this could damage the hard drive. You'll

also need a free power lead fitted with a SATA power connector. Most systems that come with SATA ports have at least one SATA power connector. If this is not the case, you will need a Molex-to-SATA adapter. In case your system has the SATA power connector but it is already occupied, use a Y-adapter that splits a lead in two.

B.3.1 Steps for installing a new internal SATA drive.

1. Find an unused SATA port using the documentation provided with your PC. If you are going to connect your new SATA drive to a SATA controller card, install the card. If you are going to connect the SATA drive to the motherboard, enable applicable motherboard jumpers, if any. Most hard drive kits include a SATA interface cable and mounting screws. Attach one end of the SATA interface cable to a SATA port on the motherboard or interface card, and the other to the drive.

2. Then plug the power-supply lead or use a Molex-to-SATA adapter.

3. Prepare your drive. If you're installing a SATA 300 hard drive, check your PC's (or SATA host adapter's) documentation to make sure it supports SATA 300 drives. If it doesn't, you might need to change a jumper setting on the drive (see the drive's manual for instructions). If you have a SATA 150 hard drive, you don't need to change any settings.

4. Turn on the PC and look for the new drive in the boot-up messages. If you don't see it, enter the PC's CMOS setup program and search the BIOS configuration menu for an option that will let you enable SATA for the ports you are using (or maybe you will just need to enable SATA). See your motherboard documentation for instructions specific to your BIOS.

5. If the operating system does not recognize the SATA drive, you need the appropriate drivers for your SATA controller. If the drive is recognized, go to step 8.

- Usually, it is best to obtain the latest driver version from the motherboard or SATA controller manufacturer's website.
- If you download a copy of the SATA controller drivers, place the driver files to a known location on your hard drive.

6. Boot from the old hard drive.

- The operating system should detect the SATA controller and install the appropriate software. You might need to provide the path to the driver files.

7. Ensure that the SATA controller and the connected SATA hard drive are correctly detected by the operating system. To do this, go to the Device Manager.

- SATA controllers usually appear under the SCSI and RAID controllers section of Device Manager, while hard drives are listed under the Disk drives section.
- The SATA controller and SATA hard drive must not be displayed in the Device Manager with a yellow exclamation mark or any other error indication.

8. After you have installed the hard disk in your computer and have configured it in BIOS, one can say that the PC "knows" about its existence and its main parameters. However, it is still not enough for the operating system to work with the hard disk. In addition, you have to create partitions on the new disk and format the partitions using Acronis True Image Home. See *Chapter 14. Adding a new hard disk*. Then configure your BIOS to boot from the SATA controller and boot from the SATA hard drive to ensure it works.

Appendix C. Hard Disk Wiping methods

Information removed from a hard disk drive by non-secure means (for example, by simple Windows delete) can easily be recovered. Utilizing specialized equipment, it is possible to recover even repeatedly overwritten information. Therefore, guaranteed data wiping is more important now than ever before.

The **guaranteed wiping of information** from magnetic media (e.g. a hard disk drive) means it is impossible to recover data by even a qualified specialist with the help of all known tools and recovery methods.

This problem can be explained in the following way: 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.

It only requires specialized software and inexpensive hardware to read data "deleted" this way by analyzing magnetization of hard disk sectors, residual magnetization of track sides and/or by using current magnetic microscopes.

Writing to magnetic media leads to subtle effects summarized as follows: every track of a disk stores **an image of every record** ever written to it, but the effect of such records (magnetic layer) becomes more subtle as time passes.

C.1 Information wiping methods' functioning principles

Physically, the complete wiping of information from a hard disk involves the switching of every elementary magnetic area of the recording material as many times as possible by writing specially selected sequences of logical 1's and 0's (also known as samples).

Using logical data encoding methods in current hard disks, you can select **samples** of symbol (or elementary data bit) sequences to be written to sectors in order to **repeatedly and effectively wipe confidential information.**

Methods offered by national standards provide (single or triple) recording of random symbols to disk sectors that are **straightforward and arbitrary decisions, in general**, but still acceptable in simple situations. The most effective information-wiping method is based on deep analysis of subtle features of recording data to all types of hard disks. This knowledge speaks of the necessity of complex multipass methods to **guarantee** information wiping.

The detailed theory of guaranteed information wiping is described in an article by Peter Gutmann. Please see:

http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html.

C.2 Information wiping methods used by Acronis

The table below briefly describes information wiping methods used by Acronis. Each description features the number of hard disk sector passes along with the number(s) written to each sector byte.

The description of built-in information wiping methods

No.	Algorithm (writing method)	Passes	Record
1.	United States Department of Defense 5220.22-M	4	1st pass – randomly selected symbols to each byte of each sector, 2 – complementary to written during the 1st pass; 3 – random symbols again; 4 – writing verification.
2.	United States: NAVSO P-5239-26 (RLL)	4	1st pass – 0x01 to all sectors, 2 – 0x27FFFFF, 3 – random symbol sequences, 4 – verification.
3.	United States: NAVSO P-5239-26 (MFM)	4	1st pass – 0x01 to all sectors, 2 – 0x7FFFFFF, 3 – random symbol sequences, 4 – verification.
4.	German: VSITR	7	1st – 6th – alternate sequences of: 0x00 and 0xFF; 7th – 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 6th to 4th security level systems. Randomly selected symbols (numbers) to each byte of each sector for 3rd to 1st 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 http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html).
7.	Bruce Schneier's method	7	Bruce Schneier offers a seven-pass overwriting method in his Applied Cryptography book. 1st pass – 0xFF, 2nd 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.

Appendix D. Startup Parameters

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 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.

