User's Guide

Acronis
True Image 9.1
Enterprise Server

END-USER LICENSE AGREEMENT

BY ACCEPTING, YOU (ORIGINAL PURCHASER) INDICATE YOUR ACCEPTANCE OF THESE TERMS. IF YOU DO NOT WISH TO ACCEPT THE PRODUCT UNDER THESE TERMS, YOU CAN CHOOSE NOT TO ACCEPT BY SELECTING "I decline..." AND NOT INSTALLING THE SOFTWARE.

Acronis True Image Enterprise Server (the Software) is Copyright © Acronis, Inc., 2000-2006. All rights are reserved. The ORIGINAL PURCHASER is granted a LICENSE to use the software only, subject to the following restrictions and limitations.

1.   The license is to the original purchaser only, and is not transferable without prior written permission from Acronis.

2.   The original purchaser can use the software on a single computer. You cannot use the software on more than a single machine, even if you own or lease all of them, without the written consent of Acronis.

3.   The original purchaser cannot engage in, nor permit third parties to engage in, any of the following:

A.   Providing or permitting use of by, or transferring the software to, third parties.

B.   Providing use of the software in a computer service business, network, timesharing or multiple user arrangement to users who are not individually licensed by Acronis.

C.   Making alterations or copies of any kind in the software (except as specifically permitted above).

D.   Attempting to unassemble, decompile or reverse-engineer the software in any way.

E.   Granting sublicenses, leases, or other rights in the software to others.

F.   Making copies, or verbal or media translations, of the users guide.

G.   Making telecommunication data transmission of the software.

Acronis has the right to terminate this license if there is a violation of its terms or default by the original purchaser. Upon termination for any reason, all copies of the software must be immediately returned to Acronis, and the original purchaser shall be liable to Acronis for any and all damages suffered as a result of the violation or default.

ENTIRE RISK

THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE SOFTWARE IS WITH YOU THE PURCHASER. Acronis DOES NOT WARRANT THAT THE SOFTWARE OR ITS FUNCTIONS WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR FREE OR THAT ANY DEFECTS WILL BE CORRECTED.

NO LIABILITY FOR CONSEQUENTIAL DAMAGES IN NO EVENT SHALL Acronis OR ITS VENDORS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR THE LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE, EVEN IF Acronis HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOFTWARE USAGE TERMS AND CONDITIONS

Under current legislation, the «License Agreement» is considered a contract between you and Acronis Inc. The contract is a legal document and its violation may result in legal action.

Illegal use and/or distribution of this software will be prosecuted.

Table of Contents

Chapter 1. Introduction

1.1 Acronis True Image Enterprise Server – a complete solution for corporate users

You have come to rely on your servers to run your business and retain key enterprise data. Acronis True Image Enterprise Server provides comprehensive, reliable, and cost-effective system protection and recovery for systems and entire networks. With Acronis True Image Enterprise Server you have peace of mind knowing you are protected and can recover from any situation.

Minimizes downtime

Acronis True Image Enterprise Server enables you to restore systems in minutes, not hours or days. An entire system can be restored from an image that includes everything the system needs to run: the operating system, applications, databases, and configurations. No reinstallation or reconfiguration is required. Moreover, complete system restoration can be performed to an existing system or to a new system with different hardware or to virtual machines. With the new Acronis Snap Restore feature, users can access a system during restore, further decreasing downtime. File-based backups provide you with the flexibility to only backup specific critical files.

Eases Administration

Wizards guide users through backup and recovery tasks, ensuring the product can be implemented with minimal user training. A central management console provides remote administration, ensuring that all systems in the network, regardless of your domain and workgroup structure, can be managed from one location. Complete, unattended restores from remote locations are supported with a remote bootable agent.

Automates Backup

With the scheduling capability in Acronis True Image Enterprise Server, you simply create backup tasks, tailored by group, at certain times or at certain events, automating backups.

To ensure that backups have occurred, or user intervention is required, you can request notifications via email or pop-up. You can view Acronis events in Windows Application Events Log or Acronis own log. Log messages can be automatically sent out to SNMP clients.

The product also supports the creation of custom commands before and after backups. For example, users can automatically run anti-virus products before an image is created and verify the validity of backups after they have been created.

Ensures 24 X 7 Uptime

With the Acronis Drive Snapshot systems can be imaged while they are in use, supporting 24 by 7 availability. This technology enables the product to backup and image critical operating system files, the master boot record and any partition-based boot records without requiring a reboot. A CPU allocation feature allows you to limit the amount of CPU usage for the application to maximize the CPUs available for mission critical applications. Moreover, users can control hard disk drive writing speeds and control network bandwidth used during backups, allowing you minimally disrupt business operations.

A several-second database suspension is provided for correct backup of mission critical applications such as Microsoft Exchange Server, Microsoft SQL Server and Oracle with support VSS. If your database or operating system does not support VSS, Acronis True Image Enterprise Server will execute your custom commands to realize database suspension.

Supports Cutting Edge Technology

Businesses today are moving to leverage the latest technologies, dual-core 64 bit processors and 64 bit operating systems. With Acronis True Image Enterprise Server, you can protect these new machines, as well as legacy ones, running one solution.

Leverages Existing Technology Investments

The product can leverage your current storage infrastructure by supporting a wide variety of storage media, so you can avoid costly hardware purchases to implement the solution. The product supports key storage technologies such as: Direct Attached Storage (DAS), Network Attached Storage (NAS), Storage Area Networks (SAN), Redundant Arrays of Independent Disks (RAID) devices, tapes, USB and IEEE-1394 (FireWire) compliant storage devices, CDs, DVDs, removable drives (Floppy, Zip, etc.) and shared storage. Moreover, the product ensures that you maximize the space on these resources with four levels of compression.

Disk cloning and new disk deployment

Acronis True Image Enterprise Server can be used to clone an image onto multiple servers. For example, a company purchased several servers and needs similar environments on each of them. Traditionally, an IT manager should install the operating system and programs on every server. With Acronis True Image Enterprise Server, the IT manager can create a disk image of the first system deployed. That image can then be duplicated onto multiple servers.

If you need to upgrade the server hard disk drive, Acronis True Image Enterprise Server simplifies the task to few mouse clicks creating the exact copy of your old disk to a new one and adjusting partitions size to fit a new hard disk.

1.2 Acronis True Image Enterprise Server Architecture

Acronis True Image Enterprise Server includes the following components.

1. **Acronis True Image Management Console** – a tool for managing data backup/restore on a local network from a single location. Facilities include remote program components installation, managing computer groups (via **Acronis True Image Group Server**) and backup archives (via **Acronis Backup Server**), scheduling individual and group backup tasks, remote data recovery, checking backup archives, setting backup/restore options on remote computers.

2. **Acronis True Image Agent** – a server application, enabling remote managing of data backup/restore on a networked computer from Acronis True Image Management Console. Acronis True Image Enterprise Server includes **Acronis True Image Agent for Windows** (to be installed on Windows-based systems) and **Acronis True Image Agent for Linux** (to be installed on Linux platform). The Agents operate in a similar way, the only difference visible to user concerns the way of installation.

3. **Acronis Backup Server** – when installed on a networked computer, automatically manages backup archives, stored on this computer, in accordance with the rules, set by an administrator.

4. **Acronis True Image Group Server** – when installed on a networked computer, allows managing and monitoring of group backup tasks on all networked computers in real time.

5. **Acronis True Image Enterprise Server** (local version) – a component for backup/restore management on a local server. Facilities include scheduling backup tasks, data recovery, exploring backup archives, cloning hard disks data and formatting partitions on new hard disks, command-line mode and scripts execution.

6. **Acronis Bootable Rescue Media Builder** - creates bootable media, its ISO image or RIS packages enabling data recovery in case of non-Windows or corrupted operating system.

1.3 New in Acronis True Image 9.1 Enterprise Server

- **Support for Windows XP Professional x64 Edition, Windows Server 2003 x64 Editions**

- **Support for GPT hard disks (disks with GUID partition table)**

- **Acronis Backup Server –** This software application, when installed on a networked computer, automatically manages backup archives, stored on this computer, in accordance with the rules, set by an administrator

- **Acronis True Image Group Server** – When installed on a networked computer, allows managing and monitoring of group backup tasks on all networked computers in real time

- **Acronis True Image Agent for Linux** – Remote backup/restore of Linux-based systems

- **Back up to/restore from FTP servers**

- **Acronis Snap Restore** – A user can start working in seconds while the system is still being restored

- **Acronis Universal Restore (optional)** – Hardware-independent live system restore

- **File-level backup and recovery**, including files opened in exclusive usage mode - In addition to an entire partition/system backup

- **Differential backup** – Backup only the changes made since the full backup

- **Fast incremental/differential backup** – Users can choose to compare files with their archived copies by date/size (fast process) or by file contents (precise, but time-consuming process)

- **Files and folders backup/restore filtering** – Saves space when creating file backups by only backing up files of the types the users want to keep. Similarly, a user can tell the program not to restore certain files from the file archive

- **Microsoft Volume Shadow Copy Service (VSS) support** (for Windows 2003 Server and higher) – Easily backup VSS compatible databases (Exchange, Oracle, SQL Server) without taking databases offline and ensuring data consistency

- **Pre/post backup/restore commands** – Users can specify their own commands which will be executed before and after the backup or restore process. For example, one might want to remove some temporary files from the disk before starting backup or configure a third party antivirus product to be started each time before the backup starts

- **User-editable default backup options** – Users can configure and save backup parameters, such as backup performance (hard disk writing speed, network bandwidth during backups), validate backup archive after backup completion, file-level security settings (preserving files' security settings in the archive, storing encrypted files in encrypted or decrypted state)

- **User-editable default restore options** – Users can configure and save restore parameters, such as files overwriting mode, the original or current date and time for restored files etc.

- **Read-write mode** of mounting images

- **Bootable backup media** – When backing up to removable media, users can make this media bootable in the same manner as rescue CD, so separate recover media is not required

- **Bootable disks ISOs and RIS packages** – In addition to burning a bootable rescue disk, users can save its ISO image for burning later, or create a RIS package for remote boot of Acronis True Image Enterprise Server

- **Acronis Bootable Agent** – Adding this Agent to the rescue disk or RIS package will enable the administrator to manage the remote computer, booted from this disk/RIS-server, with Acronis True Image Management Console. Thus, they can restore unattended systems, including blade servers, from remote locations

- **Windows Event Log and SNMP support** – Store event log messages, issued by Acronis True Image Enterprise Server, to Windows Event Log or send them to SNMP clients

- **Manage System Restore tool** (for Windows 2003 Server and higher) – Turn on/off the Windows native System Restore tool directly from Acronis True Image Enterprise Server

- **Context Help**

1.4 System requirements and supported media

1.4.1 Minimum system requirements

Acronis True Image Enterprise Server requires the following hardware:

- Pentium processor or higher

- 256 Mb RAM

- FDD or CD-RW drive for bootable media creation

- Mouse (recommended).

1.4.2 Supported operating systems

Acronis True Image Management Console

- Windows 98/Me

- Windows NT 4.0 Workstation SP6/2000 Professional SP4/XP Professional SP2

- Windows NT 4.0 Server SP6/2000 Server/2000 Advanced Server/2003 Server

- Windows XP Professional x64 Edition

Acronis True Image Agent for Windows

Acronis True Image Enterprise Server

Acronis Backup Server

Acronis True Image Group Server

- Windows NT 4.0 Workstation SP6/2000 Professional SP4/XP Professional SP2

- Windows NT 4.0 Server SP6/2000 Server/2000 Advanced Server/2003 Server

- Windows XP Professional x64 Edition, Windows Server 2003 x64 Editions

Acronis True Image Agent for Linux

- SuSE 8.0, 8.1, 8.2, 9.0, 9.1, 9.2, 9.3, RedHat 7.3, 8.0, 9.0, Advanced Server 2.1, Advanced Server 3.0, Advanced Server 4.0, Fedora Core 1, Fedora Core 2, Fedora Core 3, Fedora Core 4, Enterprise Server 3.0, Mandrake 8.0, 9.2, 10.0, 10.1, Slackware 10, Debian stable and unstable (sarge), ASPLinux 9.2, ASPLinux 10, ASPLinux 11, ASPLinux Server II, ASPLinux Server IV, Virtuozzo 2.6.x, Gentoo, UnitedLinux 1.0, Ubuntu 4.10, TurboLinux 8.0, TurboLinux 10.0 and some others Linux distributions are supported.

Acronis True Image Enterprise Server bootable standalone version enables backing up and recovery a disk/partition on a computer running any PC-based operating system.

1.4.3 Supported file systems

- FAT16/32
- NTFS
- Ext2/Ext3
- ReiserFS
- Reiser4
- Linux SWAP
- XFS
- JFS

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

For XFS and JFS file systems partition resizing feature is not supported.

1.4.4 Supported storage media

- Hard disk drives
- Networked storage devices such as Storage Area Networks (SANs) and Network Attached Storage (NAS)
- SCSI tape drives
- IDE and SCSI RAID controllers of any level
- FTP-servers*
- CD-R/RW, DVD-R/RW, DVD+R/RW**
- USB 1.0 / 2.0, FireWire (IEEE-1394) and PC card storage devices
- ZIP®, Jaz® and other removable media

* - an FTP-server must allow passive mode for file transfers. Data recovery directly from FTP-server requires the archive to consist of files no more than 2 Gb in size.

** - requires third-party DVD recording software to be installed.

1.5 Technical support

Users of legally purchased copies of Acronis True Image Enterprise Server are entitled to free technical support from Acronis. 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/enterprise/support/

Chapter 2. Acronis True Image Enterprise Server installation and starting

2.1 Installing Acronis True Image Enterprise Server components

To install Acronis True Image Enterprise Server components:

- run the Acronis True Image Enterprise Server setup file

- in the Install Menu, select the program to install: Acronis True Image Management Console, Acronis True Image Agent for Windows, Acronis Backup Server, Acronis True Image Group Server or Acronis True Image Enterprise Server (local version)

- follow the Install Wizard instructions on the screen.
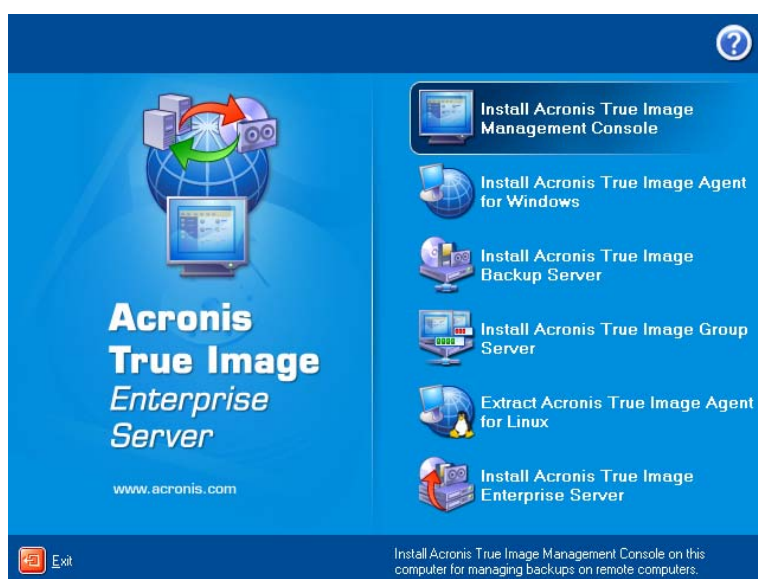
Acronis True Image Enterprise Server Install Menu Window

To install Acronis True Image Agent for Linux, extract its files to a shared network drive or removable media, assign to these files attribute Executable, then perform installation procedure on a Linux-based system.

It is recommended that you install Acronis True Image Management Console first. After that you will be able to install other components remotely to any networked computer.

For Acronis True Image Enterprise Server and Acronis True Image Agent for Windows, **Typical**, **Custom** and **Complete** installation is available. Having pressed **Custom**, you can choose to install, besides the main component, **Rescue Media Builder** and **Bart PE plug-in** for Acronis True Image Enterprise Server, or **Acronis Secure Zone manager** for Acronis True Image Agent.

With **Rescue Media Builder** you can create bootable rescue disks or RIS packages (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, its ISO image or a bootable RIS package at any time from the main program window or running **Bootable Rescue Media Builder** on its own.

Well-known **Bart PE** utility is used to boot Windows-like environment from CD. Applications are installed into Bart PE in the form of plug-ins. Choosing Bart PE plug-in installation

(disabled by default) provides the ability to include Acronis True Image Enterprise Server into Bart PE plug-in tab. The plug-in files will be placed into the component installation folder along with other program files.

Acronis Secure Zone manager lets you create, delete and resize a special hidden partition for storing backup archives (see *3.3 Acronis Secure Zone*).

When installing **Acronis True Image Group Server**, you will have to enter credentials, i.e. user account that will be used for obtaining status of backup/restore tasks from networked computers.

If a domain controller is present on the network, you can create for **Acronis True Image Group Server** a domain user account with Guest rights and remote access right to every computer. If the network does not use domain, you can create accounts with Guests rights on all computers accessed by **Acronis True Image Group Server**.

> When installed, Acronis True Image Enterprise Server (local version) creates a new device in the Device Manager list (**Control Panel -> System -> Hardware -> Device Manager -> Acronis Devices -> Acronis TrueImage Backup Archive Explorer**). Do not disable or uninstall this device, as it is necessary for connecting image archives as virtual disks (see *Chapter 12. Mounting an image as a virtual drive*).

2.2 Extracting Acronis True Image Enterprise Server components

During Acronis True Image Management Console installation, all Acronis True Image Enterprise Server components' setup (.msi) files will be placed to C:\Program Files\Common Files\Acronis\RemoteInstall folder. Thus, you will be able to remotely install, modify or repair the components using Acronis True Image Management Console or **msiexec.exe** utility.

When installing Acronis True Image Enterprise Server components on a local computer, you can save setup files for each Acronis True Image Enterprise Server component separately on a local or network drive. It will help you modify or recover the existing component installation on a local computer.

To save a component's setup file:

- run the Acronis True Image Enterprise Server setup file;
- in the Install Menu, right-click on the component name and select **Extract**;
- select location for setup file and click **Save**.

2.3 Setting up security parameters for Acronis True Image Enterprise Server

2.3.1 Usernames and passwords

Acronis True Image Enterprise Server fully supports all security standards used in Windows.

The remote access to networked computers is allowed according to the security policy set up in the local network. To have remote access to Acronis True Image Agent, the user must be a member of the Administrators or Backup operators group on this computer. To install Acronis components on a remote computer you must be a member of the Administrators group on this computer.

> It is highly recommended that you create an administrator's or backup operator's accounts with the same username and password on all networked computers for remote access to the Acronis True Image Agent.

2.3.2 Firewall setup

Acronis True Image Enterprise Server uses the following ports and IP addresses for remote operation:

- **server (Acronis True Image Agent) UDP port: 9876**
- **server (Acronis True Image Agent) TCP port: 9876, if busy chose port at random**
- **client (Acronis True Image Management Console) UDP port: 9877, if busy chose port at random**
- **IPv4 multicast address: 239.255.219.45**
- **IPv6 multicast address: FF05::fAA5:741E.**

You might have to set the appropriate firewall access options. Options for the Windows Firewall, included in Windows XP Service Pack 2 and Windows 2003 Server, are set automatically during Acronis True Image Enterprise Server components installation. However, make sure that the option **File and Printer Sharing in the Control panel -> Windows Firewall -> Exceptions** is enabled on the remote computer, before the remote operation starts.

2.4 Running Acronis True Image Enterprise Server components

2.4.1 Running Acronis True Image Enterprise Server (local version)

You can run Acronis True Image Enterprise Server in Windows by selecting **Start -> Programs -> Acronis -> Acronis True Image Enterprise Server -> Acronis True Image Enterprise Server** or 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 server bootup, when you see a corresponding message that tells you to press that key. Acronis True Image Enterprise Server will be run in the standalone mode, allowing you to recover the damaged partitions.

If your disk data is totally corrupted and you cannot boot (or if you have not activated Acronis Startup Recovery Manager), load the standalone Acronis True Image Enterprise Server version from the bootable media (supplied with the retail box or created by you using Rescue Media Builder) or RIS-server. Then you will be able to restore the disk from its previously created image.

2.4.2 Running Acronis True Image Management Console

To run Acronis True Image Management Console, select **Start -> Programs -> Acronis -> Acronis True Image Management Console -> Acronis True Image Management Console**.

2.5 Removing Acronis True Image Enterprise Server components

You can remove any Acronis True Image Enterprise Server component separately by selecting **Control panel -> Add or remove programs -> <The component name> -> Remove**. Then follow 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 in this Guide "backups"), that contains a copy of selected files/folders 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, are compressed and stored.

Backing up disks and partitions is performed in a different way: Acronis True Image Enterprise Server 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.

Acronis True Image Enterprise Server stores only those hard disk parts that contain data (for supported file systems). Further, it does not back up swap file information (pagefile.sys) 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.

A partition image includes all files and folders independent of their attributes (including hidden and system files), boot record, FAT (file allocation table) and root.

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 Enterprise Server archives have a ".tib" 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. Mounting an image as a virtual drive*) or start the image restoration and select **Restore specified files or folders**.

3.2 Full, incremental and differential backups

Acronis True Image Enterprise Server 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 as compared to incremental or differential ones.

An **incremental backup** file only contains data changed since the last full or incremental backup creation. Therefore, it is smaller and takes less time to create. But as it doesn't contain all data, all the previous incremental backups and the initial full backup are required for restoration.

Unlike incremental backup, when every backup procedure creates the next file in a "chain," a **differential backup** creates an independent file, containing all changes against the initial full archive. 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 may be an optimal solution if you often roll back the system to the initial state (like in a gaming club or Internet café, to undo changes, made by the guests). In

this case, you need not to re-create the initial full image, so the backup time is not crucial, and the restore time will be minimal.

Alternatively, 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 little as compared to the full data volume.

The same is true for incremental backup. In addition, it is most useful when you need frequent backups and possibility to roll back to any of stored states. 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. However, the cost in time and disk space (or removable media usage) will be as little as one tenth as much.

It is important to note that the above arguments are nothing but examples for your information. Feel free to make up your own backup policy in accordance with your specific tasks and conditions. Acronis True Image Enterprise Server is flexible enough to meet any real-life demands.

> 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 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 archives on the computer system itself. For archive security purposes, ordinary applications cannot access it. In the Acronis True Image Enterprise Server Wizards' windows the zone is listed along with all partitions available for storing archives. Acronis Secure Zone is necessary for using Acronis Startup Recovery Manager and Acronis Snap Restore features (see below).

Acronis Secure Zone is always available for archive creation as long as there is space for the backup file. If there is not enough space, older archives will be deleted to create space.

Acronis True Image Enterprise Server uses the following scheme to clean up Acronis Secure Zone:

- If there is not enough free space in the zone to create a backup, the program deletes the oldest full backup with all subsequent incremental/differential backups.

- If there is only one full backup (with subsequent incremental/differential backups) left and a full backup is in progress, then the old full backup and incremental/differential backups are deleted.

- Otherwise, (only one full backup left, and an incremental/differential backup is in progress) you will get a message about space error. In that case you will have to either re-create the full backup or increase Acronis Secure Zone.

Thus, you can back up data automatically on a schedule (see *Chapter 8. Scheduling tasks*), and not worry about zone overflow issues. However, if you keep long chains of incremental backups, it will be a good practice to periodically check the zone free space, indicated on the second page of the **Manage Acronis Secure Zone** wizard.

How to create, resize or delete Acronis Secure Zone using this wizard, see in *Chapter 9. Managing Acronis Secure Zone*.

3.4 Acronis Startup Recovery Manager

3.4.1 How it works

The Acronis Startup Recovery Manager enables starting Acronis True Image Enterprise Server on a local computer without loading the operating system. With this feature, if the operating system won't load for some reason, you can run Acronis True Image Enterprise Server by itself to restore damaged partitions. As opposed to booting from Acronis removable media or RIS server, you will not need a separate media or network connection to start Acronis True Image Enterprise Server. It is especially handy for traveling users.

3.4.2 How to use

To be able to use Acronis Startup Recovery Manager at boot time, prepare as follows (you can do it either locally, using Acronis True Image Enterprise Server local version, or remotely, using Acronis True Image Management Console):

1. Install Acronis True Image Enterprise Server local version or Acronis True Image Agent on a local computer.

2. Create Acronis Secure Zone on the local computer 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 while Acronis Secure Zone is missing from the system, you will be prompted to create the zone, then Acronis Startup Recovery Manager will be activated. Otherwise, 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 failure occurs on a local computer, turn on the computer and press F11 when you see the "Press F11 for Acronis Startup Recovery Manager" message. This will run a standalone version of Acronis True Image Enterprise Server that only slightly differs from the complete version. For information on restoring damaged partitions, see *Chapter 7. Restoring the backup data*.

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

3.5 Acronis Backup Server

This software application, when installed on a networked computer, automatically manages backup archives, stored on this computer, in accordance with the rules, set by an administrator. Acronis Backup Server allows the administrator to set up a uniform backup policy for the entire organization. It ensures optimal employment of storage space, used for backup archives. Outdated archives will be automatically deleted; at the same time, the latest data recovery is always possible. In addition, Acronis Backup Server facilitates creation and executing group backup tasks.

3.5.1 Backup locations, their quotas and time limits

Backup server is a networked computer where Acronis Backup Server is installed. A backup location is an automatically managed storage area for backups on a backup server. An administrator can organize one or more backup locations and set the overall limitations to size/storage time for every location, i.e. quotas and time limits. An administrator can **Move, Clear** or **Delete** existing backup locations or edit their **Quotas and time limits**.

3.5.2 Quotas and time limits for computers and users

Individual quotas and time limits determine every computer's or user's quota on a backup server. This include

1) maximum storage space, allocated to a user/computer, in Mb

2) maximum number of backups

3) maximum number of incremental backups for each full backup

4) maximum storage period for the user's/computer's archives.

These values define how Acronis Backup Server itself will handle the backup archives.

At first backup of the computer/user's data to the backup server, a full backup will be created. The next backups will be incremental, until the maximum number of incremental backups is reached. Then again a full backup and a set of subsequent incremental backups is created, then again a full backup and so on.

> As appears from the above, when backing up to backup server, a user cannot select backup mode (full, incremental, differential). The backup mode will be set by Acronis Backup Server.

> Please be aware, that in fact maximum number of incremental backups includes one initial full backup. For example, if this parameter is set to 5, Acronis Backup Server will create one full backup, then four incremental backups, then again a full backup and so on. For this reason, this parameter is also called "maximum number of backups in an archive". Archive here means a set of subsequent incrementals and the base full backup.

When number of backups or storage space exceeds the preset value, Acronis Backup Server will combine the first full backup with the next incremental one into one full backup. Then, if necessary, this backup will be combined with the next, until the occupied storage space (or number of backups) decreases to the limitation. Thus, the archive integrity will not be affected, in spite of the fact that one backup will disappear. This procedure is called *automatic consolidation*.

When storage period expires, Acronis Backup Server will delete the outdated archives without notification.

An administrator can run a check of meeting the limitations on a schedule (once, daily, weekly or monthly). All user's/computers archives on the backup server will be checked and, if some quotas and time limits are exceeded, the above processing will be executed.

3.5.3 Administrator profiles and User profiles

Profile is a set of parameters, assigned to each computer and user that backs up on the backup server. Profile includes the backup location and the above limitations. When an administrator adds a new computer or user to Acronis Backup Server database, they are assigned the default backup location, quotas and time limits. An administrator then can change these settings by editing the respective profile.

Administrator profiles are used for managing backups, created by backup tasks, remotely controlled from Acronis True Image Management Console.

An administrator assigns a backup location and sets quotas and time limits for each computer running Acronis True Image Agent. After that, when creating an individual or group backup task, he will specify the backup server as the target storage place, and every computer's backup will be directed to the assigned location, which may differ from other computers' location or be the same.

So, Administrator profiles manage the backup server resources allocation by computers.

User profiles are used for managing backups, created by backup tasks, locally controlled with Acronis True Image Enterprise Server.

An administrator assigns a backup location and sets quotas and time limits for each user, who back up their data running Acronis True Image Enterprise Server (local version). Later on, if the user specifies the backup server as the target storage place, his backup will be directed to the assigned backup location. If the user moves to another computer, his backup location, quotas and time limits remain the same.

So, User profiles manage the backup server resources allocation by users.

3.5.4 Operations with archives

Acronis Backup Server can display a list of backups, stored on the backup server, and sort the list by **Location** or **Owners** (users and computers).

An administrator, if need be, can manually **Consolidate** any backup (except for the oldest one in the archive) with the preceding backup file. The resulting file will preserve all data changes, contained in both files and have the latest backup date. Thus, the archive integrity will not be affected, in spite of the fact that one backup will disappear. Data recovery from any of the remaining backups will be possible.

3.6 Acronis Snap Restore

With this feature you can boot the OS on the crashed computer before the system is completely restored from an image, and start the work seconds after the restoration is launched. The restoration will be continued in the background.

This feature is currently available for images, being restored from the Acronis Secure Zone (see above). Naturally, Acronis Snap Restore cannot be used if the image contains no operating system (a logical partition or disk image) or when restoring file archives.

3.6.1 How it works

When the restoration procedure is started, Acronis True Image Enterprise Server:

1. Finds the sectors in the image, containing system files, and restores these sectors first. Thus, the OS is restored and can be started in a very short timeframe. Having started the OS, the user sees the folder tree with files, though file contents still is not recovered. Nevertheless, the user can start working.

2. Writes on the hard disk its own drivers, capable to intercept the system queries to the files. When the user opens files or launches applications, the drivers receive the system queries and restore the sectors that are necessary for the current operation.

3. At the same time, ATIES proceeds with the complete sector-by-sector image restoration in the background. However, the system requested sectors have the highest priority.

Finally, the image will be fully restored even if the user performs no actions at all. But if you choose to start working as soon as possible after the system failure, you will gain at least several minutes, considering that restoration of a 10-20 Gb image (most common image size) takes about 10 minutes. The larger the image size, the more time you save.

3.6.2 How to use

To be able to use Acronis Snap Restore in case of system crash, prepare as follows (you can do it either locally, using Acronis True Image Enterprise Server local version, or remotely, using Acronis True Image Management Console):

1. Install Acronis True Image Enterprise Server local version or Acronis True Image Agent on a local computer.

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

3. Activate Acronis Startup Recovery manager (see *3.4 Acronis Startup Recovery Manager*) and create bootable media or RIS package with Acronis True Image Enterprise Server (see *Chapter 10. Creating bootable* media).

4. Back up (image) the local computer's system disk to Acronis Secure Zone (see *6.2 Backing up disks and partitions (image backup)*). You can back up other disks/partitions as well, but the system image is mandatory.

> When performing Snap Restore, the current Acronis True Image Enterprise Server version always restores the entire system disk. Therefore, if your system disk consists of several partitions, all of them must be included into the image. Otherwise partitions, missing in the image, will be lost.

If failure occurs, boot the local computer from the bootable media, or RIS server, or using F11. Start the recovery procedure (see *7.3 Restoring disks/partitions or files from images*), select the system disk image from Acronis Secure Zone, choose **Use Snap Restore** and in the next window click **Proceed**. In a few seconds the computer will reboot to the restored system. Log in and work – no more reboots or other actions required.

You can perform Snap Restore running Acronis True Image Enterprise Server in supported Windows Server operating systems as well. However, it is mandatory to have a bootable media in case of Windows cannot boot.

3.7 Acronis Universal Restore

One of the fastest ways of cloning a Windows system is to deploy its image to a different computer.

However, the deployment will not be a success if the target hardware is incompatible with the most critical drivers included in the image. The restored system may be unbootable because startup drivers and components, used by the source system, cannot operate on a different motherboard, processor etc.

> Using Microsoft System Preparation Tool (sysprep) does not solve this problem, because Sysprep allows replacing drivers only for Plug-and-Play devices (sound cards, network adapters, video cards etc.). As for system HAL and boot device driver, they must be identical in the source and target computers (see Microsoft Knowledge Base, articles 302577 and 216915).

Acronis Universal Restore technology provides an efficient solution for hardware-independent system restoration by replacing the crucial HAL and hard disk controller drivers.

Acronis Universal Restore does not conflict with Microsoft System Preparation Tool (sysprep). If you got accustomed to using Sysprep, you can use both tools on the same system.

Acronis Universal Restore is an optional program feature. It should be purchased separately and installed from a separate .msi setup file. Acronis Universal Restore can only be installed on a computer where at least one of the following Acronis components is installed:

Acronis True Image Agent for Windows

Acronis True Image Enterprise Server (local version)

Bootable Media Builder.

3.7.1 How to use

You can perform the following procedure either locally or remotely, using Acronis True Image Management Console.

1. Boot the target computer into Acronis recovery environment from the bootable media, or RIS server, or using F11.

2. Start the recovery procedure (see *7.3 Restoring disks/partitions or files from images*) and select the image of the source computer for restoration.

3. You can specify Hardware Abstraction Layer (HAL) and hard disk controller drivers to be used by the restored system and/or provide a path to a driver repository on the network.

Hence, Acronis Universal Restore uses three sources for drivers search: the list of user-specified (enforced) drivers, driver repository, and the Windows default driver storage folders (in the image being restored). The program will find the most suitable drivers of all available and install them into the restored system. However, the user-defined drivers will have the priority. They will be installed, with appropriate warning, even if the program finds the better driver.

The Windows default driver storage folders are determined in the registry key SOFTWARE -> Microsoft -> Windows -> Current version -> DevicePath. Generally, it is WINDOWS/inf folder.

4. When the restore process runs Acronis True Image Enterprise Server will:

- detect the machine type and install appropriate driver for HAL

- detect IDE and SCSI controllers and install appropriate drivers. If no appropriate drivers are found in all three above sources, the user will be prompted to browse the following locations for the drivers:

Network share drive

Floppy disk

CD drive

5. The machine reboots.

6. Windows takes control and initiates the usual first-start process.

The recovery procedure can proceed under Windows as well (for example, if the operating system is loaded from the C: drive, the system partition of the other computer can be restored from an image to the D: drive). In this case, the user prompt for driver search on Network-Floppy-CD will not be issued. If a compatible driver cannot be found, Windows will suggest to ignore it or cancel restoration.

3.7.2 Using Acronis Universal Restore in virtual environment

Virtual machine technologies provide a powerful tool to help accelerate the development, testing, deployment and support of PC applications. Using Acronis True Image Enterprise Server with Acronis Universal Restore you can perform real-to-virtual and virtual-to-real computer migration in the same way as with real systems.

If the virtual hard drive uses SCSI controller, you should provide appropriate drivers while performing system restore to the virtual machine. For example, the widespread VMware environment requires Buslogic or LSI logic drivers. Use drivers bundled with your virtual machine software or download the latest drivers versions from the software manufacturer website.

3.7.3 Hints on using Acronis Universal Restore

1. The system recovered by Acronis Universal Restore may not start if the partition structure in the image or the target disk partitioning does not coincide with that of the source disk. As a result, the loader, restored from the image, will point to the wrong partition and the system will not boot or will malfunction.

Such might be the case if you:

- image not the entire source disk, but only the selected partitions

> Keep in mind, that the source disk may have a hidden maintenance partition created by the computer vendor. Therefore, if you check each partition for backup instead of checking the disk, this hidden partition will not be included into the image.

- restore not the entire source disk, but only the selected partitions. In some cases, especially if your system resides on other than the first partition, this can confuse the loader and prevent the restored system from startup

- image the system residing on the RAID array and restore the system to a RAID array with different configuration.

To avoid the problem, we recommend that you image and restore the entire system disk and use the identical RAID configuration on the source and the target computer.

2. As appears from the above, a bootable system migration from RAID to HDD and vise versa is impossible.

3. When migrating from RAID to RAID, be sure to provide an appropriate driver for the RAID controller, otherwise a basic HDD driver will be installed.

4. Acronis Universal Restore option is not available when restoring dynamic disks and volumes.

3.7.4 Benefits

1. Acronis Universal Restore can be used "after the fact": it is not necessary to create an image with the option, you can restore any image to different hardware.

2. Acronis Universal Restore allows the user to exactly specify drivers during restore, enabling their maximum compatibility with the hardware.

3. Acronis Universal Restore does not strip security identifier (SID) and user profile settings. This means that you will not need to re-join your domain or re-map network user profiles after a restore.

4. Acronis Universal Restore supports a driver repository to centrally store all drivers so users don't need to go looking for them.

3.8 Using dynamic disks and volumes

Acronis True Image Enterprise Server supports Windows LDM (also called Dynamic Disks). However, as dynamic disks are organized differently than basic, physical disk drives, their backup has some peculiar features.

You can create an image of the entire dynamic disk or one or more dynamic volumes. This is because a dynamic volume is located on several dynamic disks, so a partial backup would not create a usable image.

The current version of the software is not capable of changing the volume size and file system when an image is being restored to a dynamic volume. However, this is possible when you restore a dynamic volume to a basic disk partition.

When you create a dynamic volume image, its type information (simple, mirror, and the like) is lost, so the restoration is performed independently. In each case, the program stores and restores volume contents only.

If a basic disk image is restored to a dynamic disk, it will destroy the dynamic disk's contents. As a result, you will end up with a basic disk.

If Acronis True Image Enterprise Server runs in rescue mode (for example, booted from Bootable Rescue media), dynamic disks will be not accessible. Therefore, to be able to repair a system partition, you must keep its image on a basic, network, or removable disk.

3.9 Backing up to tape drive

Acronis True Image Enterprise Server supports SCSI tape drives. It can store backups on the tape and restore data from the tape, store large backups to multiple tapes, and append incremental/differential changes to a tape with the existing archives.

If a SCSI tape drive is connected to the computer, controlling the backup process (i.e. where you are running Acronis True Image Management Console or Acronis True Image Enterprise Server local version) the list of devices available for backup storage will be extended with a name corresponding to the drive type.

To place backup archives on a tape drive, connected to another network computer, install Acronis Backup Server on that computer. Then a new device type Acronis Backup Server will appear in the list of devices, and you will be able to access the tape under this device.

Backup and restore on the tape proceed in the same way as with other devices, with the following exceptions.

1. A full backup can be stored on an empty tape only. If you use tape that already contains data, its contents will be overwritten.

2. In case you want to keep more than one archive on the tape, for example, back up two disks separately, choose *incremental* backup mode when creating initial *full* backup for the second disk. In other situations, incremental backup is used for appending changes to the previously created archive.

3. You do not have to provide filenames for backups.

You might experience short pauses that are required to rewind the tape.

Low-quality or old tape, as well as dirt on the magnetic head, might lead to pauses that can last up to several minutes.

3.10 Viewing disk and partition information

You can change the way of data representation 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 last duplicated in the context menu invoked 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 **Arrange Icons by** button and select the column.

To select columns to view, right-click the headers line or left-click the **Choose Details** button. Then flag the columns you want to display.

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 columns by dragging their borders with the mouse.

Chapter 4. Using Acronis True Image Management Console

4.1 General information

Acronis True Image Management Console is the primary tool for managing data backup/restore on remote computers where Acronis True Image Agent is installed. The Console allows managing computer groups and corporate backup archives via Group and Backup Servers, as well as managing individual backup/restore tasks for every computer.
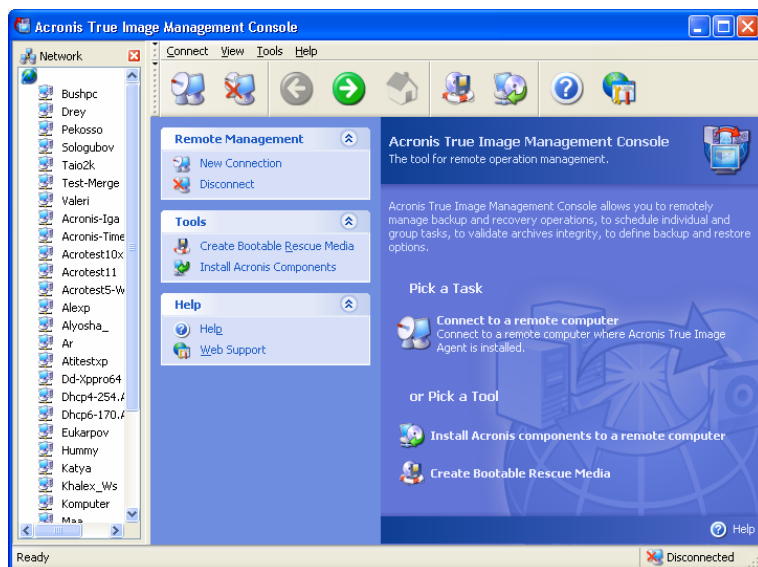
Acronis True Image Management Console main window with the Network pane active

4.2 Installing/updating Acronis components on a remote machine

Acronis True Image Management Console allows installing, updating or removing Acronis True Image Enterprise Server components on remote computers. To perform any of these operations you will need administrator rights on the target machine.

> If the remote computer runs Windows XP, the option **Control panel -> Folder options -> View -> Use simple file sharing** must be disabled on that computer.

> If the remote computer runs Windows XP with Service Pack 2 or Windows 2003 Server, the option **Control panel -> Windows Firewall -> Exceptions -> File and Printer Sharing** must be enabled on that computer.

To install Acronis components:

1. Click **Install Acronis components to a remote computer** in the center of Acronis True Image Management Console main window, on the toolbar or the sidebar, or select the same item from the **Tools** menu.

2. Select the installer location from the list (**Registered Components**, **Search removable media** or **Specify location**). The default selection **Registered Components** will use setup files from the default C:\Program Files\Common Files\Acronis\RemoteInstall folder.

3. Select the Acronis component and specify the component features you want to install (for custom component features see *2.1   Installing Acronis True Image Enterprise Server components*).

Copyright © Acronis, Inc., 2000-2006
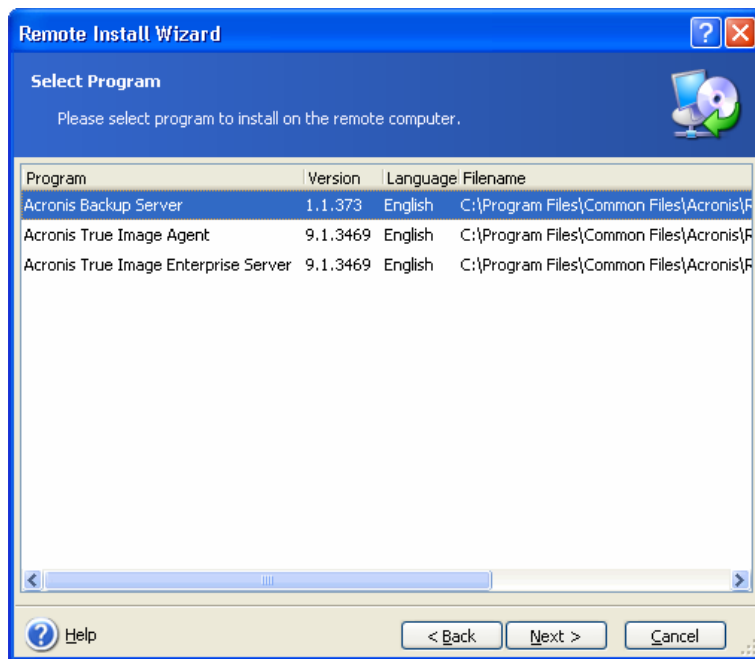
4. Specify network name or IP address of the machine on which Acronis component is to be installed. You can also select the machine from the list of available using **Browse...** button. At that point you will have to provide administrator username and password.

Acronis True Image Agent and Acronis True Image Enterprise Server installation requires the system restart. To allow immediate remote computer reboot, check the **Reboot the remote computer** box.

5. The Acronis component then will be installed on the remote computer. If system restart is necessary, the remote machine will reboot or the program will prompt you to restart the remote machine, depending on your choice on the previous step.

To update, repair, modify or remove an Acronis component on a remote computer, start the same procedure and select the desired action in appearing windows.

4.3 Managing a single remote computer

To perform any operation on a single remote computer, you must first connect to it.

4.3.1 Connecting to a remote computer

To establish a remote connection:

1. Click **Connect to a remote computer** in the center of Acronis True Image Management Console main window or on the toolbar, or select **New connection** from the sidebar or the **Connect** menu.

2. Enter the computer network name or select it using **Browse...** button. **Browse...** will open a list, including all computers controllable with Acronis True Image Management Console.

3. Enter administrator or backup operator username and password.

After connection is established, in the central part of Acronis True Image Management Console main window you will see a list of operations available:
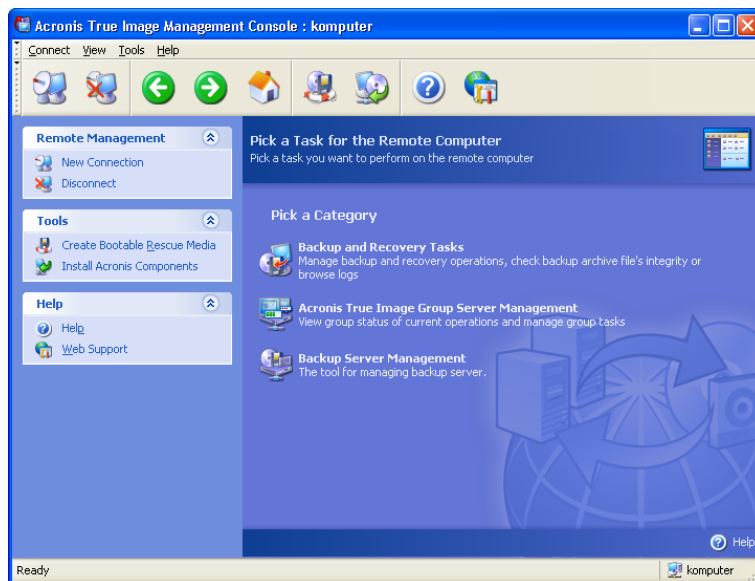
Main window of Acronis True Image Management Console when connected to a remote computer

The task list content depends on the programs installed on the connected computer. The most populated list will include managing **Backup and Recovery Tasks** (via Acronis True Image Agent), **Group Server Management** (via Acronis True Image Group Server) and **Backup Server Management** (via Acronis Backup Server).

4.3.2 Backup and recovery tasks

After clicking on **Backup and Recovery Tasks** the program window turns to the following appearance:
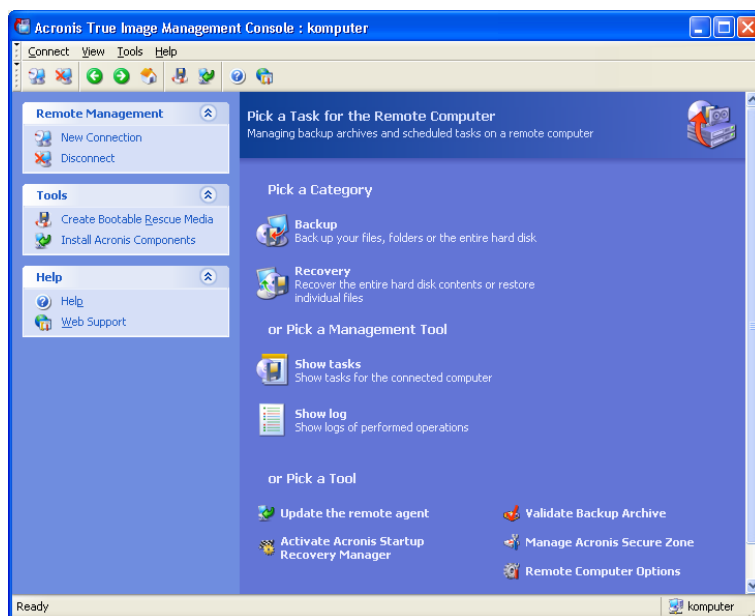
You can perform the following operations on the remote computer.

- **Backup and restore data, including system disks/partitions**

Click **Backup** or **Recovery**, then follow the Wizard's instructions. See details in *Chapter 6. Creating backup archives* and *Chapter 7. Restoring the backup data.*

- **Schedule backup operations**

Click **Show tasks -> Manage**, then follow the Wizard's instructions. See details in *Chapter 8. Scheduling tasks*.

- **Set up backup/restore options,** such as system/network resources usage, before/after backup commands etc.

Click **Remote Computer Options**, select **Default backup options** or **Default restoration options** and make settings. See details in *6.3 Setting backup options* and *7.4 Setting restore options.*

- **Validate backup archives wherever they reside, be it local, network or removable media**

Click **Validate Backup Archive**, then follow the Wizard's instructions. See details in *11.1 Validating backup archives*.

- **Set up sending notifications about Acronis True Image Agent operation and tracing** this operation in Windows Application Event Log

Click **Remote Computer Options**, select **Notifications** or **Event tracing** and make settings. See details in *11.2 Operation results notification* and *11.4 Event tracing*.

- **Browse logs of Acronis True Image Agent operation**

Click **Show log**. See details in *11.3 Viewing logs*.

- **Manage Acronis Secure Zone**

Click **Manage Acronis Secure Zone**, then follow the Wizard's instructions. See details in *Chapter 9. Managing Acronis Secure Zone*.

- **Activate Acronis Startup Recovery Manager**

Click **Activate Acronis Startup Recovery Manager**, then follow the Wizard's instructions. See details in *3.4 Acronis Startup Recovery Manager*.

- **Update the remote agent**

Click **Update the remote agent**, then follow the Wizard's instructions. The procedure is the same as described in *4.2 Installing/updating Acronis components on a remote machine*

After you perform all necessary operations on the remote computer, select **Disconnect** or **New connection** on the toolbar, sidebar or the **Connect** menu.

4.4 Managing groups of computers

4.4.1 Group server management

When connected to a remote computer where Acronis True Image Group Server is installed, click **Acronis True Image Group Server management** to display the following window.
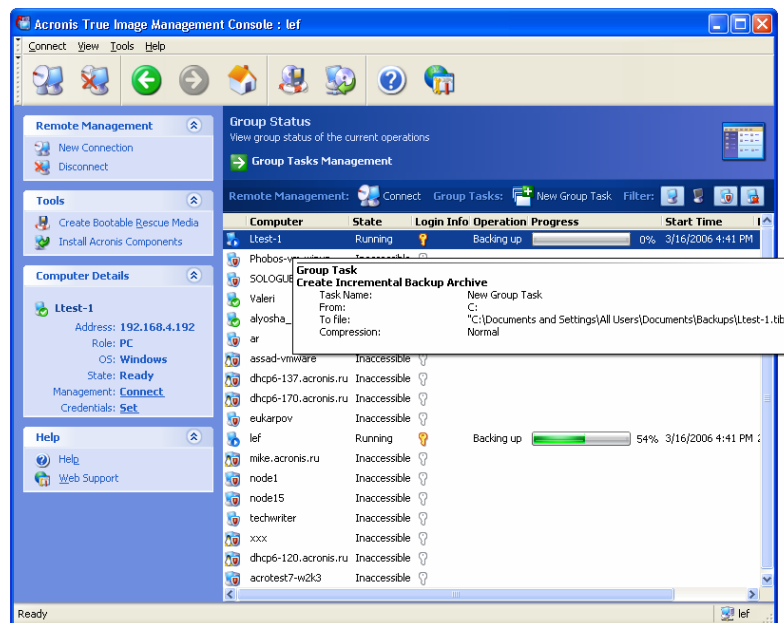
Here you can monitor states of Acronis True Image Enterprise Server tasks (backup, restore, validating backup archives) on all networked computers:

Ready – the remote computer is available for the next task

Prepare - preparations are being made on a remote machine for the task execution (analyzing partitions, preparing backup scripts, etc.)

Running – a task is being executed on the remote computer

Paused – the task is paused and waiting for user input on the remote computer

Failed – the task could not be completed because of an error

Finished – the task has been completed successfully

Cancelled – the task has been cancelled on the remote computer

Offline - the remote computer is not connected to the network, or switched off

Inaccessible - the remote computer is not accessible due to lack of access rights, firewall and security settings, etc.

Unmanaged - the Acronis True Image Agent is not installed on a remote machine.

To see details of the computer in brief (the computer role, operating system and IP-address), click on the computer name. The details are displayed on the sidebar.

To see details of the group task being executed on a remote computer, mouse over the computer.

In this window you can also:

1. Filter out from the list offline, inaccessible or unmanaged computers and vice versa, filter out online computers to see those that cannot be managed (use buttons in the **Filter** group).

2. Input and test credentials for access to each computer. To do so, click on the key icon, enter username and password and click **Test connection**. The program will issue a message displaying the test result. Key icons for successfully tested connections are colored gold.

3. Create a disk/partition backup task for several remote computers at once (see *4.4.2 Creating new group backup tasks*).

4. Connect to a remote computer to see the operation log, start or edit tasks for this computer etc. (see *4.3 Managing a single remote computer*). To do so, select a computer and click **Connect**.

5. Invoke **Group tasks management** window for viewing, deleting or rescheduling group tasks.

4.4.2 Creating new group backup tasks

You can create a disk/partition backup task for several remote computers at once. File-level backup for groups of computers is unavailable.

1. In **Group status** or **Group tasks management window**, select **New Group Task** on the toolbar. **Create Group Task Wizard** window appears to guide you through the task creation procedure.

2. Form a group for the current task: check computers in the list of remote computers.

3. Select disks/partitions to backup. You can select any combination of hard disks (by number, according to Windows numeration) and partitions (by letter); or **All hard disks**. This setting is applied to every computer in the group, so having a standard (similar) disks/partitions layout on remote computers would be a plus.
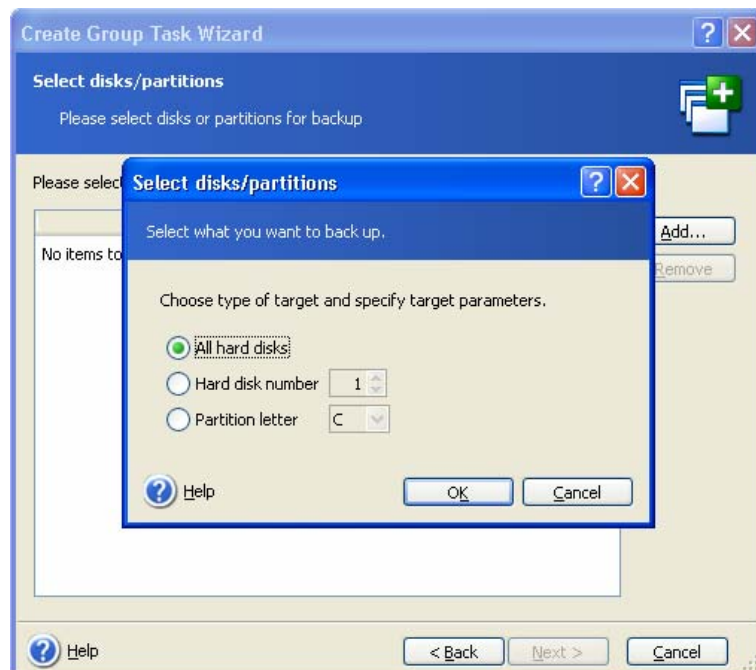
Select disk/partitions to backup

4. Specify a path to backup archive. To place every archive on its local computer, input **Local path** or select **Acronis Secure Zone**, if there is such zone on every remote computer. For more information about Acronis Secure Zone see *3.3 Acronis Secure Zone*. To place backups on the network, check **Network path**, select the target folder and specify the username and password for access to the network drive. When backing up to a backup server, choose **Personal Backup Location** or tape drive and enter backup server administrator's credentials. For more information about backup servers see *3.5 Acronis Backup Server*.

You should also provide the archive name for each computer, unless the archives are targeted to Acronis Secure Zones or a backup server. Pressing the button to the right of name input field will assign to each archive the respective computer's name.

5. Specify usual backup settings: backup mode (full, incremental or differential), a password to backup archive (if necessary), default or custom backup options and comment. For more information see *Chapter 6. Creating backup archives*.

6. Provide a name for the group task. The name will be displayed in the **Group Tasks Management** window (see below) to allow quick task identification.

7. Select when you would like the task to be started. The scheduling procedure is almost the same for individual and group tasks, see *Chapter 8. Scheduling tasks* for details.

8. If, for any reason (traffic limitation, for example), you do not want the task to start on all computers simultaneously, set **Start time shift** parameter. The task will start on all computers in turn, with time shift you specify. As soon as you select time shift, the resulting task start time for the first and the last computer will be displayed.

9. Now enter the username and password. It is supposed, that accounts with same username and password exist on all computers of the group. In this case, the task will be automatically distributed to computers. Otherwise, you will be asked for username/password to every computer in process of distribution.

10. At the final step, group task script is displayed. Up to this point, you can click **Back** to make changes in the created task.
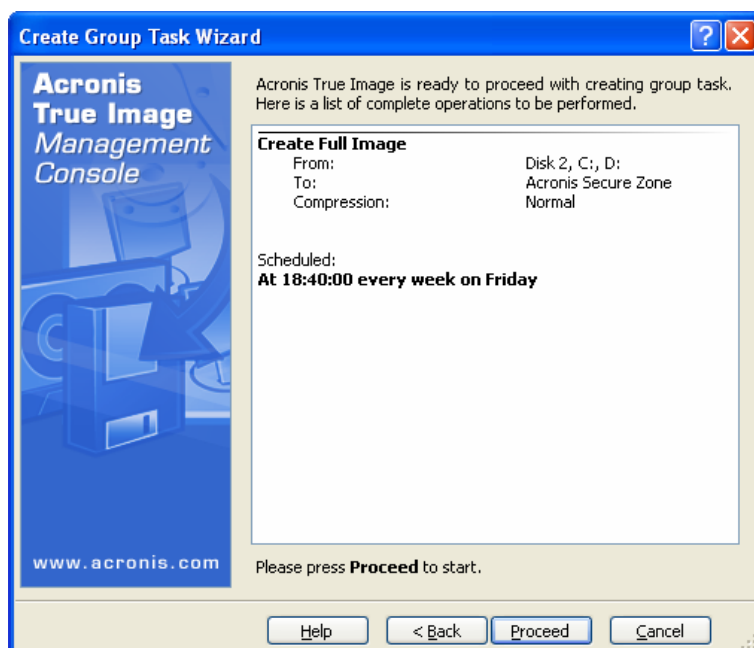
Group task script

11. After you click **Proceed**, Acronis True Image Management Console connects to every computer of the group in turn to distribute the task. If a remote computer is inaccessible (shut down, for example), a dialog box appears. In this box, choose **Ignore** to exclude the computer from the group or **Cancel** to cancel the entire task.

When distribution is completed, the group task appears in **Group Tasks Management** window. If you connect to any computer included into the group, you will see its individual task, based on the group task you successfully created.

4.4.3 Group tasks management

The **Group Tasks Management** window displays the list of group tasks.

To see details of a group task, click the button to the left of the task name. To create new or delete existing backup task, use the **New Group Task** and **Delete Group Task** items.

When deleting a group task, enter the same username and password you entered when created the task.
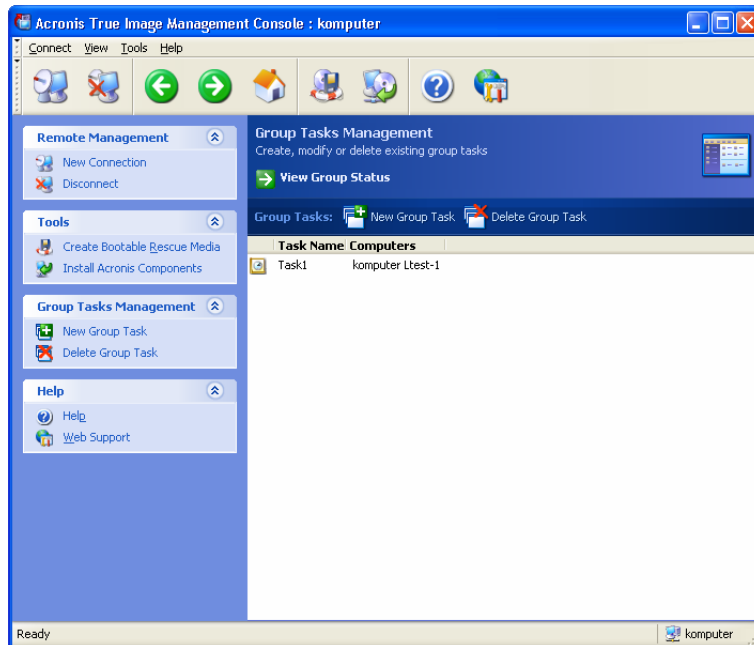
4.5 Managing backup server

Before you start managing the backup server, be sure to read section *3.5 Acronis Backup Server* stating the basic operating principles of this component.

When connected to a remote computer where Acronis Backup Server is installed, click **Acronis Backup Server management** to display the following window.
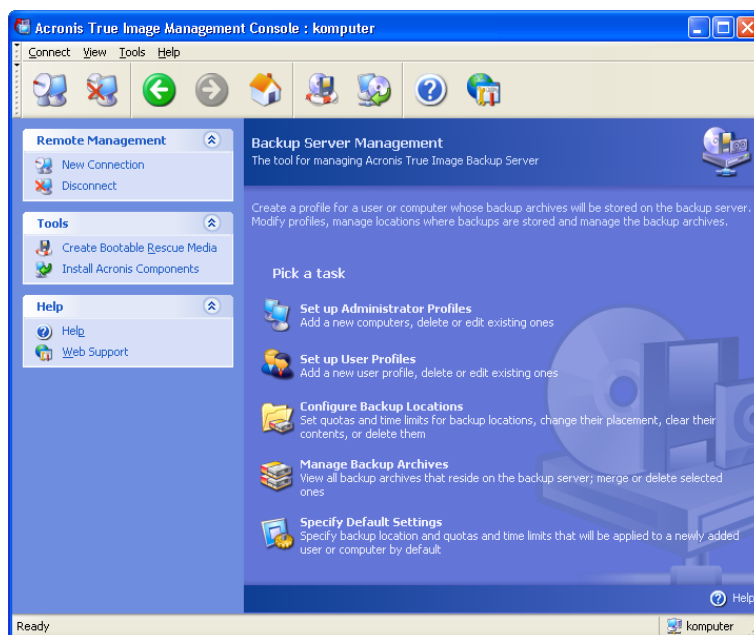
4.5.1 Default settings

Each user or computer, added to Acronis Backup Server database, is associated with the default backup location and the default user/computer quotas and time limits.

When installed on a computer (which becomes a backup server from this point on), Acronis Backup Server creates the following folder:

C:\Documents and Settings\All Users\Application Data\Acronis\BackupServer.

This folder is a default backup location.

You can change the default backup location and its quotas/time limits by selecting **Specify Default Settings -> Set backup location** and entering the desired location and values. Changing the default backup location will direct backups of newly added users/computers to another folder, while users/computers associated with old default backup location will continue back up to the old place. Thus, a new backup location is created.
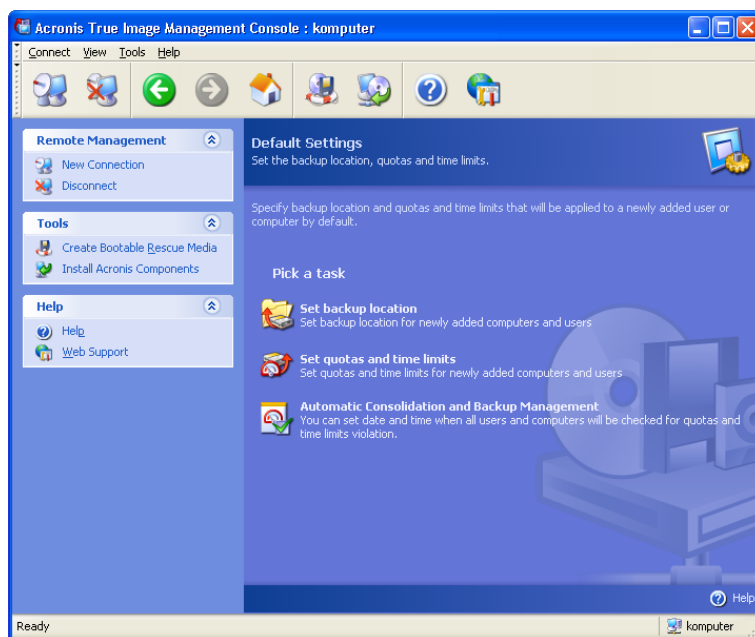
The default quotas/time limits are preset to **Unlimited**, except for **Maximum number of backups in an archive**, which is set to 5 (the largest value of this parameter is not limited, but it is recommended that you do not set unreasonably large values).

Maximum number of backups in an archive means maximum number of incremental backups plus one initial full backup. For example, if this parameter is set to 5, Acronis Backup Server will create one full backup, then four incremental backups, then again a full backup and so on. Archive here means a set of subsequent incrementals and the base full backup.

You can change the default user/computer quotas/time limits by selecting **Specify Default Settings -> Set Quotas/Time limits** and entering the desired values.
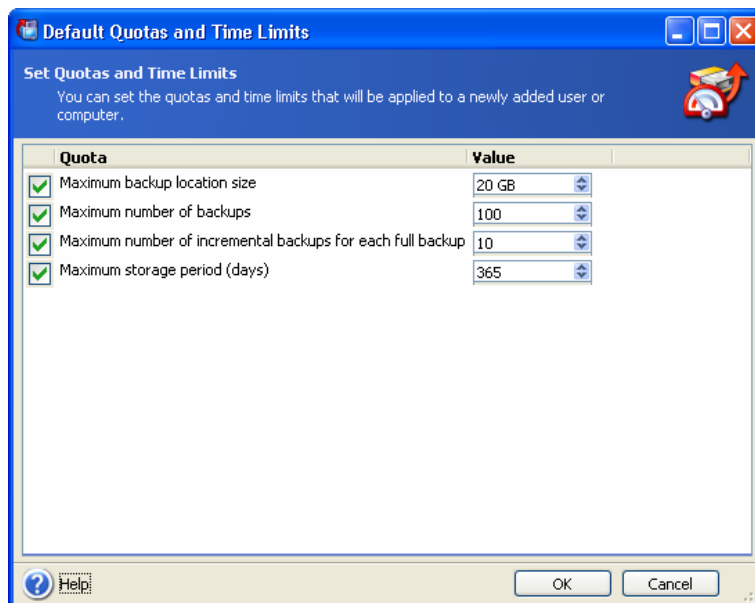
To enable Acronis Backup Server to process archives, schedule quotas/time limits check task. Select **Specify Default Settings -> Schedule Automatic Consolidation and Backup Management** and schedule one-time, daily, weekly or monthly check of all user's/computers archives on the backup server for meeting limitations. If the check reveals that some of quotas/time limits are exceeded, the archive processing described in *3.5.2 Quotas and time limits for computers and users* will be executed.

> Please take note of the fact that checking limitations has no sense if you have not changed at least one of the preset **Unlimited** values for quotas/time limits.

4.5.2 Set up Administrator profiles

To be able to remotely back up data from a networked computer where Acronis True Image Agent is installed, to backup server, add this computer to Acronis Backup Server database. Click **Set up Administrator profiles -> Add**, select the computer and specify backup location, quotas and time limits for this computer in **Add Computer Profile Wizard** windows.
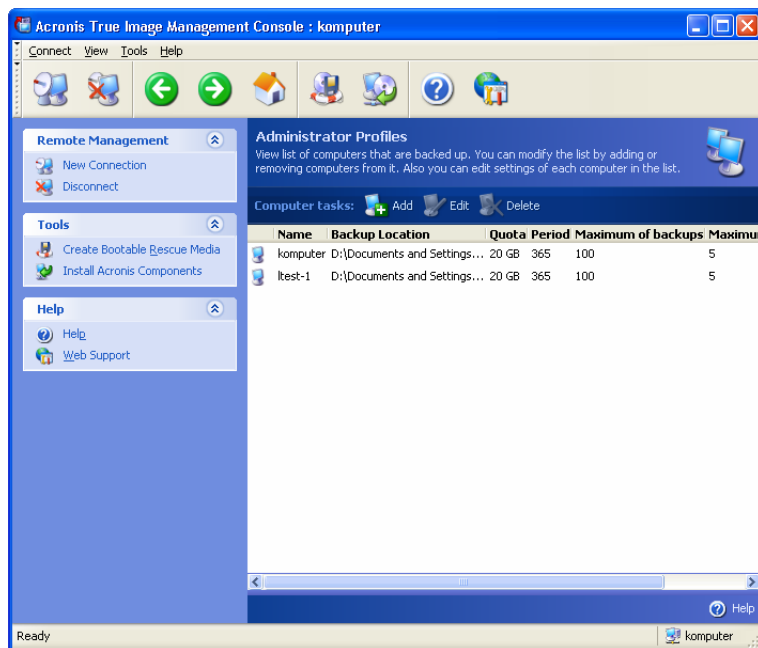
You can use the default backup location, quotas and time limits or make particular settings for the new computer. If you specify a new path to backup location for the new computer, a new backup location will be created.

You might need to change a computer profile already set. To do so, select the computer and click **Edit.** The **Edit Computer Profile Wizard** will guide you through the same selections, as the **Add Computer Profile Wizard.**

Changing the computer backup location will move all existing and redirect future backups of this computer to another folder (device etc.). As moving files may take a lot of time and system resources, it is recommended that you schedule this operation for the time when the backup server computing load will be minimal. You can do it in the **Start Parameters** window. To complete configuring the profile, click **Finish** in the final summary window.

To change a computer backup location within the same device, you must have at least as much free space on the device as the computer archives occupy, because the archives will first be copied to the new location, and then deleted from the old place.

If you select a computer and click **Clear**, all archives of this computer data will be deleted.

Deleting a computer profile will disable backup to backup server for this computer and delete its existing archives. This operation might also be time-consuming, so you can schedule it for the off-peak period.

4.5.3 Adding Users and Administrators to Acronis Backup Server database

When installed, Acronis Backup Server creates on the backup server a user group named AcronisBackupServerUsers (see **Control Panel -> Administrative Tools -> Computer Management -> Local Users and Groups**). At this point, the group contains the only user who installed the program.

By default, this user is able to manage the backup server and perform backups on base of computer profiles, i.e. has administrator's rights on the backup server.

To enable any user to back up data from any networked computer, where Acronis True Image Enterprise Server local version is installed, to backup server, an administrator should add this user to Acronis Backup Server database.

To do so, first, add this person to AcronisBackupServerUsers group. Then click **Set up User profiles -> Add**, select the user name and specify backup location, quotas and time limits for this user in **Add User Profile Wizard** windows. Use the default backup location, quotas and time limits or make particular settings for the new user. If you specify a new path to backup location for the new user, a new backup location will be created.
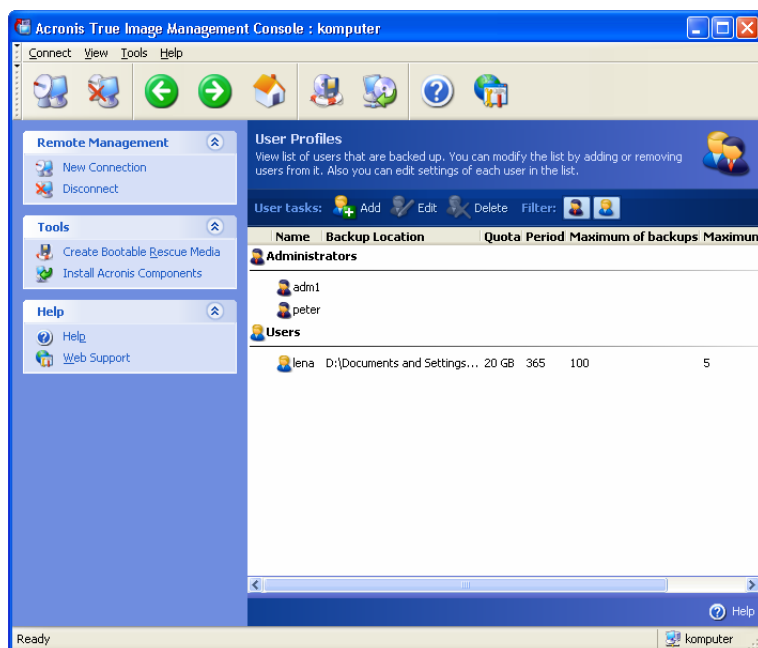
To add another administrator, first add this person to AcronisBackupServerUsers group. Then click **Set up User profiles -> Add**, select the user name and choose **Create user with administrator's rights** on the next page.

An administrator can manage all archives on the backup server regardless of their owner, while a common user can only backup or restore his data from the backup server. An administrator has no user profile, in other words, he is not assigned a backup location, quotas and time limits like common users are. He uses administrator profile for both remotely and locally controlled backups.

4.5.4 Changing User profiles

You might need to change a user profile already set. To do so, select the user and click **Edit.** The **Edit User Profile Wizard** will guide you through the same selections, as the **Add User Profile Wizard**, except administrator's or user's rights. To change the rights, you will have to delete the user profile and then add the user again with the new rights.

Changing the user's backup location will move all existing and redirect future backups, performed by the user, to another folder (device, etc). As moving files may take a lot of time and system resources, it is recommended that you schedule this operation for the time when the backup server computing load will be minimal. You can do it in the **Start Parameters** window. To complete configuring the profile, click **Finish** in the final summary window.

To change user's backup location within the same device, you must have at least as much free space on the device as the user's archives occupy, because the archives will first be copied to the new location, and then deleted from the old place.

If you select a user and click **Clear**, all archives created by this user will be deleted. The same operation for administrator profiles is impossible.

Deleting a user profile will disable backup to backup server for this user and his existing archives will be deleted. This operation might also be time-consuming, so you can schedule it for the off-peak period.

Deleting an administrator profile will not result in deleting any archives.

> There must be at least one administrator on a backup server. Therefore, deleting the last administrator profile is not possible. The maximum number of administrators is not limited.

4.5.5 Configuring Backup Locations

To display a full list of backup locations, click **Configure Backup Locations**.
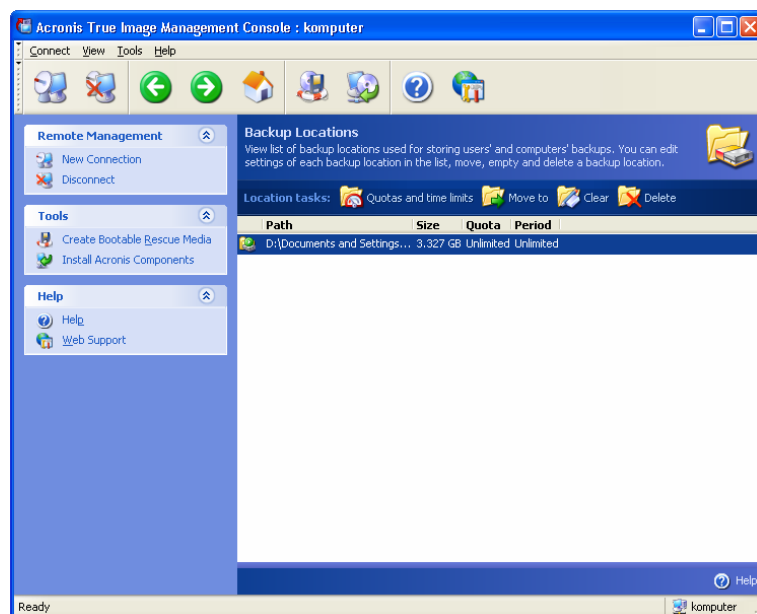
To edit limitations for a backup location, select the backup location, click on **Quotas and Time Limits** above the list and enter the new values in the appearing window.

To move a backup location along with all archives existing on it, select the backup location and click **Move to**. The **Move Backup Location Wizard** will display all users and computers associated with the selected backup location so you could make sure your choice is right. Then select the new location for the archives.

As moving files may take a lot of time and system resources, it is recommended that you schedule this operation for the time when the backup server computing load will be minimal. You can do it in the **Start Parameters** window. To complete configuring the operation, click **Finish** in the final summary window.

> To move a backup location within the same device, you must have at least as much free space on the device as all the archives in the backup location occupy, because the archives will first be copied to the new place, and then deleted from the old place.

Cleaning a backup location will delete all archives stored in this location. After clicking on **Clear** item the dialog box comes up, allowing you to view a list of backup archives to be removed before you confirm the operation.

Deleting a backup location will delete all archives stored in this location and redirect the associated computer/user's backups to the default backup location. After clicking on **Delete** item the dialog box comes up, allowing you to view a list of backup archives to be removed and a list of associated users/computers before you confirm the operation.

The default backup location cannot be deleted. If you try to do so, the program will clean the default backup location and issue an appropriate message. To delete the location completely, first reassign the default backup location by selecting **Specify Default Settings -> Set backup location**.

Cleaning and deleting backup locations might be time-consuming operations, so you can schedule them for the off-peak period.

4.5.6 Managing Archives

To display a full list of backups, stored on the backup server, click **Manage Backup Archives**.
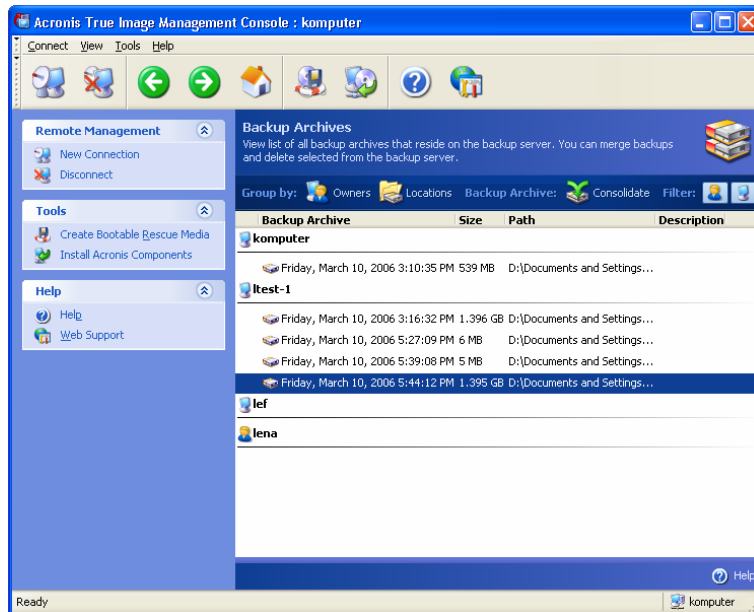
You can:

1. Sort the list by **Location** or **Owners** (users and computers) by clicking on the respective item above the list.

2. Filter out from the list all user's or all computer's backups (use buttons in the **Filter** group).

3. **Consolidate** any backup (except for the oldest one in the archive) with the preceding backup file. The resulting file will preserve all data changes, contained in both files and have the latest backup date. Thus, the archive integrity will not be affected, in spite of the fact that one backup will disappear. Data recovery from any of the remaining backups will be possible.

4.6 Creating bootable media

Bootable removable media or RIS package provides the ability to boot the standalone version of Acronis True Image Enterprise Server or Acronis True Image Bootable Agent on a crashed computer; computer, running other than Windows operating system or bare metal.

To create bootable removable media, click **Create bootable rescue media** on the toolbar or the sidebar, or select the same item from the **Tools** menu. Then follow the Wizard's instructions. See details in *Chapter 10. Creating bootable media*.

Acronis True Image Management Console does not contain Rescue Media Builder in its own installation. Therefore, to be able to create bootable media/RIS package from Acronis True Image Management Console, you must have Acronis True Image Enterprise Server or another Acronis product including Rescue Media Builder, installed on the same computer.

Chapter 5. Using Acronis True Image Enterprise Server (local version)

Acronis True Image Enterprise Server supports the command-line mode for data backup and restore, as well as the GUI mode, and can be used to execute XML scripts. Here we describe the operations available in GUI mode, which provides more functionality. For console commands and scripting see *Chapter 15. Command-line mode and scripting*.

5.1 Main program window

The main program window contains the menu, the toolbar, the sidebar, the **Active Tasks** pane and the main area. The main area contains operation icons, while the sidebar features **Tools** and **Help** panels.
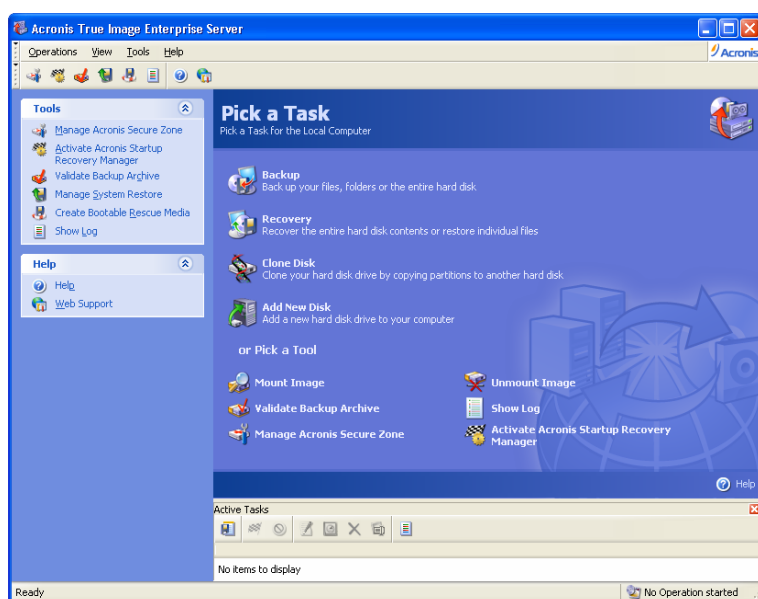
Most of the operations are represented two or even three times in different window areas, providing several ways to select them for more convenience. For example, you can start the necessary operation or tool by clicking its icon in the main area or by selecting the same item from the **Operations** or **Tools** menu.

The main window contains operation icons divided into two groups.

The **Task** group contains the following operations:

- **Backup** – create a backup archive

- **Recovery** – restore data from a previously created archive

- **Clone Disk** – transfer the OS, applications and data from the old disk to the new one

- **Add New Disk** – add a new disk for data storage leaving the OS and applications on the old one.

The **Tools** group contains the following items:

- **Mount Image** – connect a disk/partition image as a virtual drive

- **Unmount Image** – disconnect the connected virtual drive

- **Validate Backup Archive** – runs the archive integrity checking procedure

- **Show Log** – opens the Log Viewer window

- **Manage Acronis Secure Zone** – used to create, delete and resize a special hidden partition for storing archives (Acronis Secure Zone)

- **Activate Acronis Startup Recovery Manager** – activates the boot restoration manager (F11 key).

Program menu

The program menu line features the **Operations, View, Tools** and **Help** items.

The **Operations** menu contains a list of the available operations, including scheduling tasks.

The **View** menu contains items for managing the program window look:

- **Common Task Bar** – enables/disables the sidebar

- **Status Bar** – enables/disables the status bar

- **Active tasks** – enables/disables the Active Tasks pane at the bottom of the main area.

The **Tools** menu contains the following items:

- **Manage Acronis Secure Zone** – used to create, delete and resize a special hidden partition for storing archives (Acronis Secure Zone)

- **Activate Acronis Startup Recovery Manager** – activates the boot restoration manager (F11 key)

- **Validate Backup Archive** – runs the archive integrity checking procedure

- **Manage System Restore** – allows you to turn on/off Microsoft Windows System Restore tool and set its options directly from Acronis True Image Enterprise Server

- **Create Bootable Rescue Media** – runs the bootable media creation procedure

- **Show Log** – opens the Log Viewer window

- **Options** – opens a window for editing default backup/restore options, setting text appearance (fonts), configuring email/Winpopup notifications etc.

The **Help** menu is used to invoke help and obtain information about Acronis True Image Enterprise Server.

Active Tasks pane

The **Active Tasks** pane displays the scheduled and currently-being-executed tasks. It features its own toolbar. You can customize this toolbar view by right-clicking on it and selecting the desired options.

Status bar

At the bottom of the main window, there is a status bar divided into two parts. The left side briefly describes the selected operation; the right side indicates operation progress and results. If you double-click on the operation results, you will see the logs window.

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. This icon doesn't depend on the main program window being open. It is present for background execution of scheduled tasks as well.

5.2 Managing a local computer

You can perform the following operations on the local computer.

- **Backup and restore data, including system disks/partitions**

Click **Backup** or **Recovery**, then follow the Wizard's instructions. See details in *Chapter 6. Creating backup archives* and *Chapter 7. Restoring the backup data.*

- **Schedule backup operations**

Click the very left button on a tasks pane toolbar, then follow the Wizard's instructions. See details in *Chapter 8. Scheduling tasks*.

- **Set up backup/restore options,** such as system/network resources usage, before/after backup commands etc.

Select **Tools -> Options** -> **Default backup options** or **Default restoration options** and make settings. See details in *6.3 Setting backup options* and *7.4 Setting restore options.*

- **Validate backup archives wherever they reside, be it local, network or removable media**

Click **Validate Backup Archive**, then follow the Wizard's instructions. See details in *11.1 Validating backup archives*.

- **Set up sending notifications about Acronis True Image Enterprise Server operation and tracing** this operation in Windows Application Event Log

Select **Tools -> Options** -> **Notifications** or **Event tracing** and make settings. See details in *11.2 Operation results notification* and *11.4 Event tracing*.

- **Browse logs of Acronis True Image Enterprise Server operation**

Click the very right button on a tasks pane toolbar at the bottom of the window. See details in *11.3 Viewing logs*.

- **Manage Acronis Secure Zone**

Click **Manage Acronis Secure Zone**, then follow the Wizard's instructions. See details in *Chapter 9. Managing Acronis Secure Zone*.

- **Activate Acronis Startup Recovery Manager**

Click **Activate Acronis Startup Recovery Manager**, then follow the Wizard's instructions. See details in *3.4 Acronis Startup Recovery Manager*.

- **Mount partitions' images to explore and modify their contents, or to restore individual files**

Click **Mount image**, then follow the Wizard's instructions. See details in *Chapter 12. Mounting an image as a virtual drive*.

- **Unmount previously mounted partition images**

Click **Unmount image**, then follow the Wizard's instructions. See details in *12.2 Unmounting an image*.

- **Transfer the system to a new hard disk**

See *Chapter 13. Transferring the system to a new disk*.

- **Format partitions on a new hard disk**

See *Chapter 14. Adding a new hard disk*.

- **Turn on/off Windows System Restore tool**

See *11.5 Managing System Restore*.

- **Create bootable rescue media, its ISO or RIS package**

See *Chapter 10. Creating bootable media*.

Some of the above operations can be executed in command-line as well. For more information on Acronis True Image Enterprise Server command-line mode see *15.1 Working in the command-line mode*.

Chapter 6. Creating backup archives

To be able to restore the lost data or roll back your system to a predetermined state, you should first create a data or entire-system backup file.

If you are not concerned about restoration of your operating system along with all settings and applications, but plan to keep safe only certain data (the current project, for example), choose file/folder backup. This will reduce the archive size, thus saving disk space and possibly reducing removable media costs.

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 severe data damage or hardware failure. Moreover, the imaging procedure is much faster than copying files, and may significantly speed the backup process when it comes to backing up large volumes of data (see details in *3.1 The difference between file archives and disk/partition images*).

6.1 Backing up files and folders (file backup)

1. Invoke the **Create Backup Wizard** by clicking on the backup operation icon in the main program window.

2. Click **Next**.

3. Select **Files and folders** and click **Next**.

4. From the tree pane, select files and folders to back up. You can select a random set of files, folders, partitions, disks and even computers.
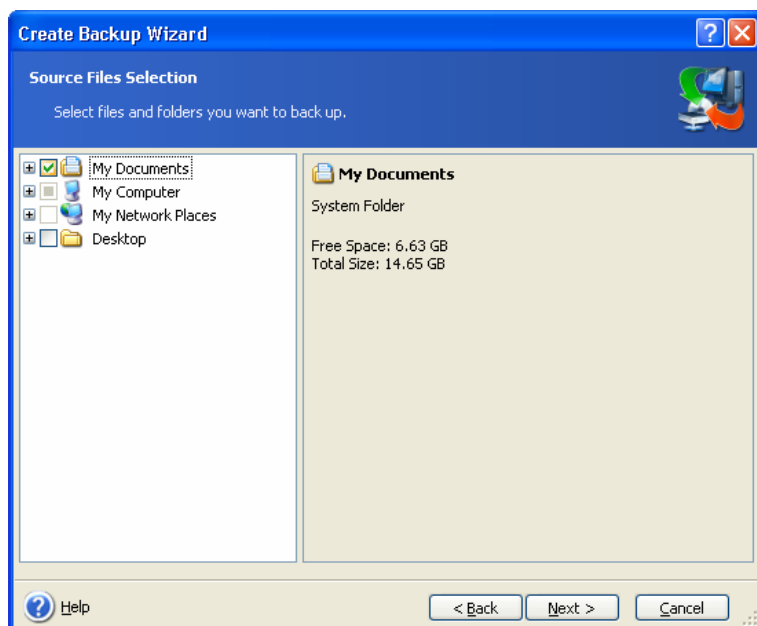
If you select a partition, disk or computer, and archive all its files, including system and hidden files, the bare-metal restore of that disk (partition, computer) still will not be possible. You also may not be able to boot the restored operating system. Therefore, it is recommended that you select only files and folders containing user data. To back up a disk or partition, use image backup.

5. Click **Next**.

6. Set filters for not to back up files of specific types. For example, you may want hidden and system files and folders, as well as files with **.~, .tmp and .bak** extensions, not to be stored in the archive.

You can also apply custom filters, using the common Windows masking rules. For example, to exclude all files with extension .exe, add ***.exe** mask. **My???.exe** mask will reject all .exe files with names, consisting of five symbols and starting with "my".

All of these settings will take effect for the current task. How to set the default filters, that will be called each time you create a file backup task, see in *6.3.2 Source files exclusion.*

7. Click **Next**.

8. Select the name and location of the archive file.

If you are going to create a full backup, type the file name in the **File Name** line, or use the file name generator (a button to the right of the line). If you select an existing archive, it will be overwritten.

If you are going to create an incremental backup (see *3.2 Full, incremental and differential backup*), select the latest full or incremental backup you have.

In fact, if all incremental backup files are stored together, it doesn't matter which one you select, as the program will recognize them as a single archive. If you stored the files on several removable disks, you must provide the latest archive file; otherwise, restoration problems might occur.

If you are going to create a differential backup, select the full backup which will be a base, or any of existing differential archives. Either way, the program will create a new differential archive file.

The "farther" you store the archive from the original folders, the safer it will be in case of data damage. 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, ftp-server or removable media will survive even if all your local hard disks are down. You can also use Acronis Secure Zone (see details in *3.3 Acronis Secure Zone*) for storing backups. In that case, you need not provide the file name.

You will need DVD UDF recording software installed for burning images on DVD disks. Examples of this software are Roxio DirectCD or Ahead InCD.

An FTP server must allow passive mode for file transfers. To enable data recovery directly from FTP server split the archive to files no more than 2 Gb in size.

9. Click **Next**.

10. Select whether you want to create a full, incremental or differential backup. If you have not backed up the selected files/folders yet, or the full archive seems too old to append incremental changes to it, choose full backup. Otherwise it is recommended that you create an incremental or differential backup (see *3.2 Full, incremental and differential backup*).
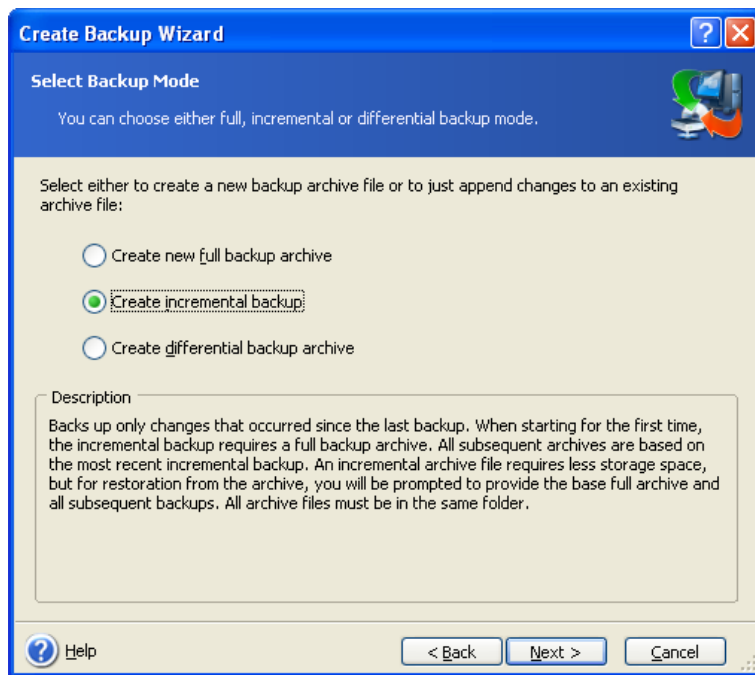
11. Click **Next**.

12. Select the backup options (that is, backup file splitting, compression level, password protection, pre/post backup commands etc.). You may **Use default options** or **Set the options manually**. If the latter is the case, the settings will be applied only to the current backup task. Alternatively, you can edit the default options from the current screen. Then your settings will be saved as default. See *6.3 Setting backup options* for more information.

13. Click **Next**.

14. Provide a comment for the archive. This can help prevent you from restoring the wrong files. 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.

15. Click **Next**.

16. At the final step, the backup task summary is displayed. Up to this point, you can click **Back** to make changes in the created task. Clicking **Proceed** will launch the task execution.

17. (For Acronis True Image Enterprise Server local version and Acronis True Image Management Console, connected to the computer being backed up) The task will appear on the **Active tasks** pane of the main window. The task progress will be shown in the 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.

In Acronis True Image Enterprise Server local version you can adjust the backup process priority. To do so, click on the process icon in the System Tray and select Low, Normal, or High priority from the appearing menu. How to set the default priority, see in *6.3.6 Backup performance*.

18. You may want to see the log when the task is completed. To view the log, click the **Show Operation Logs** button on the toolbar.

If you burn an archive to several removable media, be sure to number them, since you will have to insert them in order during the restoration.

6.2 Backing up disks and partitions (image backup)

1. Invoke the **Create Backup Wizard** by clicking on the backup operation icon in the main program window.

2. Click **Next**.

3. Select **The entire disk contents or individual partition** and click **Next**.

4. Select disks or partitions to back up. You can select a random set of disks and partitions.
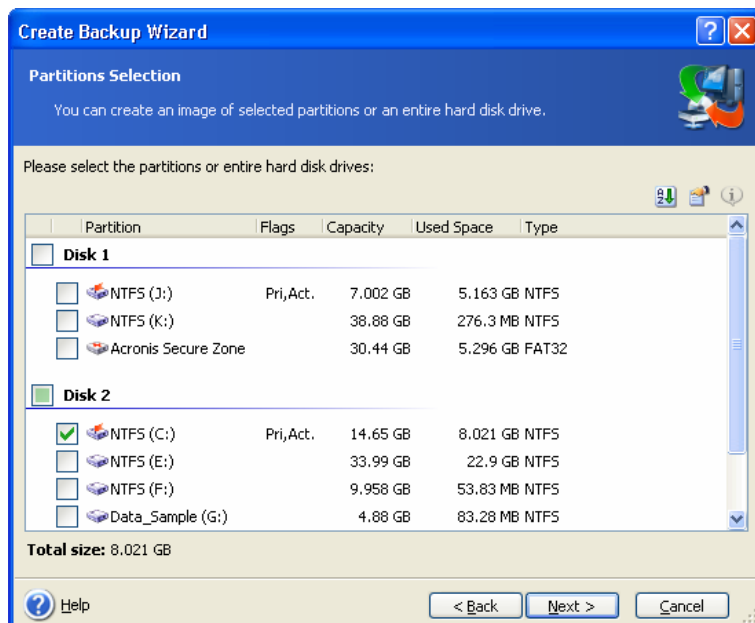
5. Click **Next**.

6. Select the name and location of the archive file.

If you are going to create a full archive, type the file name in the **File Name** line, or use the file name generator (a button to the right of the line). If you select an existing archive, it will be overwritten.

If you are going to create an incremental backup (see *3.2 Full, incremental and differential backup*), select the latest full or incremental backup you have.

> In fact, if all incremental backup files are stored together, it doesn't matter which one you select, as the program will recognize them as a single archive. If you stored the files on several removable disks, you must provide the latest archive file; otherwise, restoration problems might occur.

If you are going to create a differential backup, select the full backup which will be a base, or any of existing differential archives. Either way, the program will create a new differential archive file.

The "farther" you store the archive from the original partition, the safer it will be in case of data damage. For example, saving the archive to another hard disk will protect your data if your primary disk is damaged. Data saved to a network disk, ftp-server or removable media will survive even if all your local hard disks are down. You can also use Acronis Secure Zone (see details in *3.3 Acronis Secure Zone*) for storing backups. In that case, you need not provide the file name.

> You will need DVD UDF recording software installed for burning images on DVD disks. Examples of this software are Roxio DirectCD or Ahead InCD.

> An FTP server must allow passive mode for file transfers. To enable data recovery directly from FTP server split the archive to files no more than 2 Gb in size.

7. Click **Next**.

8. Select whether you want to create a full or incremental backup. If you have not backed up the selected disks/partitions yet, or the full archive seems too old to append incremental

changes to it, choose full backup. Otherwise it is recommended that you create an incremental or differential backup (see *3.2 Full, incremental and differential backup*).

9. Click **Next**.

10. Select the backup options (that is, backup file splitting, compression level, password protection, pre/post backup commands etc.). You may **Use default options** or **Set the options manually**. If the latter is the case, the settings will be applied only to the current backup task. Alternatively, you can edit the default options from the current screen. Then your settings will be saved as default. See *6.3 Setting backup options* for more information.

11. Click **Next**.

12. Provide a comment for the archive. This can help prevent you from restoring the wrong disk/partition. 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.

13. Click **Next**.

14. At the final step, the backup task summary is displayed. Up to this point, you can click **Back** to make changes in the created task. Clicking **Proceed** will launch the task execution.

15. (For Acronis True Image Enterprise Server local version or Acronis True Image Management Console, connected to the computer being backed up) The task will appear on the **Active tasks** pane of the main window. The task progress will be shown in the 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.

> In Acronis True Image Enterprise Server local version you can adjust the backup process priority. To do so, click on the process icon in the System Tray and select Low, Normal, or High priority from the appearing menu. How to set the default priority, see in *6.3.6 Backup performance*.

16. You may want to see the log when the task is completed. To view the log, click the **Show Operation Logs** button on the toolbar.

> If you burn an archive to several removable media, be sure to number them, since you will have to insert them in order during the restoration.

6.3 Setting backup options

To view or edit the default backup options in Acronis True Image Enterprise Server local version, select **Tools -> Options -> Default Backup Options** from the main program menu.

To do the same remotely, connect Acronis True Image Management Console to the remote computer, click **Remote Computer Options** and select **Default backup options.**

You can edit the default (or set the temporary) backup options while creating a backup task as well.
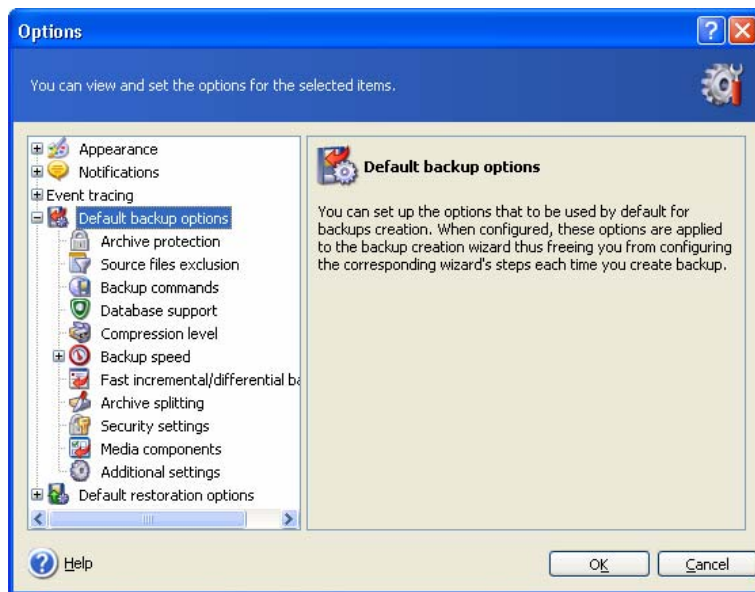
6.3.1 Archive protection

The default setting – **no password**.

An archive can be protected with a password. To protect the archive from being restored by anybody except you, enter a password and its confirmation into the text fields. A password should consist of at least eight symbols and contain both letters (in the upper and lower cases preferably) and numbers to make it more difficult to guess.

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

6.3.2 Source files exclusion

The default setting – **all files from the selected folders will be included into the archive**.

You can set the default filters for not to back up files of specific types. For example, you may want hidden and system files and folders, as well as files with **.~, .tmp and .bak** extensions, not to be stored in the archive.

You can also apply custom filters, using the common Windows masking rules. For example, to exclude all files with extension .exe, add ***.exe** mask. **My???.exe** mask will reject all .exe files with names, consisting of five symbols and starting with "my".

This option is effective for file/folders backup only. When creating a disk/partition image, you cannot filter out any files.

6.3.3 Pre/post commands

You can specify commands or batch files to be automatically executed before and after the *backup procedure*. For example, you may want to remove some tmp files from the disk before starting backup or configure a third-party antivirus product to be started each time 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.

Unchecking the **Do not perform operations until the commands execution is complete** box, checked by default, will permit the backup process to run concurrently with your commands execution.

6.3.4 Database support

Database servers, such as MS SQL Server and MS Exchange, prove to be troublesome to backup, partially due to open files and indexes and partially due to rapid data changes. Therefore many system administrators prefer to suspend the database at the backup (capturing the Snapshot) moment.

1. Volume Shadow Copy Service

Microsoft Volume Shadow Copy Service (VSS) provides the infrastructure for backup on running systems by keeping up coordination between user applications that update data on disk and backup applications. VSS is available in Microsoft Windows XP and Microsoft Windows Server 2003 operating systems.

If your database is compatible with **Microsoft Volume Shadow Copy Service (VSS)**, then checking the **Enable VSS support** box in **Database support** window will ensure completion of all transactions before the backup process starts. Then the database will be ready to access immediately after recovery. The examples of VSS-aware databases are Exchange, Oracle, SQL Server.

2. Before/after data capture commands

However, VSS is not available in server operation systems older than **Windows 2003 Server**, and not all databases support VSS. In these cases, the transactions completion can be ensured with executing batch files or scripts that pause the appropriate Windows services and automatically resume them after data capture.

An example of a batch file, suspending the Windows services for MS Exchange:

```
net stop msexchangesa /y /y

net stop "Microsoft Exchange Routing Engine"
```

An example of a batch file, resuming the Windows services for MS Exchange:

```
net start "Microsoft Exchange System Attendant"

net start "Microsoft Exchange Event"

net start "Microsoft Exchange IMAP4"

net start "Microsoft Exchange MTA Stacks"

net start "Microsoft Exchange POP3"

net start "Microsoft Exchange Routing Engine"
```

Create batch files in any text editor (for example, name it 'pause_services.bat' and 'resume_services.bat'). Use **Edit** buttons to the right of **Before data capture command** and **After data capture command** fields, to open the **Edit Command** window where you can browse folders to find the respective batch files or scripts. A single command can be specified in the same window along with its arguments and working directory.

It is critical to note that these commands, as opposed to **Pre/post commands** above, will be executed before and after *data capture* process, which takes seconds, while the entire backup procedure may take quite long time. Therefore, the database idle time will be minimal.

Before/after data capture commands can also be used for purposes, different from suspending the database, especially if VSS support is enabled. You may want to suspend an application other than database, for example. The commands execution and the VSS actions will be sequenced as follows:

"before" commands -> VSS Suspend -> data capture -> VSS Resume -> "after" commands.

Unchecking the **Do not perform operations until the commands execution is complete** box, checked by default, will permit the backup process to run concurrently with your commands execution.

6.3.5 Compression level

The default setting – **Normal**.

If you select **None**, the data will be copied without any compression, which may significantly increase the backup file size. However, if you select **Maximum** compression, the backup will take longer to create.

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

Generally, it is recommended that you use the default **Normal** compression level. You might want to select **Maximum** compression for removable media to reduce the number of blank disks required.

6.3.6 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 physical characteristics of devices.

1. Backup process priority

The default setting – **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 of backup priority may 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 default setting – **Maximum**.

Backing up in the background to an internal hard disk (for example, to Acronis Secure Zone) may slow other programs performance because of large amounts of data transferred to the disk. You can limit the hard disk usage by Acronis True Image Enterprise Server 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 default setting – **Maximum**.
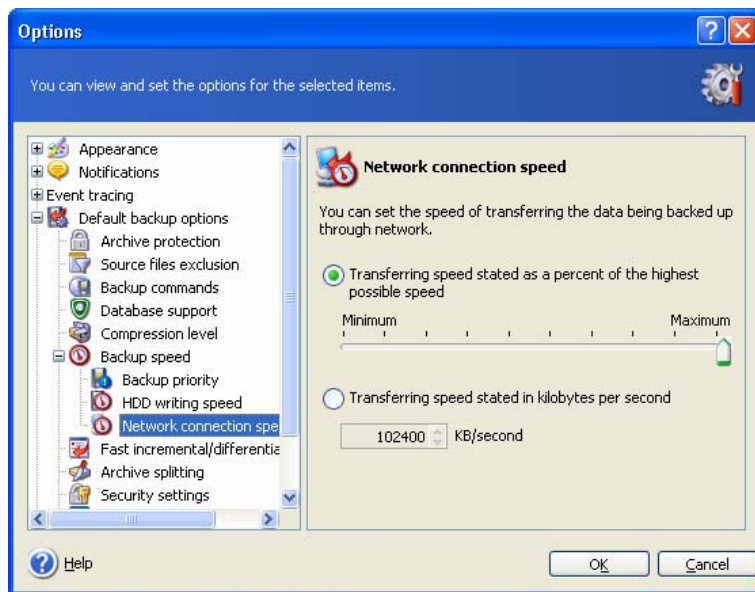
If you frequently backup data to network drives, think of limiting the network usage used by Acronis True Image Enterprise Server. To set the desired data transfer speed, drag the slider or enter the bandwidth limit for transferring backup data in kilobytes per second.

6.3.7 Fast incremental/differential backup

The default setting – **Use fast incremental/differential backup**.

Incremental/differential backup captures only changes in data occurred since the last backup. To speed up the backup process, Acronis True Image Enterprise Server determines whether the file has changed by file size and the date/time when the file was last saved. Disabling this feature will make the program compare the entire file contents to that stored in the archive.

This option relates only to disk/partition (image) backup.

6.3.8 Archive splitting

Sizeable backups can be split into several files that together make the original backup. A backup file can be split for burning to removable media or saving on ftp-server (data recovery directly from ftp-server requires the archive to be split into files no more than 2 Gb in size).

The default setting – **Automatic**. With this setting, Acronis True Image Enterprise Server will act as follows.

When backing up to the hard disk: If the selected disk has enough space and its file system allows the estimated file size, the program will create a single archive file.

If the storage disk has enough space, but its file system does not allow the estimated file size, Acronis True Image Enterprise Server will automatically split the backup into several files.

> FAT16 and FAT32 file systems have a 4 GB file size limit. At the same time, the existing hard drives capacity may reach as much as 160GB. Therefore, an archive file might easily exceed this limit, if you are going to back up the entire disk.

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

When backing up to a diskette, CD-R/RW or DVD+R/RW: Acronis True Image Enterprise Server will ask you to insert a new disk when the previous one is full.

Alternatively, you can select **Fixed size** and enter the desired file size or select it from the drop-down list. The backup will then be split into multiple files of the specified size. That comes in handy when backing up to a hard disk with a view to burning the archive to CD-R/RW or DVD+R/RW later on.

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

6.3.9 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 user, specified in the permissions, you may not be able to read or modify this file.

To completely eliminate this kind of problem, you can disable preserving files' security settings in archives. Then the restored files/folders will always inherit the permissions from the folder, where they are restored to (parent folder or disk, if restored to the root).

Alternatively, you can disable files' security settings during restoration, even if they are available in the archive (see *7.4.5 File-level security* settings below). The result will be the same.

In archives, store encrypted files in decrypted state

The default setting – **disabled**.

If you do not use encryption feature, available in Windows 2003 Server and Windows XP 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/folders backup.

6.3.10 Media components

The default setting – **disabled**.

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

> The current program version does not support creating bootable DVDs.

Choose the basic components, necessary for boot and restoring data, on the **General** tab.

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 at boot from the media and clicking "restore" all data will be silently restored to the original place. No options or selections like resizing partitions will be possible.

If you want more functionality during restoration, write a standalone version of **Acronis True Image Enterprise Server** to the rescue disk. Then you will be able to configure the restore task using Restore Data Wizard, use Acronis Snap Restore or Acronis Universal Restore etc.

Under **Advanced** tab you can select full, safe or both Acronis True Image Enterprise Server loader version. The safe version does not have USB, PC card or SCSI drivers and is useful only in case the full version does not load. If you want the computer, booted from the media, to be accessible for remote control with Acronis True Image Management Console, add **Acronis Bootable Agent** to the media. If you have other Acronis products, such as Acronis Disk Director Suite, installed on your computer, the bootable versions of these programs' components will be offered as **Advanced** as well.

In case you check **Do not place additional components if there is no free space** box, the program will try to write at least basic component to media, short of space.

6.3.11 Additional settings

1. Validate backup archive upon operation completion

The default setting – **disabled**.

You can choose to check the backup data integrity. Verification will be performed immediately after the archive is created.

> To check data from an incremental backup, you must have all previous incremental backup files and the initial full backup. If any of successive backups is missing, validation is impossible.
>
> To check data from a differential backup, you must have the initial full backup as well.
>
> However, if you created several differential or both incremental and differential backups based on the same full backup (and therefore, in the same folder), you will need ALL of these successive backups to validate the archive.

2. Overwrite data on a tape without user confirmation

The default setting – **disabled**.

A full backup, when created on a tape drive, overwrites all data stored on the tape (see *3.9 Backing up to tape drive* for more information). In this situation, Acronis True Image Enterprise Server will warn that you are about to lose data on the tape. To disable this warning, check the middle box.

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

The default setting – **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 be impossible if the user is away, because the program will wait for pressing **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.

Chapter 7. Restoring the backup data

7.1 Restore under Windows or boot from CD?

As mentioned above (see *2.4.1 Running Acronis True Image Enterprise Server (local version)*), Acronis True Image Enterprise Server can be run in several ways. We recommend that you first try to restore data running Acronis True Image Enterprise Server under Windows, because this method 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 load.

The boot CD from which you loaded the program does not keep you from using other CDs with backups. Acronis True Image Enterprise Server is loaded entirely into RAM, so you can remove the bootable CD to insert the archive disk.

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

7.1.1 Network settings in rescue mode

When booted from removable media, RIS server or by Startup Recovery Manager, Acronis True Image Enterprise Server may not detect the network. Such might be the case if there is no DHCP server in your network or your computer address was not identified automatically for some reason.

To enable connection, specify network settings manually in the window, available at **Tools -> Options -> Network adapters.**
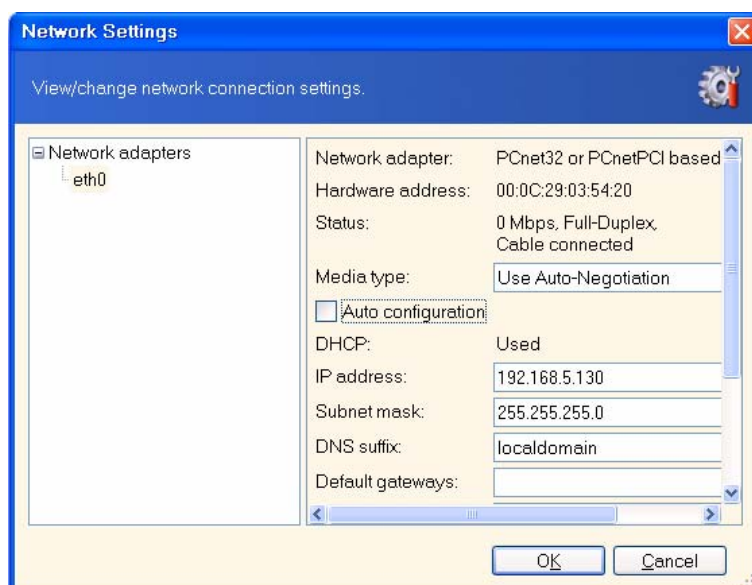
7.2 Restoring files and folders from file archives

Here we describe how to restore file/folders from a file backup archive. You can restore the desired files/folders from a disk/partition image as well. To do so, mount the image (see *Chapter 12. Mounting an image as a virtual drive*) or start the image restoration and select **Restore specified files or folders** (see *7.3 Restoring disks/partitions or files from images*).

1. Invoke the **Restore Data Wizard** by clicking on the restore operation icon in the main program window.

2. Click **Next**.

3. Select the archive. If the archive is located in Acronis Secure Zone, select it to choose the archive on the next step.

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

Data recovery directly from ftp-server requires the archive to consist of files no more than 2 Gb in size. If you suppose that some of the files may be larger, first copy the entire archive (along with the initial full backup) to a local hard disk or network share disk.

If you added a comment to the archive, it will be displayed to the right of the drives tree. If the archive was protected with a password, Acronis True Image Enterprise Server will ask for it. The comment and the **Next** button will be unavailable until you enter the correct password.

4. Click **Next**.

5. If you are to restore files from an archive, containing incremental backups, Acronis True Image Enterprise Server will suggest that you select one of successive incremental backups by date/time of its creation. Thus, you can return the files/folders to a certain moment.

To restore data from an incremental backup, you must have all previous incremental backup files and the initial full backup. If any of successive backups is missing, restoration is impossible.

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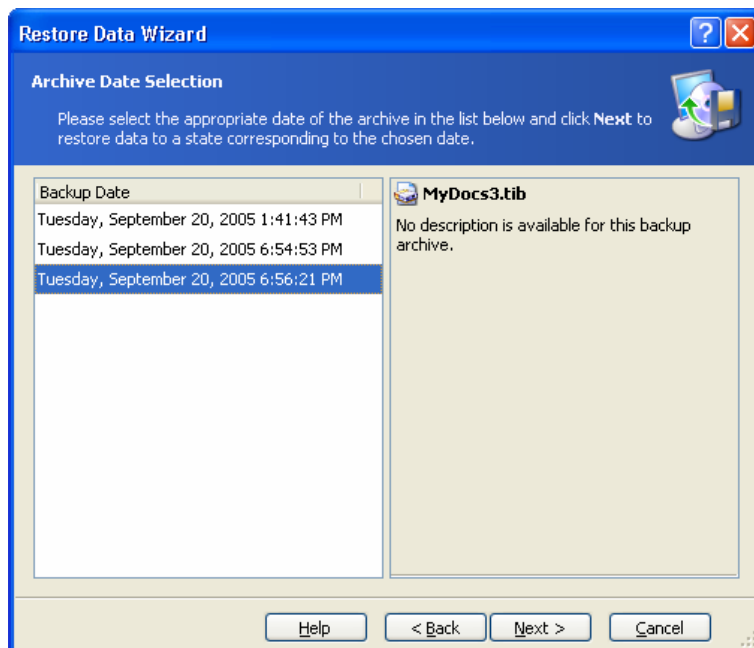
6. Click **Next**.

7. Select a folder on your computer where you want to restore selected folders/files (a target folder). You can restore data to their original location or choose another folder, if necessary.

8. Click **Next**.

9. 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.
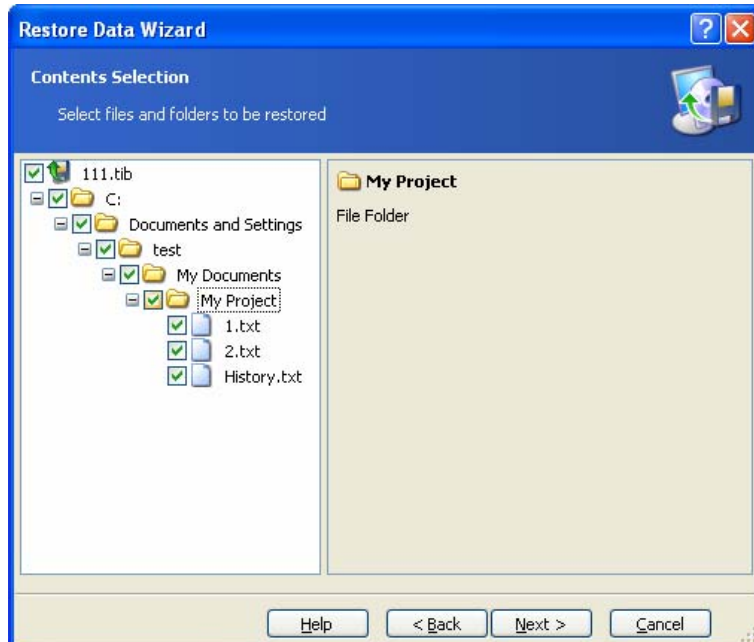
10. Click **Next**.

11. Select the options for restoration process (that is, pre/post restoration commands, restoration process priority, file-level security settings etc.). You may **Use default options** or **Set the options manually**. If the latter is the case, the settings will be applied only to the current restore task. Alternatively, you can edit the default options from the current screen. Then your settings will be saved as default. See *7.4 Setting restore options* for more information.

12. Click **Next**.

13. Set filters for not to restore files of specific types. For example, you may want hidden and system files and folders, as well as files with **.~, .tmp and .bak** extensions, not to be restored from the archive.

You can also apply custom filters, using the common Windows masking rules. For example, to exclude all files with extension .exe, add ***.exe** mask. **My???.exe** mask will reject all .exe files with names, consisting of five symbols and starting with "my".

All of these settings will take effect for the current task. How to set the default filters, that will be called each time you restore data, see in *7.4.1 Files to restore exclusion*.

14. Click **Next**.

15. The next selection allows you to keep useful data changes, made since the selected backup was created. Choose what to do if the program finds in the target folder a file with the same name as in the archive.
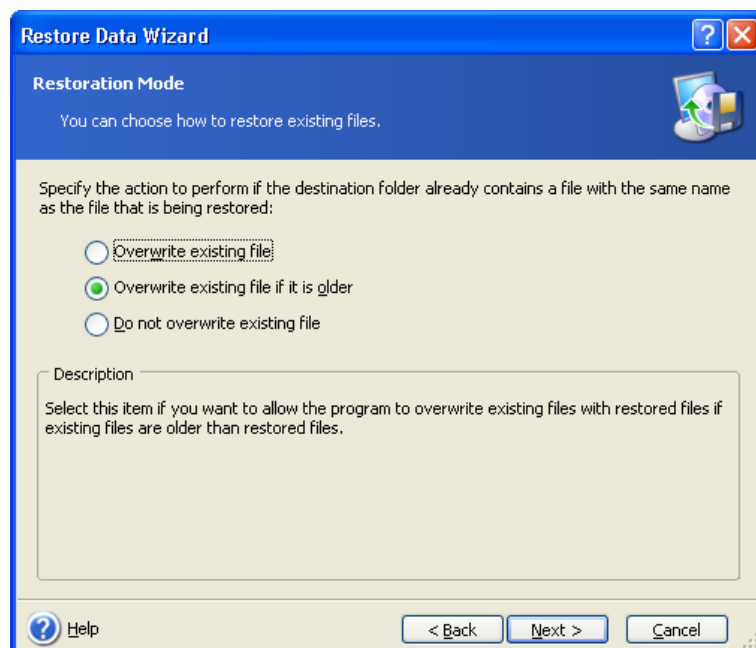
Overwrite existing file – this will give the archived file unconditional priority over the file on the hard disk.

Overwrite existing file if it is older – this will give the priority to the most recent file modification, whether it is in the archive or on the disk

Do not overwrite existing file – this will give the file on the hard disk unconditional priority over the archived file.

16. At the final step, the restoration summary is displayed. Up to this point, you can click **Back** to make changes in the created task. Clicking **Proceed** will launch the task execution.

17. (For Acronis True Image Enterprise Server local or standalone version, or Acronis True Image Management Console, connected to the target computer) The task will appear on the **Active tasks** pane of the main window. The task progress will be shown in the special window. You can stop the procedure by clicking **Cancel**. Please keep in mind that the aborted procedure still may cause changes in the destination folder.

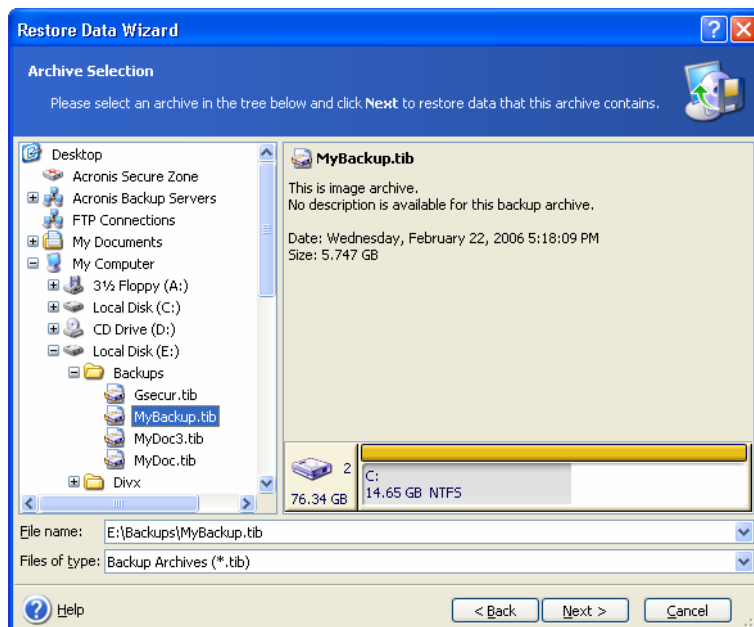## 7.3 Restoring disks/partitions or files from images

To restore a partition (disk) from an image, Acronis True Image Enterprise Server 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) can not be blocked, close applications that use this partition (disk) and start over. If you can not determine which applications use the partition (disk), close them all.

7.3.1 Starting the Restore Data Wizard

1. Invoke the **Restore Data Wizard** by clicking on the restore operation icon in the main program window.

2. Click **Next**.

7.3.2 Archive selection

1. Select the archive. If the archive is located in Acronis Secure Zone, select it to choose the archive at the next step.

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

Data recovery directly from ftp-server requires the archive to be split into files no more than 2 Gb in size. If you suppose that some of the files may be larger, first copy the entire archive (along with the initial full backup) to a local hard disk or network share disk.

If you added a comment to the archive, it will be displayed to the right of the drives tree. If the archive was protected with a password, Acronis True Image Enterprise Server will ask for it. The partitions layout, the comment and the **Next** button will be unavailable until you enter the correct password.

2. Click **Next**.

3. If you are to restore data from an archive, containing incremental backups, Acronis True Image Enterprise Server will suggest that you select one of successive incremental backups by date/time of its creation. Thus, you can return the disk/partition to a certain moment.
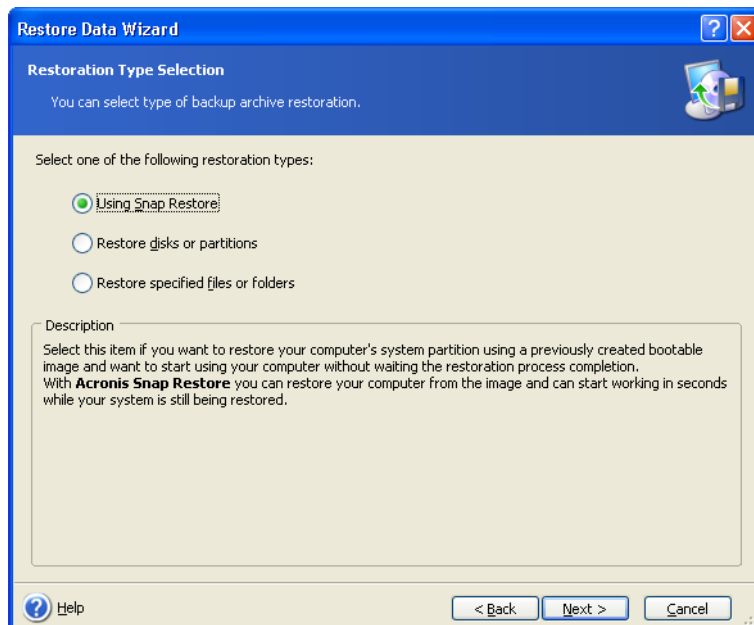
To restore data from an incremental backup, you must have all previous incremental backup files and the initial full backup. If any of successive backups is missing, restoration is impossible.

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

4. Click **Next**.

7.3.3 Restoration type selection

1. Select what you want to restore:

Restore specified files or folders

With this selection, you will be further offered 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 to restore files instead of disk/partition, uncheck the unnecessary folders. Otherwise you will restore a lot of excessive files. Then you will be taken directly to Restoration Summary screen (*7.3.13 Restoration summary and executing restoration*).

Restore disks or partitions

Having selected a usual way of disks/partitions recovery, you will have to make all settings described below.

Using Snap Restore

When restoring a system disk/partition image from Acronis Secure Zone, you will have the third opportunity – to use **Acronis Snap Restore**. Having selected this option, you will proceed directly to the summary window (*7.3.13 Restoration summary and executing restoration*). In a few seconds after pressing **Proceed** the computer will reboot to the restored system. Log in and work – no more reboots or other actions required. More about Acronis Snap Restore see in *3.6 Acronis Snap Restore*.

When performing Snap Restore, the current Acronis True Image Enterprise Server version always restores the entire system disk. Therefore, if your system disk consists of several partitions and you are planning to use Acronis Snap Restore, all partitions must be included into the image. Otherwise partitions, missing in the image, will be lost.

However, you can choose an ordinary way of restoration for that image. This will allow you to make changes to the restored partition, that would be impossible when using Acronis Snap Restore.

Finally, if you are not going to recover the system, but only want to repair damaged files, select **Restore specified files or folders**.

2. Click **Next**.

7.3.4 Selecting a disk/partition to restore

1. The selected archive file can contain images of several partitions or even disks. Select which disk/partition to restore.
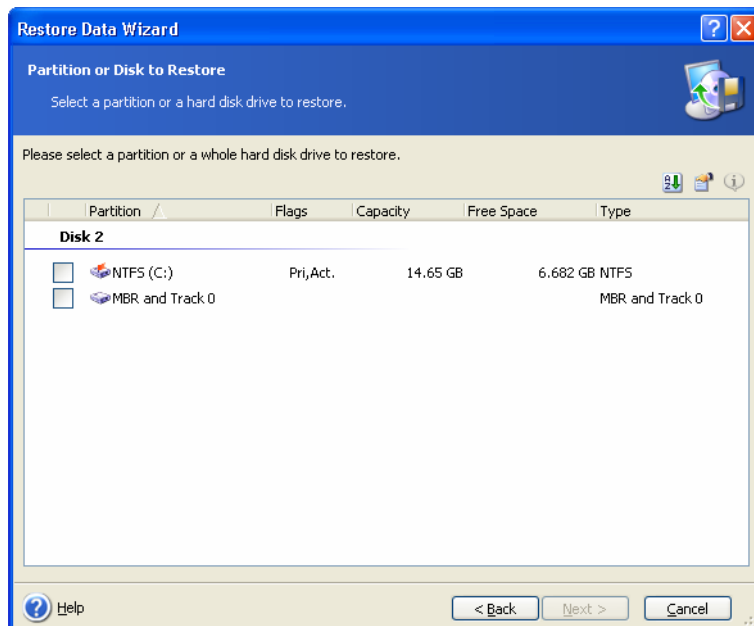
Disk and partition images contain a copy of track 0 along with MBR (Master Boot Record). It appears in this window in a separate line. You can choose whether to restore MBR and track 0 by checking the respective box. Restore MBR if it is critical to your system boot.

2. Click **Next**.

7.3.5 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 their 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 restored partition will be replaced by the image data, so be careful and watch for non-backed-up data that you might need.

2. Click **Next**.

7.3.6 Changing the restored partition type

1. 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 an operating system from it, you will select **Active**.

If you restore a system partition to another hard disk with its own partitions and OS, most probably, 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 server from booting.

2. Click **Next**.

7.3.7 Changing the restored partition file system

1. Though seldom required, you can change the partition file system during its restoration. Acronis True Image Enterprise Server can make the following file system conversions: **FAT 16 -> FAT 32, Ext2 -> Ext3**. For partitions with other native file systems this option is not available.

> Let us imagine you are to restore a partition from an old, low-capacity FAT16 disk to a newer disk. FAT16 would not be effective and might even be impossible to set on the high-capacity hard disk. That's because FAT16 supports partitions up to 4 GB, so you will not be able to restore a 4 GB FAT16 partition to a partition that exceeds that limit without changing the file system. It would make sense here to change the file system from FAT16 to FAT32.
>
> However, keep in mind that not all operating systems support FAT32. MS-DOS, Windows 95 and Windows NT 3.x, 4.x do not support FAT32 and will not be operable after you restore a partition and change its file system. These can be normally restored on a FAT16 partition only.

2. Click **Next**.

7.3.8 Changing the restored partition size and location

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

Using this feature, you can redistribute the disk space between partitions being restored. In this case, you will have to restore the partition to be reduced first.
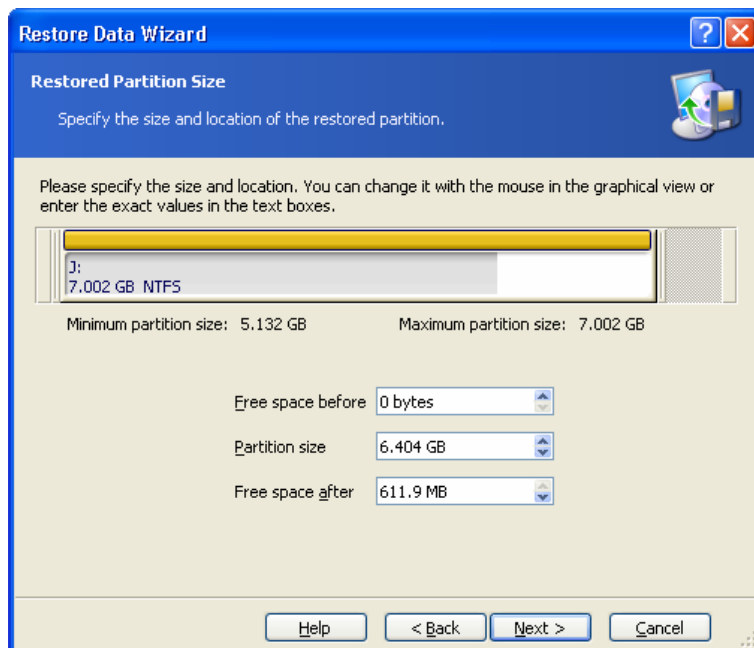
These changes might be useful if you are to copy your hard disk to a new high-capacity one by creating its image and restoring it to a new disk with larger partitions. This way of cloning is used if it is impossible to connect the second hard disk to the server (for more details about cloning see *13.1 General information*).

2. Click **Next**.

7.3.9 Assigning a letter to the restored partition

1. Acronis True Image Enterprise Server will assign an unused letter to a restored partition. You can select the desired letter from a drop-down list. If you set the switch to **No**, no letters will be assigned to the restored partition, hiding it from OS.

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

2. Click **Next**.

7.3.10 Restoring several partitions at once

1. 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.

If you want to restore another disk (partition), select **Yes, I want to restore another partition or hard disk drive**. Then you will return to the partition selection window (7.3.4) again and will have to repeat the above steps. Otherwise, don't set this switch.

2. Click **Next**.

7.3.11 Setting restore options

1. Select the options for restoration process (that is, pre/post restoration commands, restoration process priority etc.). You may **Use default options** or **Set the options manually**. If the latter is the case, the settings will be applied only to the current restore task. Alternatively, you can edit the default options from the current screen. Then your settings will be saved as default. See *7.4 Setting restore options* for more information.
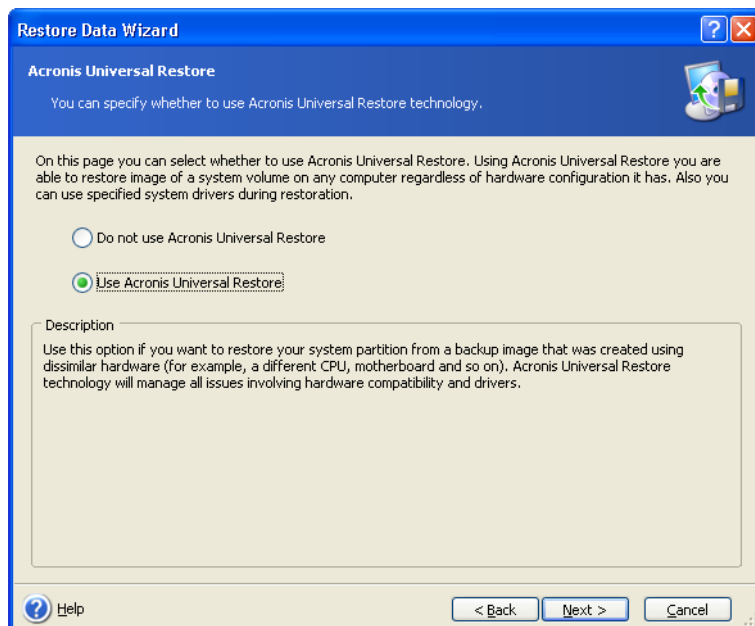
2. Click **Next**.

7.3.12 Using Acronis Universal Restore

Acronis Universal Restore is an optional Acronis True Image Enterprise Server feature. It should be purchased separately and installed from a separate .msi setup file. The following is true for Acronis True Image Enterprise Server installations including Acronis Universal Restore.

Acronis Universal Restore option is not available when restoring dynamic disks and volumes.

1. Using Acronis Universal Restore will help you create a bootable system clone on a different hardware (for more information see *3.7 Acronis Universal Restore*). Choose this when restoring a system disk (partition) to a computer with other processor, motherboard or hard disk controller than in the imaged system.

2. Click **Next**.

3. You can specify a path to the driver repository (a folder or folders on a network drive or CD where the program will search for drivers).
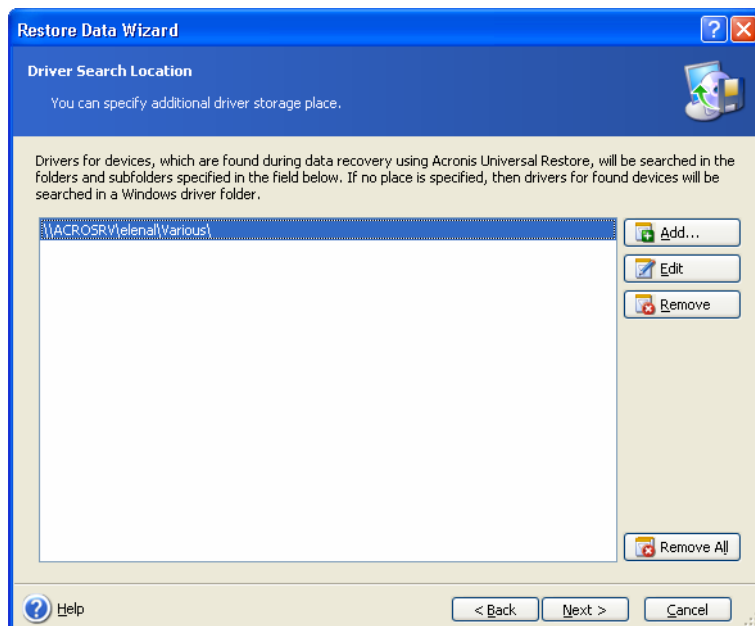
4. Click **Next**.

5. If you know which drivers will fit for the new hardware, add them to the drivers list in the next window. You can add HAL and hard disk controller drivers. Drivers for devices (sound cards, network adapters, video cards etc.) will be found by Windows itself when it boots.

Thus, Acronis Universal Restore uses three sources for drivers search: the driver repository, the list of user-specified (enforced) drivers, and the Windows default driver storage folders (in the image being restored). The program will find the most suitable drivers of all available and install them into the restored system. However, the drivers defined by the user (enforced drivers), will have the priority. They will be installed, with appropriate warning, even if the program finds the better driver.

> When migrating from RAID to RAID, be sure to specify an appropriate driver for the RAID controller in the **Forcedly Installed Drivers** window. Otherwise a basic HDD driver will be installed.

> When restoring the system to a virtual machine that uses SCSI hard drive controller, be sure to specify SCSI drivers for virtual environment in the **Forcedly Installed Drivers** window. Use drivers bundled with your virtual machine software or download the latest drivers versions from the software manufacturer website.

6. Click **Next**.

7.3.13 Restoration summary and executing restoration

1. At the final step, the restoration summary is displayed. Up to this point, you can click **Back** to make changes in the created task. If you click **Cancel**, no changes will be made to disk(s). Clicking **Proceed** will launch the task execution.

2. (For Acronis True Image Enterprise Server local version, or Acronis True Image Management Console, connected to the target computer) The task will appear on the **Active tasks** pane of the main window. The task progress will be shown in the 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.

If Acronis Universal Restore finds no HAL or hard disk controller drivers compatible with the new hardware in all available sources, you will be prompted to browse network share drive, floppy disk or CD to select missing drivers. On starting Windows, it will initialize a common procedure for installing new hardware. At this point, you will be able to specify drivers for devices, if Windows cannot find them automatically.

7.4 Setting restore options

To view or edit the default restore options in Acronis True Image Enterprise Server local version, select **Tools -> Options -> Default Restoration Options** from the main program menu.

To do the same remotely, connect Acronis True Image Management Console to the remote computer, click **Remote Computer Options** and select **Default Restoration options.**

You can edit the default (or set the temporary) restore options while creating a restore task as well.
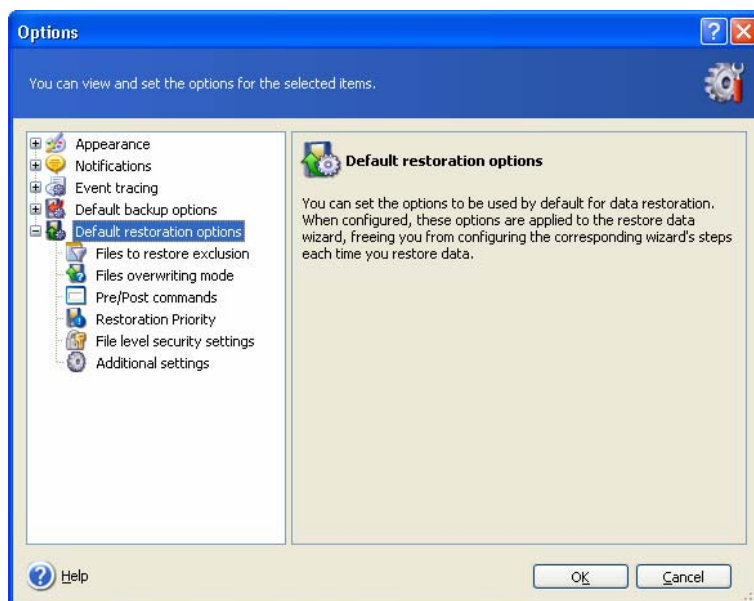
7.4.1 Files to restore exclusion

The default setting – **Restore all files**.

You can set the default filters for not to restore files of specific types. Use the common Windows masking rules. For example, to exclude all files with extension .exe, add ***.exe** mask. **My???.exe** mask will reject all .exe files with names, consisting of five symbols and starting with "my".

This option is effective only when restoring files from file/folders archives. When restoring files from a disk/partition image, you cannot filter out any files.

7.4.2 Files overwriting mode

This option allows you to keep useful data changes, made since the backup being restored was done. Choose what to do if the program finds in the target folder a file with the same name as in the archive.

Overwrite existing file – this will give the archived file unconditional priority over the file on the hard disk.

Overwrite existing file if it is older – this will give the priority to the most recent file modification, whether it is in the archive or on the disk.

Do not overwrite existing file – this will give the file on the hard disk unconditional priority over the archived file.

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

7.4.3 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.

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

7.4.4 Restoration priority

The default setting – **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. Increasing of restoration priority may speed up the restore process due to taking resources from the other currently running processes. The effect will depend on total CPU usage and other factors.

7.4.5 File-level security settings

The default setting – **Restore files with their security settings**.

If the files' security settings were preserved during backup (see *6.3.9   File-level security* settings), you can choose whether to restore files' security settings 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/folders archives.

7.4.6 Additional settings

1. You can choose whether to restore files' date and time from the archive or assign the files the current date and time.

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

> To check data from an incremental backup, you must have all previous incremental backup files and the initial full backup. If any of the successive backups are missing, validation is impossible.
>
> To check data from a differential backup, you must have the initial full backup as well.
>
> However, if you created several differential or both incremental and differential backups based on the same full backup (and therefore, in the same folder), you will need ALL of these successive backups to validate the archive.

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

Verification of the file system is available only when restoring disk/partitions under Windows and for FAT16/32 and NTFS file systems.

Chapter 8. Scheduling tasks

Acronis True Image Enterprise Server allows you to schedule periodic backup tasks. Doing so will give you peace of mind, knowing that your data are safe.

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

All the scheduled tasks appear in the **Active Tasks** area of the main window. You can start, stop, edit, delete and rename the scheduled tasks.

8.1 Creating scheduled tasks

1. To invoke the **Schedule Task Wizard**, click on its icon on the **Active Tasks** toolbar or select **Operations -> Schedule Task** from the main menu.

2. Click **Next**.

3. Configure a backup task in the usual way (see *Chapter 6. Creating backup archives*). If you choose to create the backup archive on a network drive, you will have to enter a user name and a password for network access.

4. Set the task execution periodicity.
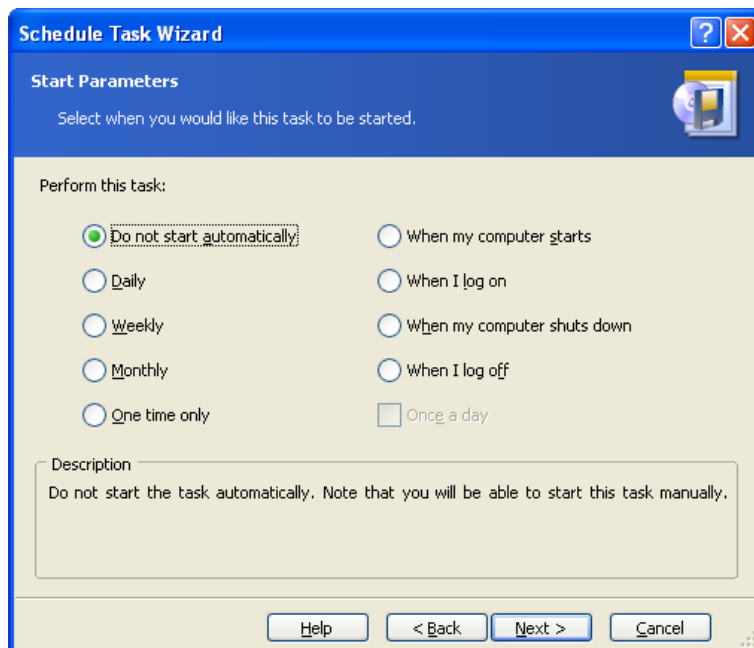
- **Do not start automatically** – the task will be saved, but not launched automatically. You will be able to launch it later by clicking the start button on the Active Tasks pane

- **Daily** – the task will be executed once a day or once in several days

- **Weekly** – the task will be executed once a week or once in several weeks on selected day

- **Monthly** – the task will be executed once a month on the selected day

- **One time only** – the task will be executed once at the specified time and day

- **When my computer starts** – the task will be executed at every OS startup

- **When I log on** – the task will be executed each time the current user logs in to the OS

- **When my computer shuts down** – the task will be executed before every server shutdown or reboot

- **When I log off** – the task will be executed each time the current user logs off of the OS.

  Some of these options might be disabled depending on the operating system.

5. Click **Next**.

6. Specify the task start time and other schedule parameters, according to the selected periodicity (see 8.1.1 - 8.1.4).

7. Click **Next**.

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

In the upper field, enter a user name. Enter a password twice in two fields below.

9. At the final step, the task configuration is displayed. Up to this point, you can click **Back** to make changes in the created task. If you click **Cancel**, all settings will be lost. Click **Finish** to save the task.

10. The task schedule and default name appear on the **Active tasks** pane of the main window. You are prompted to rename the task just now. If you do not want to do it, press Enter or Esc key.

8.1.1 Setting up daily execution

If you select the daily execution, set the **Start time** and days on which you want to execute the task:
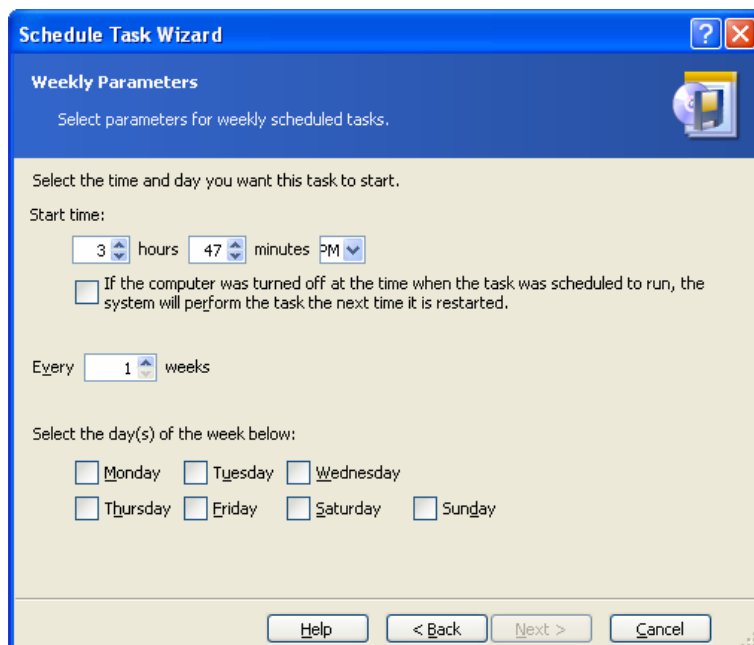
- **Every day**

- **Weekdays**

- **Every x days** – once in several days (specify the interval).
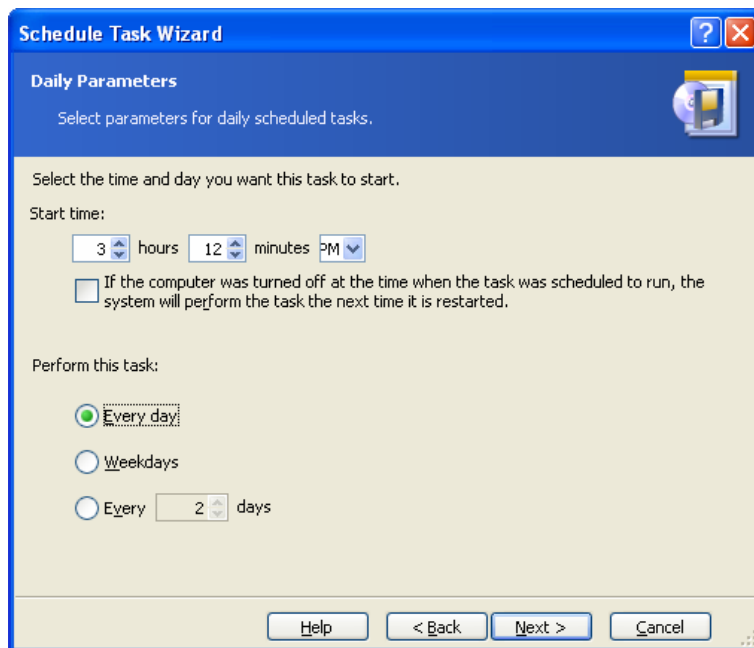
If the computer is off when the scheduled time comes, the task won't be performed, but you can force the missed task to launch at the next system startup by checking a box under the **Start time** fields.

8.1.2 Setting up weekly execution

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

If the computer is off when the scheduled time comes, the task won't be performed, but you can force the missed task to launch at the next system startup by checking a box under the **Start time** fields.

8.1.3 Setting up monthly execution

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

- **Day** – on the specified date

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

If the computer is off when the scheduled time comes, the task won't be performed, but you can force the missed task to launch at the next system startup by checking a box under the **Start time** fields.

8.1.4 Setting up one-time execution

If you select the one-time execution, set the **Start time** and date on which to execute the task:

If the computer is off when the scheduled time comes, the task won't be performed, but you can force the missed task to launch at the next system startup by checking a box under the **Start time** fields.

8.2 Managing scheduled tasks

The task Status, Schedule, Last Run Time and Last Result are shown on the **Active tasks** pane of the main window. To view the other task details, right-click on its name.

There are two ways of changing the task parameters. Editing allows you to change any task parameters. This is performed in the same way as creation, however, the earlier selected options will be set, so you have to enter only the changes. To edit a task, select it and click **Edit the Selected Task** on the **Active tasks** toolbar.

If you want to change only periodicity and/or start time, click **Schedule the Selected Task** on the **Active tasks** toolbar. Then you will have to perform only scheduling steps, leaving the backup settings the same.

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

To rename a task, select it, click **Rename the Selected Task** on the **Active tasks** toolbar, enter the new task name and press Enter.

Chapter 9. Managing Acronis Secure Zone

9.1 Creating Acronis Secure Zone

Acronis Secure Zone can be located on any local disk. It is created using unallocated space, if available, or at the expense of free space on a partition. A computer can have only one secure zone. To create a zone on another disk, you must first delete an existing zone.

When you click **Manage Acronis Secure Zone** in the menu, the program searches for the zone on all local drives. If a zone is found, the wizard will offer to delete or resize it. If there is no zone, you'll be prompted to create it.

1. Before creating the Acronis Secure Zone, you can estimate its size. To do this, start backup and select all data you are going to backup into the Acronis Secure Zone. At the **Set Backup Options** step choose **Set the options manually**, then set compression level. You will see the estimated full backup size. Multiply this by about 1.5 to be able to create incremental or differential archives.

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

3. Select the partitions from which space will be used to create the zone.
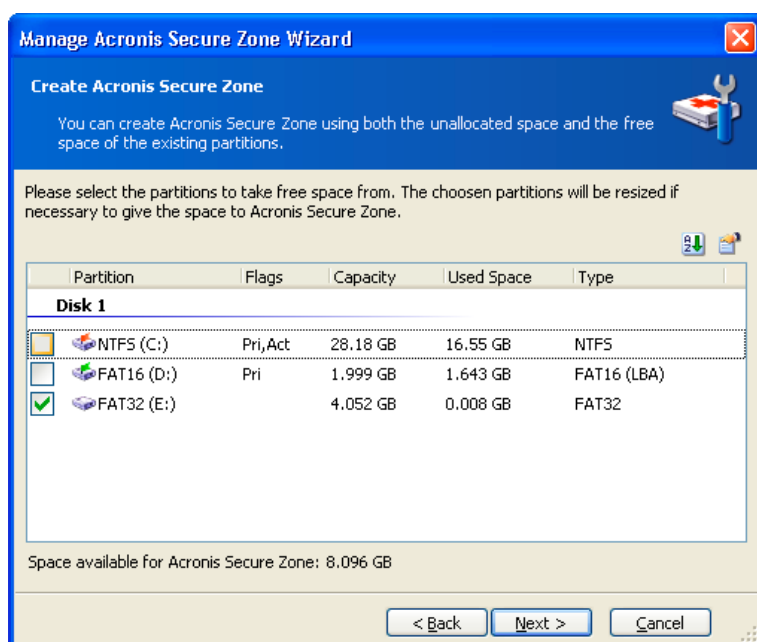
4. In the next window, enter the size of the zone or drag the slider.

5. After this, you will be prompted to activate Acronis Recovery Manager, to be able to start Acronis True Image Enterprise Server at boot time by pressing F11 key. Alternatively, you can activate this feature later from main program window.

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

After you click **Proceed**, Acronis True Image Enterprise Server will start creating the zone. Progress will be reflected in the 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. When prompted by the wizard, select **Manage Acronis Secure Zone**.

2. Select to increase or decrease the zone. You might need to increase it to provide more space for archives. The opposite situation might arise if either 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.
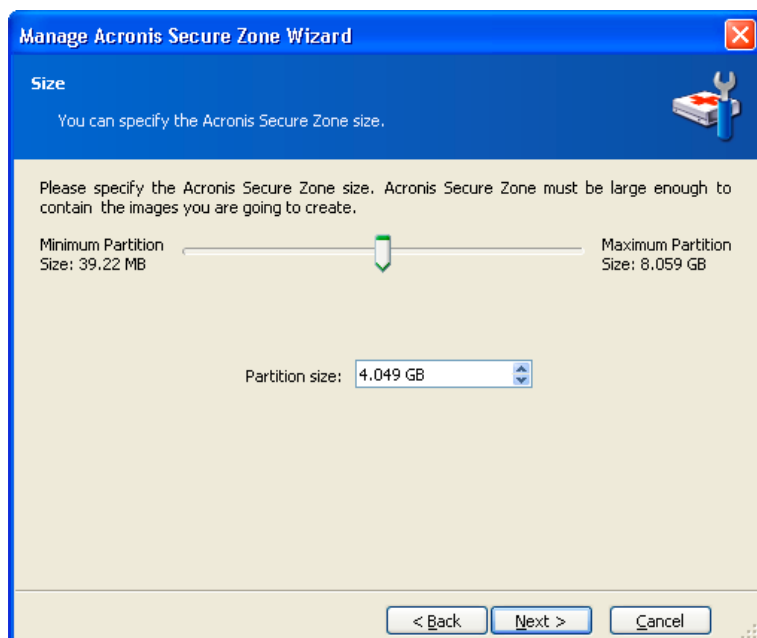
4. Enter the new size of the zone or drag the slider.

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

After you click **Proceed**, Acronis True Image Enterprise Server will start resizing the zone. Progress will be reflected in the 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 Deleting Acronis Secure Zone

1. When prompted by the wizard, select **Remove Acronis Secure Zone**.

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

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

After you click **Proceed**, Acronis True Image Enterprise Server 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 disable Acronis Startup Recovery Manager if it is activated and destroy all backups stored in the zone.

Chapter 10. Creating bootable media

You can run Acronis True Image Enterprise Server on a bare metal or on a crashed computer that cannot boot. You can also back up disks on a non-Windows computer, copying all its data sector-by-sector into the backup archive. To do so, you will need bootable media with the standalone Acronis True Image Enterprise Server version.

If you purchased the boxed product, you already have such a bootable CD, because the installation CD contains, besides the program installation files, the Acronis True Image Enterprise Server standalone bootable version.

If you purchased Acronis True Image Enterprise Server on the Web, you can create bootable media using the Bootable Media Builder. For this, you will need a CD-R/RW blank, several formatted diskettes (the wizard will tell you the exact number), or any other media your server can boot from, such as a Zip drive.

Acronis True Image Enterprise Server also provides the ability to create an ISO image of a bootable disk on the hard disk. If there is a Microsoft RIS server in your local network, an IT administrator can save the bootable data on this server as well. Then any networked computer will be able to boot any program from the RIS package.

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

> This feature is available both in Acronis True Image Enterprise Server local version and Acronis True Image Management Console. However, Acronis True Image Management Console does not contain Rescue Media Builder in its own installation. Therefore, to be able to create bootable media/RIS package from Acronis True Image Management Console, you must have Acronis True Image Enterprise Server local version or another Acronis product including Rescue Media Builder, installed on the same computer.

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

1. Click **Create Bootable Rescue Media** on the toolbar or the sidebar, or select **Create Bootable Rescue Media** from the **Tools** menu. You can also run the Bootable Rescue Media Builder without loading Acronis True Image Enterprise Server by selecting **Programs -> Acronis -> True Image -> Bootable Rescue Media Builder** from the **Start menu**.

2. Select which components of Acronis programs you want to place on the bootable media.
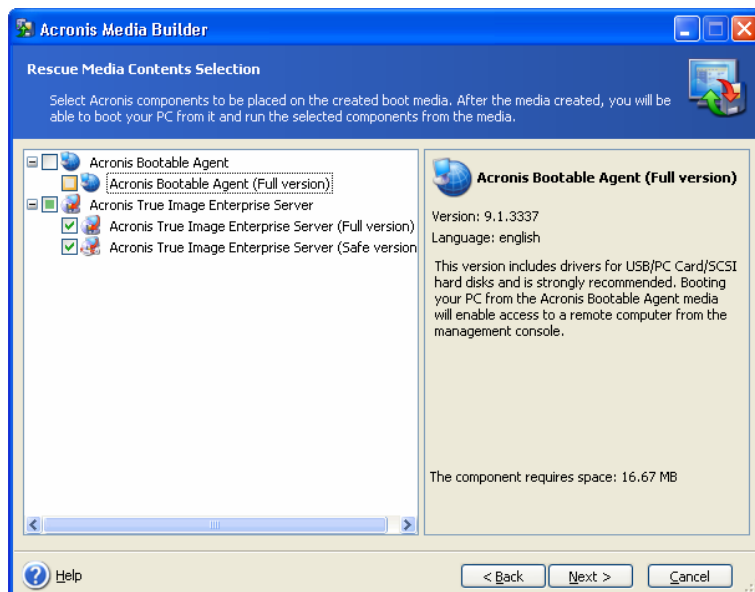
Acronis True Image Enterprise Server offers the following components:

- **Acronis True Image Enterprise Server full version**

Includes support of USB, PC Card and SCSI interfaces along with the storage devices connected via them, therefore is highly recommended.

- **Acronis True Image Enterprise Server safe version**

Does not include USB, PC Card, or SCSI drivers. Recommended for use in case of problems with running Full version

- **Acronis Bootable Agent full version**

The bootable version of Acronis True Image Agent. This component is designed to provide unattended restores from remote locations.

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

3. Select the type of bootable media (CD-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 or save bootable data on the RIS server.

Having created an ISO disk image, you will be able to burn it onto any kind of DVD recordable, using DVD recording software. Creating a bootable DVD directly from Bootable Media Builder is impossible.

When using 3.5″ diskettes, you will be able to write on a diskette (or a set of the diskettes) only one component at a time (for example, Acronis True Image Enterprise Server). To write another component, start Bootable Media Builder once again.
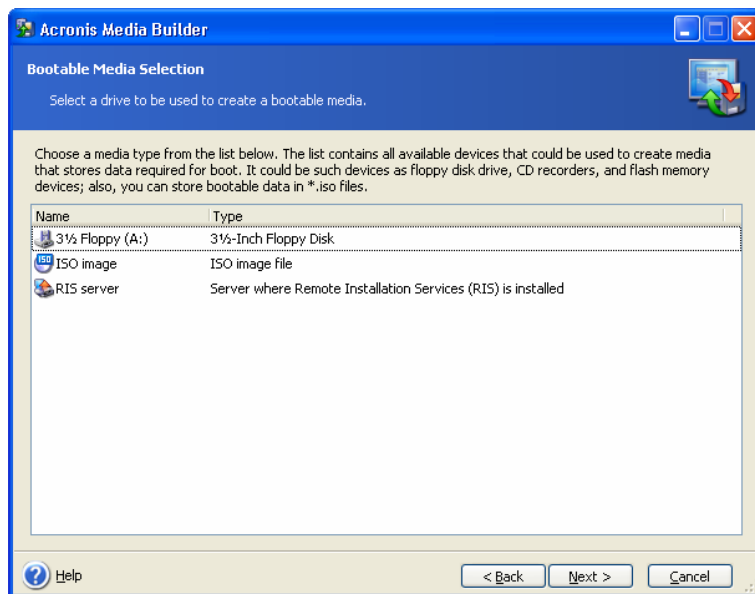
4. If you are creating a CD, DVD, diskettes or any removable media, insert the blank disk so the program can determine its capacity. If you chose to create a bootable disk ISO image, specify the ISO file name and the folder where to place it. If you chose to save bootable data on a RIS server, specify the server and provide the user name and password to access it.

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

After you create a boot disk, identify it and keep it in a safe place.

Chapter 11. Other operations

11.1 Validating backup archives

To be certain that your archives are not damaged, you can check their integrity.

1. To invoke the **Backup Archive Validation Wizard**, select **Validate Backup Archive** in the main window or in the **Tools** group or click **Validate Backup Archive** on the toolbar.

2. Click **Next**.

3. Select the archive to validate. If the archive is located in Acronis Secure Zone, select it to choose the archive on the next step.
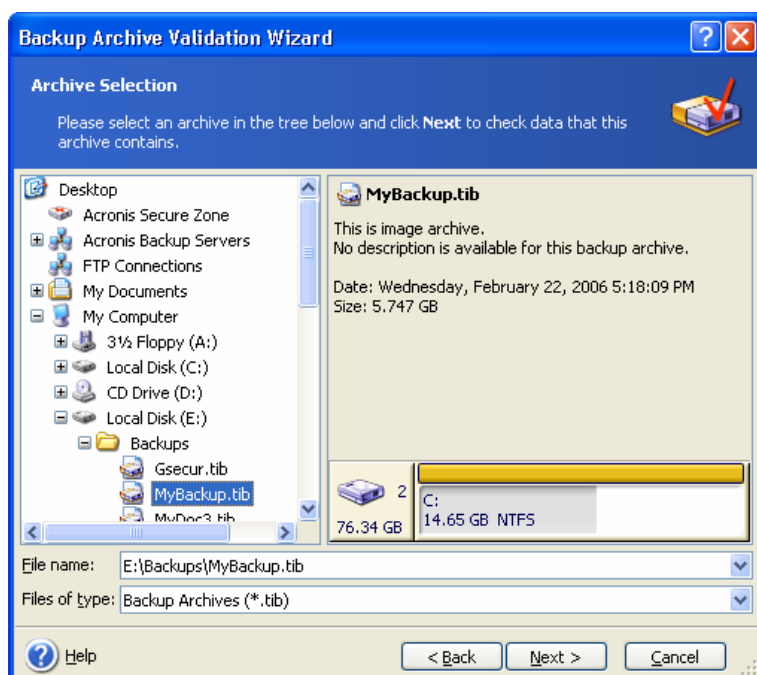
4. Click **Next**.

5. Clicking **Proceed** will launch the validation procedure. After the validation is complete, you will see the results window. You can cancel checking by clicking **Cancel**.

> To check data from an archive, containing incremental backups, you must have all incremental backup files and the initial full backup. If any of successive backups is missing in the archive, the validation is impossible.
>
> To check data from a differential backup, you must have the initial full backup as well.
>
> However, if you created several differential or both incremental and differential backups based on the same full backup (and therefore, in the same folder), you will need ALL of these successive backups to validate the archive.

## 11.2 Operation results notification

Sometimes a backup or restore procedure can last for 30 minutes or more. Acronis True Image Enterprise Server 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 the e-mail notification, select **Tools -> Options -> Notifications -> E-mail**:
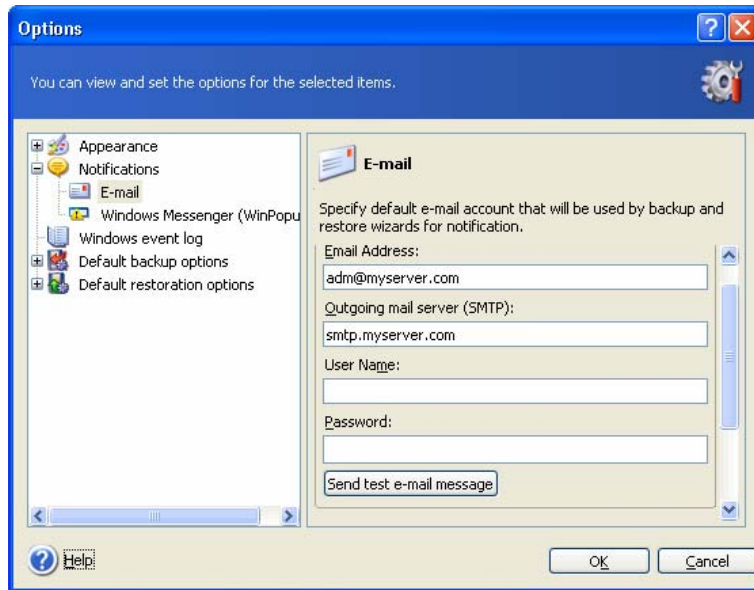
Provide the email address to which notifications will be sent and the outgoing SMTP server name. A user name and a password might also be needed if the SMTP server requires authentication.

Below in 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)

- when 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.

11.2.2 WinPopup notification

To set up WinPopup notification, select **Tools -> Options -> Notifications -> WinPopup**:
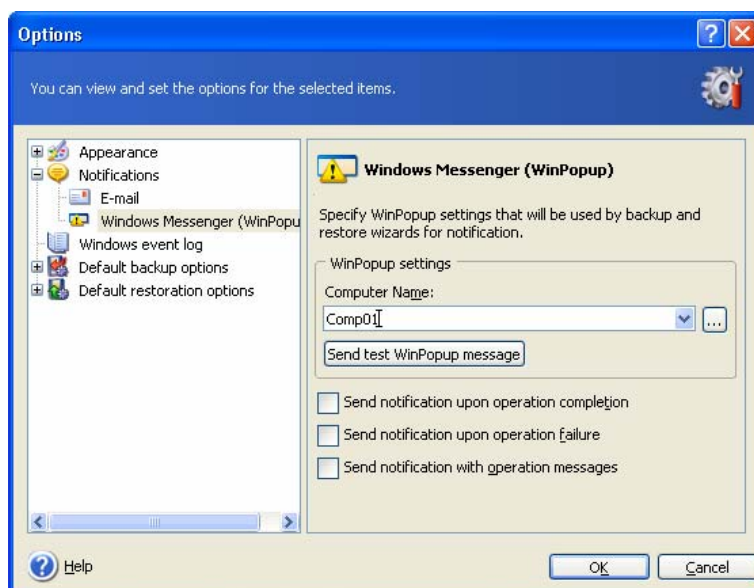
Provide the name of the computer to which notifications will be sent.

Below in 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 logs

Acronis True Image Enterprise Server allows users to view its working logs. They can provide information about scheduled tasks results, including reasons for failure, if any.

To invoke the log window, select **Show log** on the toolbar or from the **Tools** menu.

The log browsing window contains two panes: the left one features the log list, while the right one shows selected log contents.
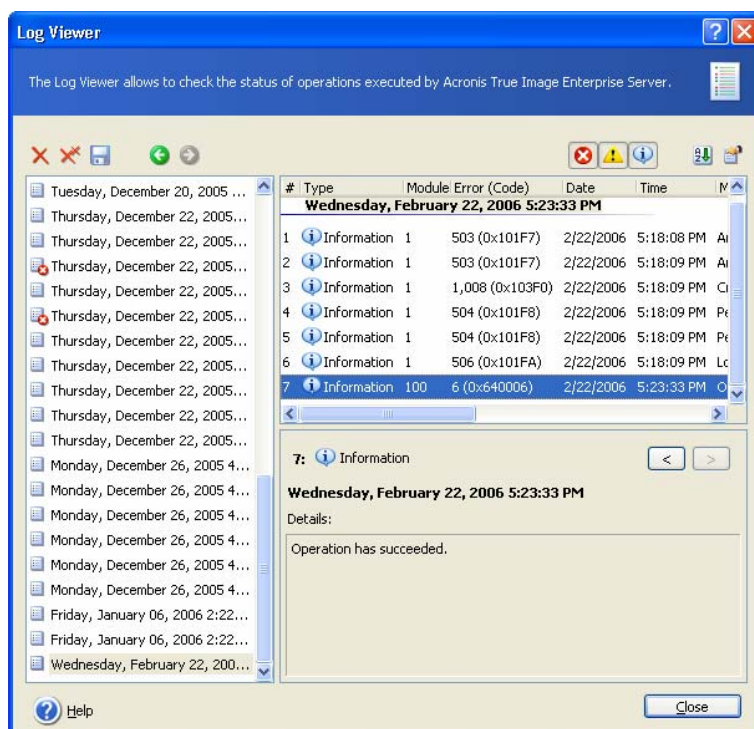
The left panel can contain up to 50 logs. If there are more, you can browse the list using the **More** and **Less** buttons with the left and right arrows.

To delete a log, select it and click **Delete**.

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

The right window features the list of steps contained in the selected log. The three buttons to the right control message filters: the white cross in the red circle filters error messages, the exclamation sign in a yellow triangle filters warnings, and the "i" in the blue circle filters information messages.

To select columns (step parameters) to display, right-click the headers line or left-click the **Choose Details** button. Then check the desired parameters.

To sort messages by a particular parameter, click its header (click again to reverse order) or the **Arrange Icons by** button (the second from the right) and select the desired parameter.

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

11.4 Event tracing

11.4.1 Windows event log

You can choose whether to store event log messages, issued by Acronis True Image Enterprise Server, to Windows Event Log (to see this log, run **eventvwr.exe** or select **Control Panel -> Administrative tools -> Event Viewer -> Application**).

The default setting – **Do not save messages**

To change this setting, select **Tools -> Options -> Windows event log**.

An additional choice is available between recording **All events, Warnings and Errors**, or **Errors only**.

11.4.2 SNMP notifications

You can choose whether to send event log messages, issued by Acronis True Image Enterprise Server, to computers, running SNMP (Simple Network Management Protocol) management applications.

The default setting – **Do not send messages to SNMP clients**

Having chosen **Send messages to SNMP clients**, specify a name or IP address of the client computer. Otherwise messages will be sent to all SNMP clients found in the local network.

An additional choice is available between sending **All events, Warnings and Errors**, or **Errors only** messages.

Acronis True Image Enterprise Server provides the following SNMP objects to SNMP management applications:

1.3.6.1.4.1.24769.100.200.1.0 - string identifying a type of occurred event (Information, Warning, Error)

1.3.6.1.4.1.24769.100.200.2.0 - string containing text description of occurred event (it looks identically to messages published by Acronis True Image Enterprise Server in its log).

11.5 Managing System Restore

Microsoft Windows System Restore tool, available in Windows XP and Windows 2003 Server operating systems, is used to undo harmful changes to the system without losing recently changed or created user data. To run the System Restore tool or find out more about it, select **Start -> Programs -> Accessories -> System Tools -> System Restore**. (Please be aware that the older Windows Server versions do not feature System Restore, therefore, under these operating systems **Manage System Restore** tool is unavailable.)

If you run Acronis True Image Enterprise Server regularly, this feature in your operating system is redundant. You can turn it off, freeing up to 12% of your hard disks space, directly from Acronis True Image Enterprise Server.

This feature is available in Acronis True Image Enterprise Server local version only. Managing System Restore using Acronis True Image Management Console is impossible.

1. To invoke the **System Restore Management Wizard**, select **Manage System Restore** from the menu or from the **Tools** group, or click **Manage System Restore** on the toolbar.

2. Click **Next**.

3. Now you can turn on/off System Restore on all your hard disk(s) partitions at once or do it individually for each partition.

> Note that you cannot turn off System Restore on the system disk (partition), yet keep it on other disks (partitions).

4. Click **Next**.

5. The program lists the configured changes. You can click **Back** to choose different settings. If you click **Cancel**, all new settings will be lost. Click **Proceed** to apply the changes.

> If you turn off System Restore on any disk or partition, all previously created restore points for that disk (partition) will be deleted. Please make sure you do not need those restore points before proceeding.

Chapter 12. Mounting an image as a virtual drive

Acronis True Image Enterprise Server can **mount partition images as virtual drives**, thus letting you access them as though they were physical drives. This 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.

> This feature is available in Acronis True Image Enterprise Server local version only. Mounting images using Acronis True Image Management Console is impossible.

> Please keep in mind that, though both file archives and disk/partition images have a default ".tib" extension, only **partition images** can be mounted. If you want to view file archive contents, use the Restore Data Wizard (see *7.2 Restoring files and folders from file archives*, steps 1-9).

> The current version of Acronis True Image Enterprise Server can mount an image archive only if all its volumes reside in the same directory. If your archive spans several CD-R/RW discs and you wish to mount the image, you should copy all volumes to a hard disk drive or network drive.

12.1 Mounting an image

1. Invoke the **Mount Image Wizard** by clicking on the **Mount Image** operation icon in the main program window.

2. Click **Next**.

3. Select the archive from the drives tree. If the archive is located in Acronis Secure Zone, select it to choose the archive at the next step.
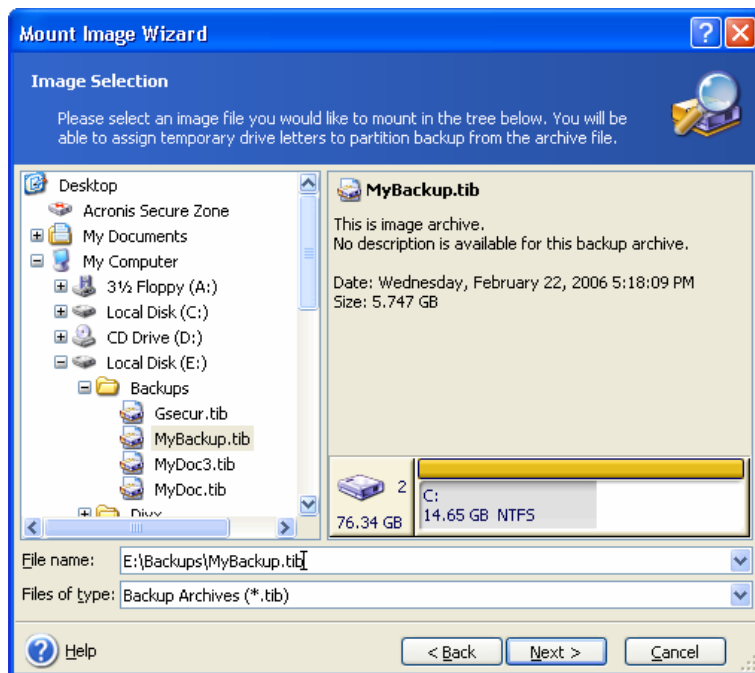
If you added a comment to the archive, it will be displayed to the right of the drives tree. If the archive was protected with a password, Acronis True Image Enterprise Server will ask for it. Neither the partitions layout, nor the **Next** button will be enabled until you enter the correct password.

4. Click **Next**.

5. If you are to mount an incremental image, Acronis True Image Enterprise Server will suggest that you select one of successive incremental archives by date/time of its creation. Thus, you can explore the partition state to a certain moment.

> To mount an incremental image, you must have all previous incremental images and the initial full image. If any of successive images is missing, connection is impossible.

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

6. Click **Next**.

7. Select a partition to mount as a virtual disk. (Note that you cannot mount the entire disk.)

You can also select a letter to be assigned to the virtual disk from the **Drive letter** drop-down list. If you do not want to assign a letter to the virtual drive, select **Do not assign**.
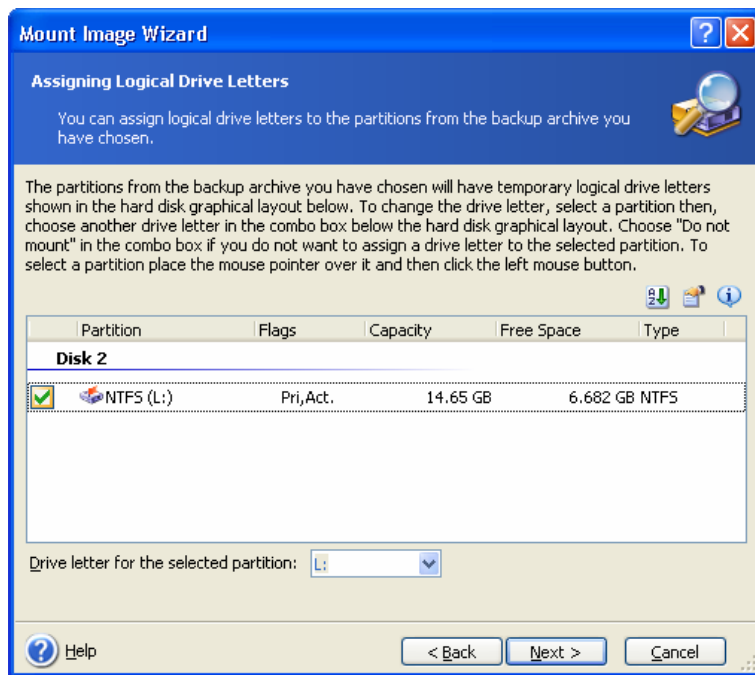
8. Click **Next**.

9. Select whether you want to mount image in **Read-only** or **Read/Write** mode.

10. Click **Next**.

11. If you select **Read/Write** mode, the program assumes that the connected 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 comment to this file.

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

13. After the image is connected, the program will run Windows Explorer, showing its contents. Now you can operate 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.

12.2 Unmounting an image

We recommend that you unmount the virtual disk after all necessary operations are finished, as keeping up virtual disks takes considerable system resources. If you do not, the virtual disk will disappear after your server is turned off.

To disconnect the virtual disk, click **Unmount Image** and select the disk to unmount. You can also unmount the disk in Windows Explorer by right-clicking on its icon and selecting **Unmount**.

Chapter 13. Transferring the system to a new disk

13.1 General information

Sooner or later any server user finds out that his 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. In this case, you have to transfer the system to a higher-capacity hard disk.

> This feature is available in Acronis True Image Enterprise Server local version only. Transferring systems using Acronis True Image Management Console is impossible.

To transfer the system, you must first install the disk in the server. If a server doesn't have a bay for another hard disk, you can temporarily install it in place of your CD-ROM. If that is not possible, you can clone a hard disk by creating its 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 several simple actions to transfer all the data, including partitions, folders and files, to a newer 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 older 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 corresponding 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) until data transfer is completed.

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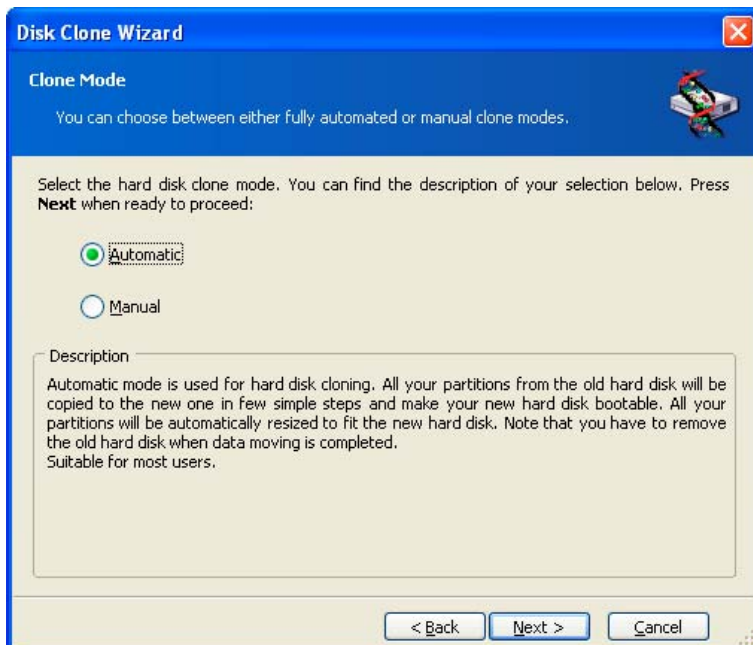
We recommend using automatic mode in most cases. The manual mode can be useful if you need to change the disk partition layout.

If the program finds two disks, one partitioned and another unpartitioned, it will automatically recognize the source disk as the partitioned disk and the destination disk as the unpartitioned disk, so the next two steps will be bypassed.

13.3.2 Selecting source disk

If the program finds several partitioned disks, it will ask you which is the source (i.e. the older data disk).
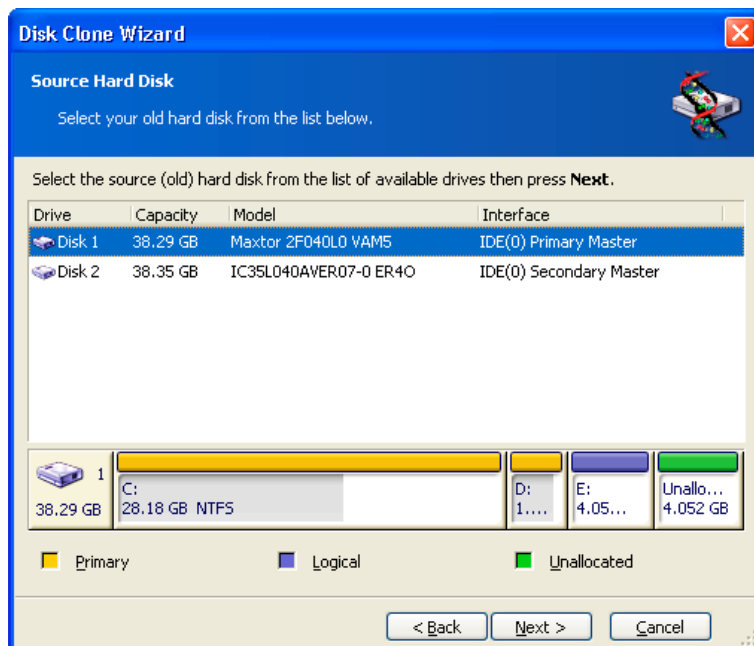
You can determine the source and destination using the information provided in this window (disk number, capacity, label, partition and file system information).

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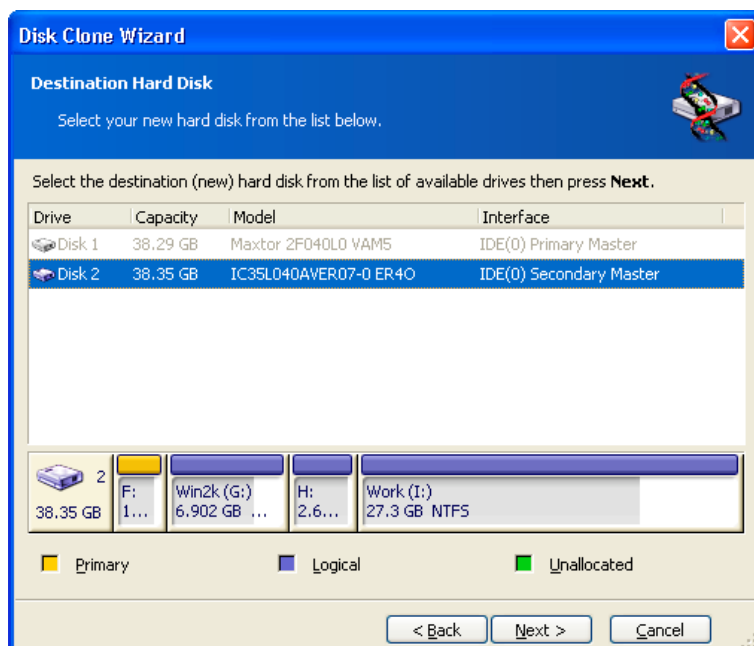
The previously selected source becomes grayed-out and disabled for selection.

If either 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 **Nonempty Destination Hard Disk** window stating that the destination disk contains partitions, perhaps with data.

You will have to select between:

- **Delete partitions on the destination hard disk** – all existing partitions will be deleted during cloning and all their data will be lost.
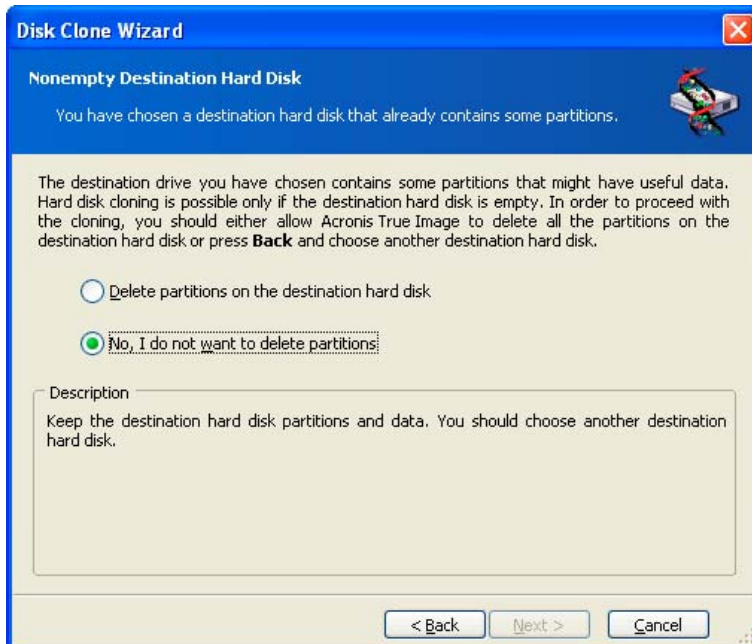
- **No, I do not want to delete partitions** – no existing partition will be deleted, discontinuing the cloning operation. You will only be able to cancel this operation and return to select another disk.

To continue, select the first choice and click **Next**.

> 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.**

13.3.5 Old and new disk partition layout

If you selected the automatic mode before, the program will ask you for nothing further. You will see the window graphically illustrating information (as rectangles) 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.

Next you will see the cloning summary.

13.3.6 Old disk data

If you selected the manual mode, the program will ask you what to do with the old disk:

- **Create a new partition layout** – All existing partitions and their data will be deleted (but they will also be cloned to the new disk, so you won't lose them)

- **Keep data** – leave the old disk partitions and data intact
- **Destroy data** – destroy all data on the old disk.
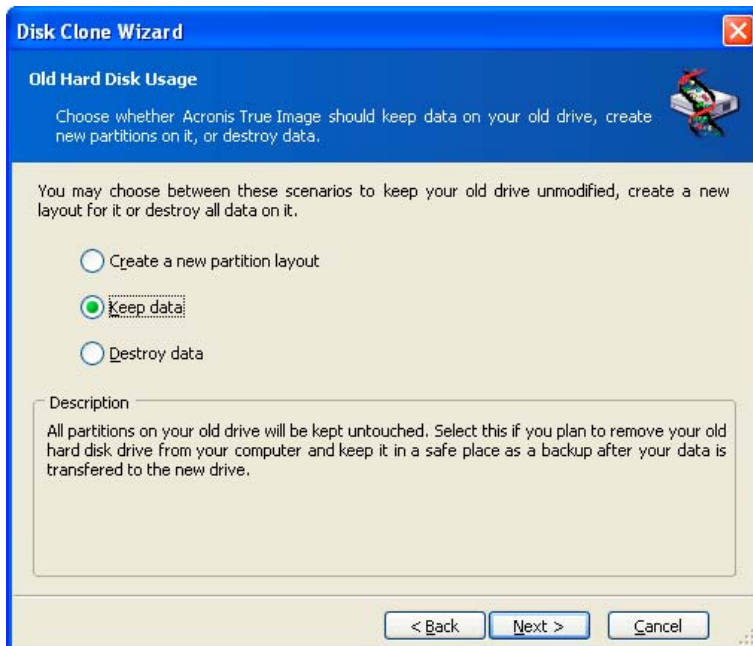
If you are going to sell or give away your old disk, we recommend that you make sure you destroyed the data on it.

If you are going to keep it for data storage, you can create a new partition layout on it. In this case, the disk will be ready right after cloning is complete.

To protect yourself from unforeseen consequences, it would be better to leave the old disk data intact, as you will be able to delete it later.

13.3.7 Destroying the old disk data

If you elected to destroy the old disk data in the previous step, you will have to select the destruction method now:

- **Quick** – quick one-pass destruction
- **Normal** – multipass destruction
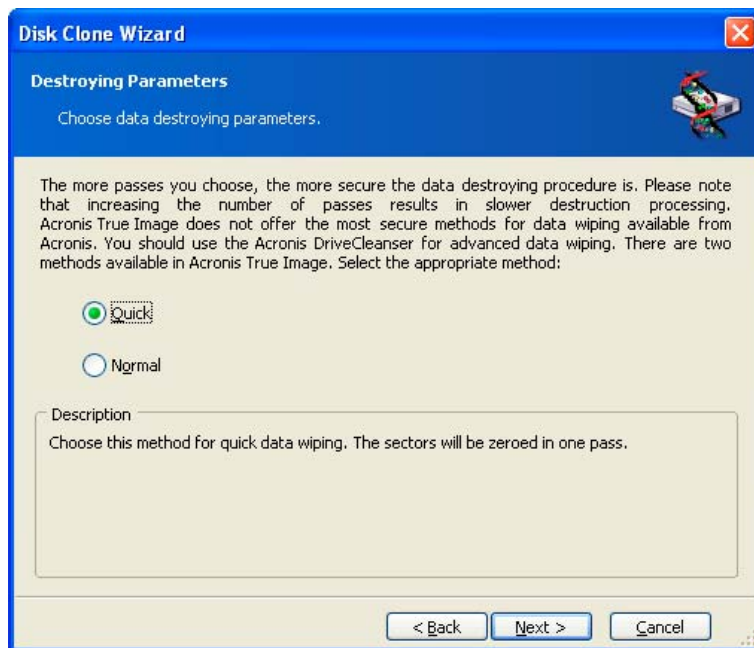
The second method takes more time, but makes it impossible to recover data afterwards, even with special equipment.

The first method is less secure, but is still suitable for most cases.

13.3.8 Selecting partition transfer method

Acronis True Image Enterprise Server will offer you the following data transfer 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
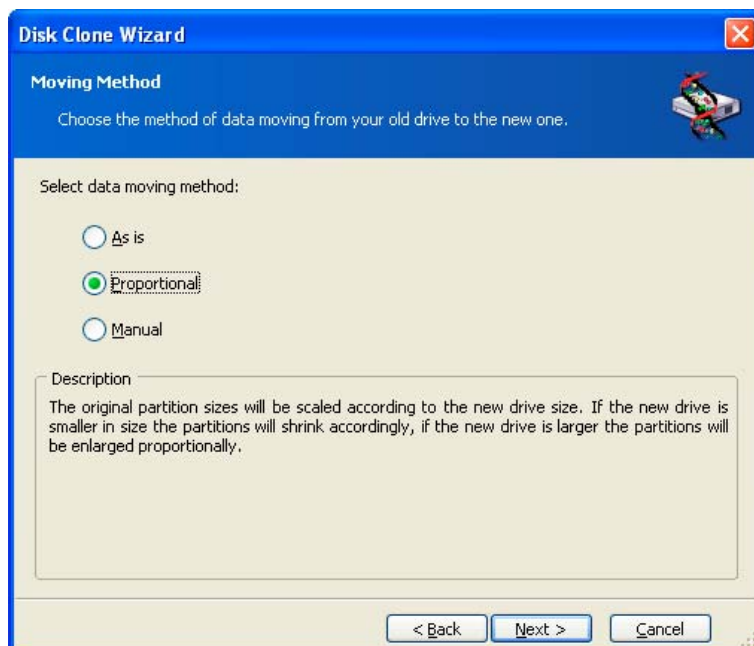
If you elect to transfer information "as is," a new partition will be created for every old one with the same size and type, file system and label. The unused space will become

unallocated. Further, 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 inexpedient, as they leave much unallocated space on the new disk. Using the "as is" method, Acronis True Image Enterprise Server 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 the 4 GB size limit.

Depending on the selected combination, you will proceed to either the old disk partitioning window, or the disk partition layout window (see below).

13.3.9 Partitioning the old disk

If you selected **Create a new partition layout** earlier in the process, it is now time to repartition your old disk.

During this step, you will see the current disk partition layout. Initially, the disk has unallocated space only. This will change when you create new partitions.

Having completed the required steps, you will add a new partition. To create another one, simply repeat those steps.

If you make a mistake, click **Back** to redo.

After you create the necessary partitions, uncheck the **Create new partition in unallocated space** box and click **Next**.

13.3.10 Old and new disk partition layouts

In the next window, you will see rectangles indicating the source hard disk, including its partitions and unallocated space, as well as the new disk layout.
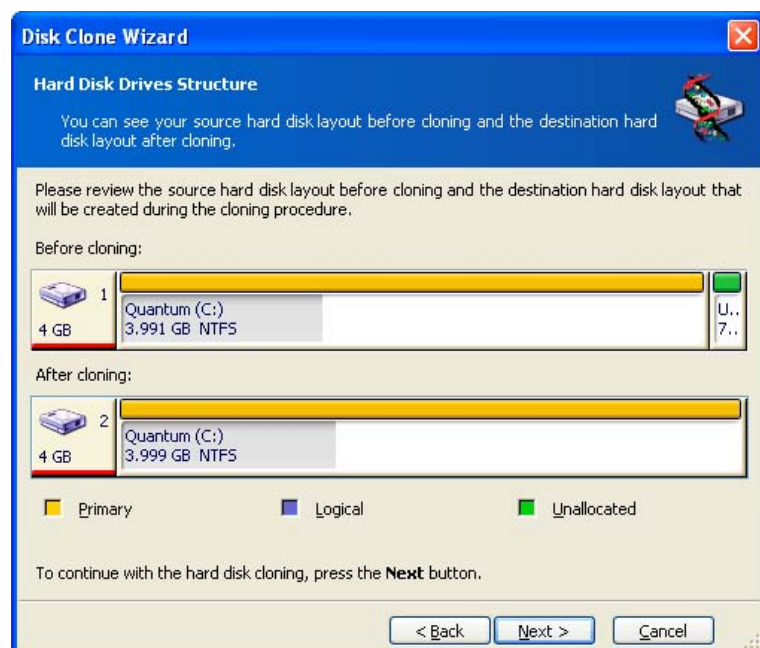
Along with the hard disk number, you will also see disk capacity, label, partition and file system information. Different partition types, including primary, logical and unallocated space are marked with different colors.

If you have selected manual partition creation before, the partition layout will look different. This partitioning method is described below.

13.3.11 Cloning summary

In the next window, you will see a list of briefly described operations to be performed on the disks.
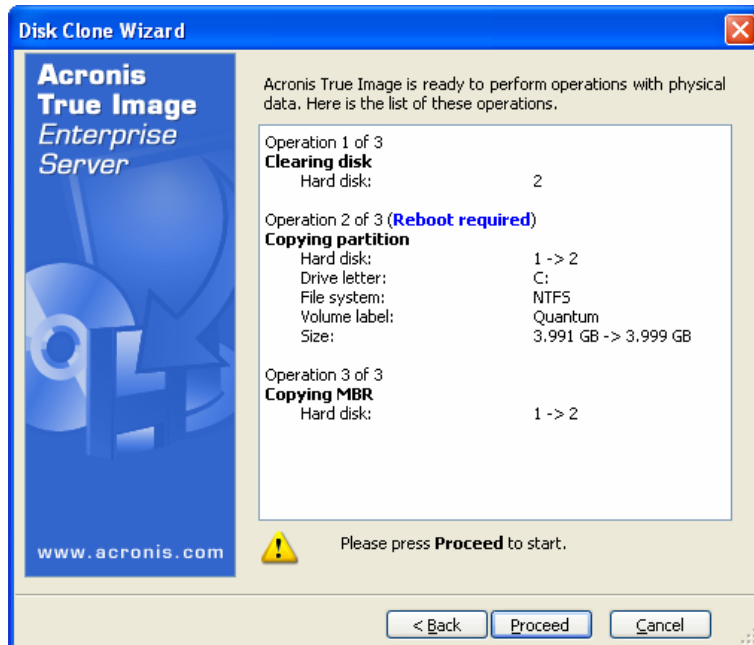
Cloning a disk containing the currently active operating system will require reboot. In that case, after clicking **Proceed** you will be asked to confirm the reboot. Canceling the reboot will cancel the entire procedure.

Cloning a non-system disk or a disk containing an operating system, but not active one at the moment, will proceed without reboot. After you click **Proceed**, Acronis True Image Enterprise Server will start cloning the old disk to the new disk, indicating the progress in the 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 operation is complete, you will see the results message.

13.4 Cloning with manual partitioning

13.4.1 Old and new disk partition layouts

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 rectangles indicating the source hard disk, including its partitions and unallocated space, as well as 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.
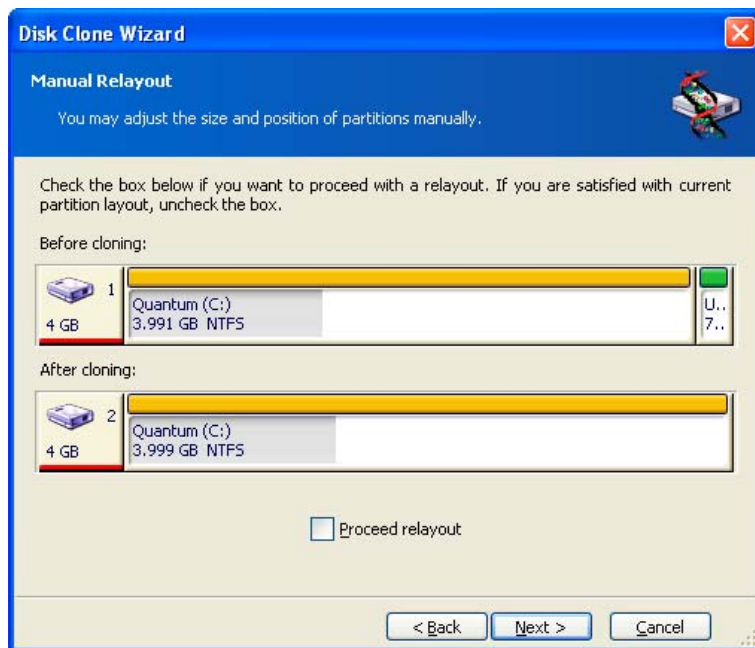
To resize either partition, check the **Proceed relayout** box. If you are satisfied with the partition layout shown, uncheck this box (if checked). Clicking **Next**, you will proceed to the cloning summary window.

Be careful! Clicking **Back** in this window will reset all size and location changes that you've selected, so you will have to specify them again.

First, select a partition to resize. It will be underlined in red.

Resize and relocate it on the next step.

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

If the cursor turns to 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 to 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 **Next**. You will be taken two steps back to the partition layout. You might have to perform some more resizing and relocation before you get the layout you need.

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 server has space for another disk, it would be easier to add a data disk drive than to clone a system one.

This feature is available in Acronis True Image Enterprise Server local version only. Adding disks using Acronis True Image Management Console is impossible.

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

14.1 Selecting a hard disk

Select the disk that you've added to the server.
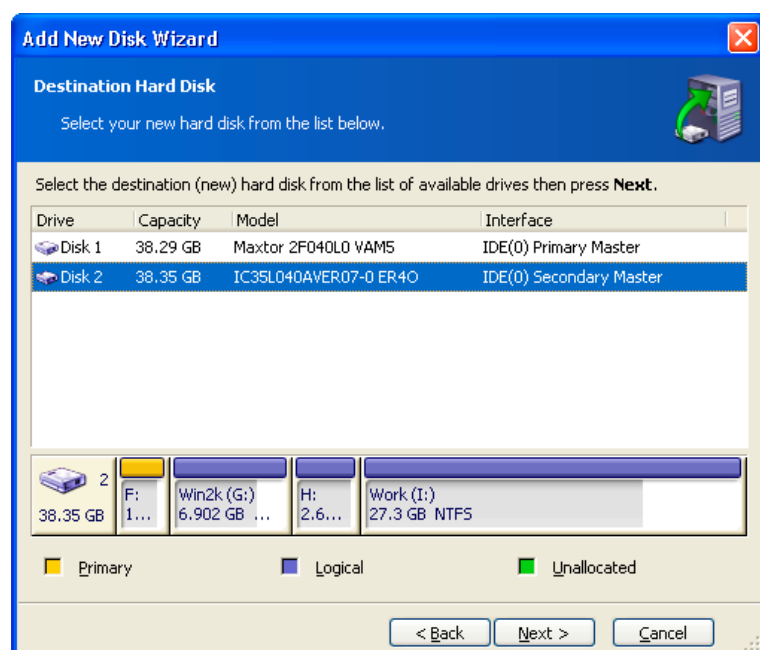
This window might be bypassed if the program detects the new disk itself. In this case, you will immediately proceed to the new partition creation.

If there are any partitions on the new disk, they must be deleted first.

Select **Delete partitions on the destination hard disk** and click **Next** 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, select **Create new partition in unallocated space** and click **Next** to perform steps required by the partition creation wizard.

You will be prompted to set the new partition location and size. You can do this by both entering values to **Unallocated space before, Partition size, Unallocated space after** fields, by dragging partition borders or the partition itself.

Copyright © Acronis, Inc., 2000-2006

If the cursor turns to 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 to 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). Having provided the new partition location and size, you can input a label for the new partition.

If you make a mistake at partitioning, click **Back** to redo the process.

Finally, you will be taken back to the partition layout screen. Check the resulting partitions layout and start creating another partition or move on by unchecking **Create new partition in unallocated space** and clicking **Next**.

14.3 Disk add summary

The disk add summary contains a list of operations to be performed on disks.
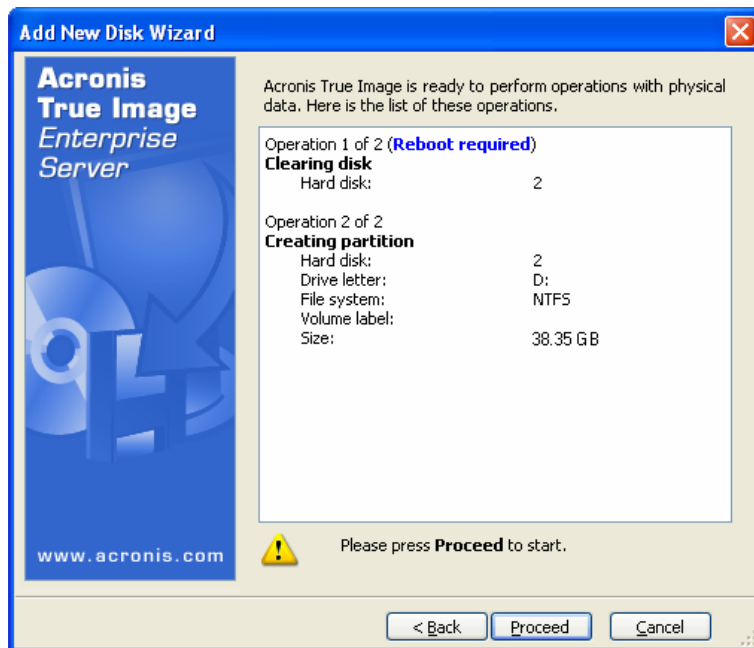
After you click **Proceed**, Acronis True Image Enterprise Server will start creating and formatting new partitions, indicating the progress in the special window. You can stop this procedure by clicking **Cancel**. In that case, you will have to repartition and format the new disk or repeat the disk add procedure.

Chapter 15. Command-line mode and scripting

Acronis True Image Enterprise Server (local version) supports the command-line mode, as well as the GUI mode, and can be used to execute XML scripts.

15.1 Working in the command-line mode

An administrator might need a console interface in some situations. Acronis True Image Enterprise Server supports this mode with **TrueImageCmd.exe** utility. The file is located in a folder where Acronis True Image Enterprise Server has been installed, by default it is

C:\Program Files\Acronis\TrueImageEnterprise.

15.1.1 Supported commands

TrueImageCmd has the following format:

```
trueimagecmd /[command] /[option1] [option2]…
```

The following commands are supported (each command may be accompanied by additional options):

1. create

Creates an image file with the specified file name. A complete image is created by default. Use the /incremental option to create an incremental image.

Options

```
/progress:[on | off]
```

Shows/hides the progress information (percent completed). It is shown by default.

```
/filename:[filename]
```

Sets the image file name.

```
/password:[password]
```

Protects an image with a password.

```
/net_user:[username]
```

Specifies a user name when creating an image on a network drive.

```
/net_password:[password]
```

Specifies a user password when creating an image on a network drive.

```
/harddisk:[disk number]
```

Specifies the hard disks to include into the image file by numbers. The list of available hard disks is provided by the /list command. An image may contain data of more than one hard disk. In that case, separate disk numbers by commas, e.g.:

```
        /harddisk 1,3
```

```
/partition:[partition number]
```

Specifies the partitions to include into the image file by numbers. The list of available partitions is provided by /list. Partition numbers are specified as <disk number>-<partition number>, e.g.:

```
/partition: 1-1,1-2,3-1
```

`/file_partition:[partition letter]`

Specifies the partition where the image file will be stored (by letter or number). This option is used with /filename:file_name. In that case the file name must be specified without drive letter or root folder. For example:

```
/file_partition:D /filename:"\1.tib"
```

`/raw`

Use this option to create an image of a disk (partition) with unrecognized or unsupported file system. This will copy all disk/partition contents sector-by-sector. Without this option only the sectors containing useful system and user data are imaged.

`/compression:[0...9]`

Specifies the image compression level. It ranges from 0 to 9 and is set to 3 by default.

`/incremental`

Sets the image type to incremental. If there is no a basic image file to append an incremental one, a complete image will be created.

`/split:[size in MB]`

Splits image file into parts of the specified size.

`/reboot`

Reboots the server after the operation is completed.

`/log:[file name]`

Creates a log file of the current operation with the specified file name.

2. deploy

Restores a disk or partition from an image.

Options

`/filename:[filename]`

Specifies the name of the image file to restore.

`/net_user:[username]`

Specifies a user name when restoring an image from a network drive.

`/net_password:[password]`

Specifies a user password when restoring an image from a network drive.

`/file_partition:[partition letter]`

Specifies the partition where the image file is stored (by letter or number). This option is used with /filename:file_name. In this case the file name must be specified without drive letter or root folder. For example:

```
/file_partition:D /filename:"\1.tib"
```

`/password:[password]`

Specifies the password for the image file (if required).

`/harddisk:[disk number]`

Specifies the hard disks to restore by numbers.

`/partition:[partition number]`

Specifies the partitions to restore by numbers.

`/target_harddisk:[disk number]`

Specifies the hard disk number where the image will be restored.

`/start:[start sector]`

Sets the start sector for restoring a partition to the hard disk unallocated space.

`/size:[partition size in sectors]`

Sets the new partition size (in sectors).

`/type:[active | primary | logical]`

Sets the new partition type. By default (if this option is not defined) an active partition is created on the first hard disk and logic partitions on other disks.

`/target_partition:[partition number]`

Specifies the target partition number for restoring a partition over the existing one. If the option is not specified, the program assumes that the target partition number is the same as the partition number specified with the /partition option.

`/reboot`

Reboots the server after the operation is completed.

`/log:[file name]`

Creates a log file of the current operation with the specified file name.

3. list

Lists the available drives and partitions.

Options

`/filename:[filename]`

Lists the image file contents.

`/password:[password]`

Specifies the password for the image file (if required).

4. clone

Clones a hard disk.

Options

`/harddisk:[disk number]`

Specifies a source hard disk which will be cloned to the new hard disk.

`/target_harddisk:[disk number]`

Specifies the target hard disk number where the source hard disk will be cloned.

5. explore

Connects an image file as a virtual drive.

Options

`/filename:[image file name]`

The image file name.

`/password:[image password]`

The password for the image file (if required).

`/partition:[partitions list]`

Specifies a list of partitions to be mounted as virtual drives. Without this option, all partitions stored in the image file will be mounted.

`/letter`

Assigns letters to the mounted drives. This option is used with /partition option only.

`/net_user:[username]`

Specifies a user name when exploring an image from a network drive.

`/net_password:[password]`

Specifies a user password when exploring an image from a network drive.

`/log:[file name]`

Creates a log file of the current operation with the specified file name.

6. unplug

Unmounts the image file connected as a virtual drive.

Options

`/letter:X`

Specifies the virtual disk to be disconnected by letter.

`/letter:all`

Disconnects all virtual drives.

7. asz_create

Creates Acronis Secure Zone on the selected drive.

Options

`/harddisk:X`

Specifies the hard disk number where the Acronis Secure Zone will be created.

`/partition:[partitions list]`

Specifies partitions from which free space will be taken for Acronis Secure Zone creation.

```
/size:[ASZ size in sectors]
```

Sets the Acronis Secure Zone size (in sectors). If this size is not specified, it will be set as average between maximal and minimal values, including unallocated spaces on the all listed partitions.

```
/asz_activate
```

Activates the Acronis Secure Zone after creation (or, rather, activates Acronis Startup Recovery Manager).

/asz_activate option will not take effect, if the system partition is resized during Acronis Secure Zone creation. Use /asz_activate command to activate Acronis Secure Zone after it is created.

```
/reboot
```

Reboots the server after the Acronis Secure Zone is created.

```
/log:[file name]
```

Creates a log file of the current operation with the specified file name.

8. asz_delete

Deletes the Acronis Secure Zone from your hard disk.

Options

```
/partition:[partitions list]
```

Specifies partitions to which free space will be added after the Acronis Secure Zone is deleted. If you specify several partitions, the space will be distributed proportionally to each partition's size.

```
/log:[file name]
```

Creates a log file of the current operation with the specified file name.

9. asz_activate

Activates the Acronis Secure Zone (or, rather, activates Acronis Startup Recovery Manager). This command may also be used as an option with 'asz_create' command.

10. verify

Verifies the image archive data integrity.

Options

```
/filename:[filename]
```

Specifies the name of the image file to verify.

```
/password:[image password]
```

Specifies the password for image file (if required).

```
/net_user:[username]
```

Specifies a user name when verifying an image from a network drive.

```
/net_password:[password]
```

Specifies a user password when verifying an image from a network drive.

11. help

Shows help for commands.

15.1.2 trueimagecmd.exe usage examples

1. Create image

```
trueimagecmd /create /filename:"C:\Test\1.tib" /partition:2-
1,1-3
```

- This will create an image named **1.tib** of the partitions 2-1 and 1-3. Image will be saved to c:\Test\ folder.

```
trueimagecmd /create /filename:"\Test\1.tib" /partition:2-1,1-
3 /file_partition:3-1
```

- This will create an image named **1.tib** of the partitions 2-1 and 1-3. Image will be saved to partition 3-1.

```
trueimagecmd /create /filename:"C:\Test\1.tib"
/password:qwerty /harddisk:2 /reboot /raw /incremental
/compression:5 /split:640 /progress:off
```

- This will append an incremental image to the image named 1.tib of hard disk 2. The image will be saved to c:\Test\ folder, protected with password "qwerty", split into parts of 640 MB, and contain all cluster data. Image compression level is 5. The server will be rebooted after the operation is completed.

2. Restore image

```
trueimagecmd /deploy /filename:"C:\Test\1.tib" /partition:2-1
```

- This will restore partition 2-1 from image 1.tib.

```
trueimagecmd /deploy /filename:"C:\Test\1.tib"
/password:qwerty /harddisk:2
```

- This will restore hard disk 2 from image 1.tib, protected with password 'qwerty'.

```
trueimagecmd /deploy /filename:"C:\Test\1.tib" /partition:2-1
/target_partition:1-1
```

- This will restore partition 2-1, stored in image 1.tib, to partition 1-1.

```
trueimagecmd /deploy /filename:"C:\Test\1.tib" /partition:2-1
/target_harddisk:3 /start:0 /size:64000 /type:logical
```

- This will restore partition 2-1, stored in image 1.tib, to hard disk 3. A new logical partition will be created on disk 3 from 0 to 64000 sector.

```
trueimagecmd /deploy /filename:z:\Server30Cdrive.tib
/partition:1-1 /target_partition:2-1 /type:active
/password:123qwe
```

- This will restore partition 1-1, stored in image Server30Cdrive.tib, protected with password '123qwe', to partition 2-1. The restored partition will be of active type.

3. List

```
trueimagecmd /list
```

- This will list available partitions.

4. Clone

```
trueimagecmd /clone /harddisk:2 /target_harddisk:3
```

- Clone hard disk 2 to hard disk 3.

5. Explore image

```
trueimagecmd /explore /filename:\\myserver\backup\mybackup.tib
/net_user:john /net_password:qwerty
```

- This will connect all images, stored in file mybackup.tib on the network drive, as virtual drives.

15.1.3 Command-line mode usage under DOS

For use in the MS-DOS compatible environments Acronis True Image Enterprise Server includes the **TrueImageCmdDos.exe** utility. It is located in a folder where Acronis True Image Enterprise Server has been installed, by default it is C:\Program Files\Acronis\TrueImageEnterprise.

15.2 Scripting

15.2.1 Script execution parameters

Scripts are executed by the **TrueImageTerminal.exe** utility located in the Acronis True Image Enterprise Server installation folder (i.e. C:\Program Files\Acronis\TrueImageEnterprise). This utility is also used to monitor backup progress.

TrueImageTerminal execution parameters:

TrueImageTerminal.exe [arguments]

Arguments include the following:

/help – outputs help information about TrueImageTerminal.exe parameters.

/progress – outputs progress of backup operations run either from Acronis True Image Enterprise Server graphics user interface, or from the script.

/execute: [script file name] – executes a script. If there are several scripts to be executed, they are queued. An example for executing MyBackup.tis script:

```
TrueImageTerminal.exe /execute:C:\MyBackup.tis
```

/nowait – an optional script execution argument. Enables to terminate TrueImageTerminal before backup is finished. Example:

```
TrueImageTerminal /execute:C:\MyBackup.tis /nowait
```

> By pressing **Ctrl+C** you can force backup progress output off and switch TrueImageTerminal to background operation.

> You can terminate backup operation executed by TrueImageTerminal by pressing **Ctrl+B**.

15.2.2 Script structure

Scripts are written in the XML language and you can use the following tags:

Source. Specifies the partitions or disks to be imaged. Letters assigned to partitions must be used without colon. Disk numbers correspond to their system numbers. To create images of several partitions or disks, use the SOURCE tag for each of them, e.g.:

```
<source letter ="C" />

<source letter ="D" />

<source disk ="1" />

<source disk ="2" />
```

Target. Specifies the name and the location of an image file, e.g.:

```
<target file="E:\Mybackup2.tib" username="username"
password="password" />
```

username and *password* parameters are optional. They are used to access networked resources.

As a target for the image files you can indicate CD-R/RW or tape drive.

Options. This tag can be used with a number of additional parameters:

Compression: specifies the backup compression level. Can be *None, Low, Normal, High*.

Incremental: specifies if you need to create an incremental image file. If equal to "false" (or "0"), a complete image file will be created. If there is already a file with the name specified, it will be replaced without warnings. If equal to "true" (or "1") and there is already a file with the name specified, an incremental image will be created. Otherwise the program will create a complete image file. The default value for this parameter is "true".

Description: adds a description to an image file. The comment must be a single string (though its length is not limited.)

Split: splits a large image file into a number of smaller files of the specified size, which can be provided in bytes, kilobytes, megabytes, etc.

Password: adds password protection to an image file.

15.2.3 Script usage examples

The following example illustrates the usage of a script to backup two partitions (logical drives), C and F. *mybackup2.tib* is specified as an incremental image file. High compression level is selected and the image is to be split into 650MB parts for recording to CD-R/RW media. Password protection will also be added. The entire script must be located between the *<backup>* and *<backup/>* tags.

```
<? xml version="1.0" encoding="utf-8" ?>

<backup>

<source letter ="c" />

<source letter ="f" />

<target file="e:\mybackup2.tib" />

<options compression="high" incremental="true"
description="this is my backup" split="650 Mb" password="" />
```

```
</backup>
```

The script for backing up to tape (tapeN specifies the tapes numbers):

```
<? xml version="1.0" encoding="utf-8" ?>

<backup>

<source letter ="c" />

<source letter ="f" />

<target cdrw="\taperecorder\\\.\tape0|||" />

<target cdrw="\taperecorder\\\.\tape1|||" />

<options compression="high" incremental="true"
description="this is my backup" />

</backup>
```