



User's Guide

Acronis® True Image Echo *Workstation*

Copyright © Acronis, Inc., 2000-2009. All rights reserved.

"Acronis" and "Acronis Secure Zone" are registered trademarks of Acronis, Inc.

"Acronis Compute with Confidence", "Acronis Startup Recovery Manager", "Acronis Active Restore" and the Acronis logo are trademarks of Acronis, Inc.

Linux is a registered trademark of Linus Torvalds.

Windows and MS-DOS are registered trademarks of Microsoft Corporation.

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

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

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

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

Table of Contents

Chapter 1. Introduction	7
1.1 Acronis® True Image Echo Workstation – a complete solution for corporate users	7
1.2 Acronis True Image Echo Workstation components	8
1.3 New in Acronis True Image Echo Workstation	9
1.4 Supported file systems and storage media	11
1.4.1 <i>Supported file systems</i>	11
1.4.2 <i>Supported storage media</i>	11
1.5 License policy	11
1.6 Technical support	12
Chapter 2. Acronis True Image Echo Workstation installation and startup	13
2.1 System requirements	13
2.1.1 <i>Minimum hardware requirements</i>	13
2.1.2 <i>Supported operating systems</i>	13
2.2 Security parameters	14
2.2.1 <i>Credentials</i>	14
2.2.2 <i>Firewall setup</i>	14
2.2.3 <i>Encrypted communication</i>	14
2.2.4 <i>Security parameters in Acronis Administrative Template</i>	15
2.3 Installing Acronis True Image Echo Workstation components	16
2.3.1 <i>Installation of Acronis True Image Echo Workstation local version and Acronis True Image Agent for Windows</i>	17
2.3.2 <i>Installation of Acronis Group Server</i>	18
2.3.3 <i>Acronis Backup Server installation and setup</i>	18
2.3.4 <i>Acronis Universal Restore installation</i>	22
2.4 Extracting Acronis True Image Echo Workstation components	22
2.5 Running Acronis True Image Echo Workstation components	22
2.5.1 <i>Running Acronis True Image Echo Workstation (local version)</i>	22
2.5.2 <i>Running Acronis True Image Management Console</i>	23
2.5.3 <i>Running other Acronis components</i>	23
2.6 Removing Acronis True Image Echo Workstation components	23
Chapter 3. General information and proprietary Acronis technologies	24
3.1 The difference between file archives and disk/partition images	24
3.2 Full, incremental and differential backups	24
3.3 Acronis Secure Zone®	25
3.4 Acronis Startup Recovery Manager	26
3.4.1 <i>How it works</i>	26
3.4.2 <i>How to use</i>	26
3.5 Acronis Backup Server	27
3.5.1 <i>Backup locations</i>	27
3.5.2 <i>Quotas and time limits for computers and users</i>	28
3.5.3 <i>Administrators and Users</i>	28
3.5.4 <i>Operations with archives</i>	29
3.6 Acronis Active Restore	29
3.6.1 <i>Limitations in using Acronis Active Restore</i>	29
3.6.2 <i>How it works</i>	29
3.6.3 <i>How to use</i>	30
3.7 Acronis Universal Restore	30
3.7.1 <i>Acronis Universal Restore purpose</i>	30
3.7.2 <i>Acronis Universal Restore general principles</i>	31
3.7.3 <i>Acronis Universal Restore and Microsoft Sysprep</i>	31

3.7.4	<i>Limitations in using Acronis Universal Restore</i>	32
3.7.5	<i>Getting Acronis Universal Restore</i>	32
3.8	Backing up to tape libraries and tape drives	32
3.8.1	<i>Backing up to a locally attached tape device</i>	33
3.8.2	<i>Understanding backup to tape devices attached to the Backup Server</i>	34
3.8.3	<i>Backing up to a tape device through Acronis Backup Server</i>	36
3.8.4	<i>Restoring data from archives located on tape devices</i>	36
3.9	Viewing disk and partition information	37
Chapter 4. Using Acronis True Image Management Console.....		38
4.1	General information	38
4.2	Installing/updating Acronis components on remote machines	38
4.3	Managing a single remote computer.....	40
4.3.1	<i>Connecting to a remote computer</i>	40
4.3.2	<i>Backup and recovery tasks</i>	42
4.4	Managing groups of computers.....	44
4.4.1	<i>Group status display</i>	44
4.4.2	<i>Creating new group tasks</i>	46
4.4.3	<i>Group tasks management</i>	48
4.4.4	<i>Acronis Group Server options</i>	49
4.5	Managing backup server	49
4.5.1	<i>Default settings</i>	50
4.5.2	<i>Set up Administrator profiles</i>	52
4.5.3	<i>Adding Users and Administrators to the Acronis Backup Server database</i>	53
4.5.4	<i>Changing User profiles</i>	55
4.5.5	<i>Configuring Backup Locations</i>	55
4.5.6	<i>Managing Archives</i>	56
4.5.7	<i>Limiting access to Acronis Backup Server</i>	57
Chapter 5. Using Acronis True Image Echo Workstation (local version).....		59
5.1	Main program window	59
5.2	Managing a local computer.....	61
Chapter 6. Creating backup archives		64
6.1	Backing up files and folders (file backup)	64
6.2	Backing up disks and partitions (image backup)	68
6.3	Setting backup options.....	70
6.3.1	<i>Archive protection</i>	71
6.3.2	<i>Source files exclusion</i>	71
6.3.3	<i>Pre/post commands</i>	72
6.3.4	<i>Database support</i>	72
6.3.5	<i>Compression level</i>	73
6.3.6	<i>Backup performance</i>	73
6.3.7	<i>Fast incremental/differential backup</i>	74
6.3.8	<i>Archive splitting</i>	74
6.3.9	<i>File-level security settings</i>	75
6.3.10	<i>Media components</i>	75
6.3.11	<i>Error handling</i>	76
6.3.12	<i>Dual destination backup</i>	77
6.3.13	<i>Wake On LAN</i>	77
6.3.14	<i>Additional settings</i>	78
Chapter 7. Restoring the backup data		80
7.1	Considerations before recovery.....	80
7.1.1	<i>Restore under Windows or boot from CD?</i>	80
7.1.2	<i>Network settings in rescue mode</i>	80
7.1.3	<i>Recovering dynamic volumes</i>	81
7.2	Restoring files and folders from file archives	81

7.3 Restoring disks/partitions or files from images	84
7.3.1 <i>Starting the Restore Data Wizard</i>	85
7.3.2 <i>Archive selection</i>	85
7.3.3 <i>Restoration type selection</i>	86
7.3.4 <i>Selecting a disk/partition to restore</i>	87
7.3.5 <i>Selecting a target disk/partition</i>	87
7.3.6 <i>Changing the restored partition type</i>	88
7.3.7 <i>Changing the restored partition file system</i>	89
7.3.8 <i>Changing the restored partition size and location</i>	89
7.3.9 <i>Assigning a letter to the restored partition</i>	90
7.3.10 <i>Restoring several disks or partitions at once</i>	90
7.3.11 <i>Using Acronis Universal Restore</i>	90
7.3.12 <i>Setting restore options</i>	91
7.3.13 <i>Restoration summary and executing restoration</i>	91
7.4 Setting restore options.....	91
7.4.1 <i>Files to exclude from restoration</i>	92
7.4.2 <i>Files overwriting mode</i>	92
7.4.3 <i>Pre/post commands</i>	92
7.4.4 <i>Restoration priority</i>	93
7.4.5 <i>File-level security settings</i>	93
7.4.6 <i>Specifying mass storage drivers</i>	93
7.4.7 <i>Additional settings</i>	94
7.4.8 <i>Error handling</i>	94
7.5 Creating dynamic disks and volumes	95
7.5.1 <i>Creating dynamic volumes</i>	95
Chapter 8. Scheduling tasks.....	98
8.1 Creating scheduled tasks.....	98
8.1.1 <i>Setting up daily execution</i>	100
8.1.2 <i>Setting up weekly execution</i>	101
8.1.3 <i>Setting up monthly execution</i>	102
8.1.4 <i>Setting up one-time execution</i>	102
8.1.5 <i>Setting up event-driven execution</i>	103
8.2 Managing scheduled tasks.....	103
Chapter 9. Managing the Acronis Secure Zone	105
9.1 Creating Acronis Secure Zone	105
9.2 Resizing the Acronis Secure Zone.....	107
9.3 Changing the password for Acronis Secure Zone	108
9.4 Deleting Acronis Secure Zone	108
Chapter 10. Creating bootable media	109
10.1 Creating Acronis rescue media	109
10.2 Creating a Win PE ISO with Acronis True Image Echo Workstation.....	111
Chapter 11. Operations with archives.....	112
11.1 Validating backup archives	112
11.2 Exploring archives and mounting images	112
11.2.1 <i>Exploring an archive</i>	113
11.2.2 <i>Mounting an image</i>	114
11.2.3 <i>Unmounting an image</i>	116
11.3 Consolidating backups.....	116
Chapter 12. Notifications and event tracing	120
12.1 Email notification	120
12.2 WinPopup notification	120
12.3 Viewing logs.....	121
12.4 Event tracing.....	122

12.4.1	Windows event log	122
12.4.2	SNMP notifications.....	123
12.5	Managing System Restore	123
Chapter 13. Working with a virtual environment		125
13.1	Backing up data on virtual machines	125
13.2	Recovering data on virtual machines	125
13.3	Using the disk conversion feature.....	126
13.3.1	Recover data on the VM.....	126
13.3.2	Recover both data and the VM	126
13.3.3	Physical to virtual migration	126
13.3.4	Converting workloads	127
13.4	Converting disk images to virtual disks	127
Chapter 14. Transferring the system to a new disk.....		129
14.1	General information	129
14.2	Security	130
14.3	Executing transfers	130
14.3.1	Selecting Clone mode	130
14.3.2	Selecting source disk	130
14.3.3	Selecting destination disk	131
14.3.4	Partitioned destination disk	132
14.3.5	Old and new disk partition layout.....	132
14.3.6	Old disk data	132
14.3.7	Destroying the old disk data	133
14.3.8	Selecting partition transfer method	134
14.3.9	Partitioning the old disk	135
14.3.10	Old and new disk partition layouts	135
14.3.11	Cloning summary.....	136
14.4	Cloning with manual partitioning	136
14.4.1	Old and new disk partition layouts	136
Chapter 15. Adding a new hard disk		138
15.1	Selecting a hard disk.....	138
15.2	Creating new partitions	138
15.3	Disk add summary	139
Chapter 16. Command-line mode and scripting		140
16.1	Working in the command-line mode	140
16.1.1	TrueImageCmd supported commands.....	140
16.1.2	Common options (options common for most trueimagecmd commands)	143
16.1.3	Specific options (options specific for individual trueimagecmd commands).....	145
16.1.4	Trueimagecmd.exe usage examples.....	150
16.1.5	ICompGS.exe tool: adding machines to the group server out of a *.txt file.....	154
16.1.6	Ebasrvdb.exe tool: generate an XML file with the backup mapping details.....	154
16.1.7	Command-line mode usage under DOS	155
16.2	Scripting	155
16.2.1	Script execution parameters	155
16.2.2	Script structure	155
16.2.3	Script usage examples	156

Chapter 1. Introduction

1.1 Acronis® True Image Echo Workstation – a complete solution for corporate users

Acronis True Image Echo Workstation is a comprehensive backup and recovery solution for heterogeneous computer infrastructure that may include any combination of physical and virtual, networked and standalone Windows-based computers.

Acronis True Image Echo Workstation creates a transportable image, independent of the hardware platform that can be restored directly to and from any virtual or physical environment.

Minimizes downtime

Acronis True Image Echo Workstation 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. It is not necessary to reinstall software or reconfigure your system or network settings. The complete system restoration can be performed to an existing system, to a new system with different hardware, or to virtual machines. With the Acronis Active Restore feature, users can access the system and begin working during the restore process, further decreasing downtime. File-level 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 the domain or 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 Echo Workstation, you simply create backup tasks, tailored by group, or certain times or events.

To ensure that backups have occurred, or if user intervention is required, you can request notifications via email or Windows Pop-up. You can view Acronis events in the Windows Application Events Log or Acronis own log files. 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 the image has been created. And because these tasks can be scheduled, you need not recreate the script to run the pre- and post-event tasks each time; you can set the scheduled events once and they will run each time automatically.

Ensures 24 X 7 Uptime

With Acronis' patented drive snapshot technology, systems can be imaged while they are in use, ensuring 24-by-7 system 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 CPU's

availability for mission critical applications. Additionally, users can control hard disk drive writing speeds and control network bandwidth used during backups, allowing minimal disruption of business operations.

Supports Leading Edge Technology

Businesses today are moving to leverage the latest technologies, including dual-core, 64-bit processors and 64-bit operating systems. With Acronis True Image Echo Workstation, you can protect these new machines, as well as legacy computers, running a single application with a common interface.

Leverages Existing Technology Investments

The product can leverage your current storage infrastructure by supporting a 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), 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 Echo Workstation can be used to clone an image onto multiple machines. For example, let's say a company purchased several computers and needs similar environments on each of them. Traditionally, the IT manager would install the operating system and programs on every computer. With Acronis True Image Echo Workstation, the IT manager would configure a single computer, then create a disk image of the system. That image can then be duplicated onto multiple computers.

If you need to upgrade the hard disk drive, Acronis True Image Echo Workstation 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.

Volumes conversion

Acronis True Image Echo Workstation can back up and recover dynamic volumes.

Dynamic volume as is can be recovered over the same volume or unallocated space of a dynamic group. Acronis True Image Echo Workstation has necessary tools for any-to-any disks conversion in terms of basic disks and dynamic volumes of any type (simple, spanned, striped, mirrored or RAID 5). The tools are available in bootable program version as well. Having booted the Acronis environment, you can easily prepare the desired dynamic group on bare metal or a computer with non-Windows operating system.

1.2 Acronis True Image Echo Workstation components

Acronis True Image Echo Workstation includes the following components.

1. **Acronis True Image Management Console** is a tool for remote access to Acronis components. Administrator uses the console to install, configure and control the components from remote.
2. **Acronis True Image Agent** is an application that resides on client computers and performs Acronis operations such as data backup or restore.
3. **Acronis Group Server** is a management tool that provides ability to schedule, monitor and manage group backup tasks. It deploys group tasks to the agents, polls the

agents for the status of running tasks and provides the administrator with the summary tasks state display over the network.

4. **Acronis Backup Server** is an application for centralized storage and management of enterprise backup archives.

The administrator can set space quotas and backup schemes, schedule check tasks that consolidate backups in case of quota violation, perform one-time backups consolidation. This ensures optimal usage of the storage capacity. Acronis Backup Server also enables users to access a tape library, connected to the server.

5. **Acronis True Image Echo Workstation** (local version) is a locally controlled computer management tool with additional functionality as compared to Acronis True Image Agent. The local version supports, besides backup and recovery operations, exploring archives, mounting images as virtual drives, cloning hard disks data and formatting partitions on new hard disks, creating dynamic volumes, command-line mode and scripts execution.

6. **Acronis Universal Restore** is a separately sold add-on to Acronis True Image Echo Workstation that automatically configures Windows drivers in a system, recovered on dissimilar hardware. This enables the seamless system start and operation.

7. **Acronis Bootable Rescue Media Builder** - creates bootable media, its ISO image or the RIS package thus enabling data recovery over bare metal, non-Windows or corrupted operating systems.

1.3 New in Acronis True Image Echo Workstation

Management console

Reconnect (last connect) option

Centralized installation and update of Acronis components on multiple computers

Group server

Import and export computers through txt/csv files (in the command-line mode - txt files)

Run, stop, restart, edit, check group tasks

Group validation tasks

Set how often to check the computers state (status refresh rate)

Wake on LAN for backup

Backup server

Import/export archives from external locations

Limit number of connections

Limit bandwidth used per connection

Access to tape library for every user

Backup

Backup of dynamic volumes

Backup and restore of 2+TB volumes

Encrypting backups with industry-standard AES cryptographic algorithm (key size 128, 192, 256 bit)

Multi-volume snapshot for databases spread on several disks

Control network bandwidth usage when backing up to FTP

Error handling: ignore bad sectors, silent mode (no pop-ups, continue on all errors)

Dual destination backup: local + network share

Archive bit reset (file-level backup only)

Generating time-based names for backup files

Recovery

Recovery of dynamic volumes

Recovery of system dynamic volumes on dissimilar hardware using Acronis Universal Restore or Acronis Active Restore

Scheduling

Schedule archive validation

Start every N hours within daily schedule

Start on free disk space change by the specified amount

Cloning a task

Notification via e-mail

Multiple e-mail addresses

From and Subject fields

Logon to incoming mail server

Operations with archives

Convert disk images to virtual disks for VMware, Microsoft, XenServer and Parallels virtual machines

Consolidate backup files (create a consistent copy of archive while deleting selected backups)

Explore archives (open in read-only mode any image or file-level backup)

Operations with hard disks

Convert basic disk to dynamic

Create dynamic volumes

CLI features

MBR restore

Backup to FTP server

Allow logs on net share

Merge unallocated space by moving partitions and create Acronis Secure Zone on the space

Security

Encrypted (SSL) communication between Acronis True Image Echo Workstation components

1.4 Supported file systems and storage media

1.4.1 Supported file systems

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

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

1.4.2 Supported storage media

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

* - Data recovery directly from an FTP server will require the archive to consist of files no more than 2GB in size, so please note this during the backup image creation. It is recommended that you change the source computer firewall settings to disable the **Routing and Remote Access** Windows service. The previous versions of the software recommended for the target FTP server the usage of passive mode for file transfers and usage of ports 20 and 21 at the source computer for both TCP and UDP protocols. The current version has no such limitations: you can use active or passive mode and any port, changing the default settings at **Options->Backup Options->Advanced settings**.

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

1.5 License policy

Acronis True Image Echo Workstation licensing is based on number of computers on which Acronis True Image Agent and/or Acronis True Image Echo Workstation local version are to be installed. This means you need one license for each computer you are going to backup, whether you will control it on-site (with the local program version) or remotely (using Acronis True Image Agent), or use both ways of control. The number of Acronis True Image Management Console, Acronis Group Server and Acronis Backup Server installations is not counted.

Acronis Universal Restore is an option to Acronis True Image Echo Workstation and has its own serial number.

1.6 Technical support

As part of a purchased annual Support charge you are entitled to Technical Support as follows: to the extent that electronic services are available, you may electronically access at no additional charge, Support services for the Software, which Acronis shall endeavor to make available twenty four (24) hours a day, seven (7) days per week. Such electronic services may include, but are not limited to: user forums; software-specific information; hints and tips; bug fix retrieval via the internet; software maintenance and demonstration code retrieval via a WAN-accessible FTP server; and access to a problem resolution database via Acronis customer support system.

Support shall consist of supplying telephone or other electronic support to you in order to help you locate and, on its own, correct problems with the Software and supplying patches, updates and other changes that Acronis, at its sole discretion, makes or adds to the Software and which Acronis makes generally available, without additional charge, to other licensees of the Software that are enrolled in Support.

Upon mutual agreement by both parties, Acronis shall:

(i) supply code corrections to you to correct Software malfunctions in order to bring such Software into substantial conformity with the published operating specifications for the most current version of the Software unless your unauthorized modifications prohibit or hamper such corrections or cause the malfunction;

or (ii) supply code corrections to correct insubstantial problems at the next general release of the Software.

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

Chapter 2. Acronis True Image Echo Workstation installation and startup

2.1 System requirements

2.1.1 Minimum hardware requirements

Acronis True Image Echo Workstation requires the following hardware:

- Pentium processor or higher
- 512MB RAM
- FDD or CD-RW drive for bootable media creation
- Mouse (recommended).

2.1.2 Supported operating systems

Acronis True Image Management Console

- Windows Professional 2000 SP4/XP Professional SP3
- Windows XP Professional x64 Edition
- Windows Vista all Editions (except for installation of Acronis components on remote machines running Vista)

Acronis True Image Agent

Acronis True Image Echo Workstation

- Windows Professional 2000 SP4/ Professional XP SP3
- Windows XP Professional x64 Edition
- Windows Vista all Editions (except for the Acronis Active Restore feature)

Acronis Backup Server

Acronis Group Server

- Windows Professional 2000 SP4/ Professional XP SP3
- Windows XP Professional x64 Edition
- Windows Vista all Editions

Acronis Universal Restore (optional)

- Windows 2000 Professional SP4/XP Professional SP3
- Windows XP Professional x64 Edition
- Windows Vista all Editions

Acronis True Image Echo Workstation bootable version enables disk-level backup and recovery on a computer running any PC-based operating system.

2.2 Security parameters

2.2.1 Credentials

Acronis True Image Echo Workstation fully supports all security standards used in Windows.

To install Acronis components on a computer, the user must be a member of the Administrators group on the computer.

To get access to Acronis True Image Agent, installed on a computer, the user must be a member of the Administrators or Backup operators group on the computer.

The Acronis Group Server uses administrator's credentials to perform data backup tasks on the computers. You will be asked for the credentials during the Acronis Group Server installation. The credentials you provide will be used for running the Acronis Group Server service and also applied to all networked computers.

Therefore, it is recommended that you have a uniform account for all computers where the Acronis True Image Agent is installed. Domain administrators can use the domain administrator account. In a workgroup, it would make sense to create identical accounts in the Administrators group on each computer with Acronis True Image Agent.

If you do not wish to create a uniform account, provide credentials for each computer after Acronis Group Server installation as described in point 4 of *4.4.1 Group status display*.

You can combine both methods, for example, to set up a uniform account for domain members and set individual accounts for members of a workgroup.

2.2.2 Firewall setup

Acronis True Image Echo Workstation 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 choose a port at random
- client (Acronis True Image Management Console) UDP port: 9877, if busy choose a 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, are set automatically during Acronis True Image Echo Workstation 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.

2.2.3 Encrypted communication

Acronis True Image Echo Workstation provides capability to secure all data transferred between Acronis components within local net and through DMZ, including the backup stream.

Encryption starts on the first (earliest) stage of connection attempt, so all data transferred on the next steps (including data required for client authentication) is encrypted.

Once Acronis True Image Echo Workstation components are installed, encrypted communication between the components is enabled automatically.

The earlier versions of Acronis True Image Workstation did not support encrypted communication, therefore connection to such components, if they present on the network, will not be encrypted. You have an option to completely disable non-encrypted communication with some or all Acronis True Image Echo Workstation components. In this case, the components will not be able to communicate with components of earlier versions. For how to disable non-encrypted communication, see the next section.



The earlier versions of Acronis True Image Management Console cannot communicate with Acronis True Image Echo Workstation agents. The console must be upgraded to the Acronis True Image Echo Workstation console.

Encryption is provided with Secure Socket Layer mechanism. There are two stakeholders of the encryption operation:

- **Client application** – the application that tries to establish (initiates) connection. This could be the Acronis True Image Management Console or Acronis Group Server. Acronis True Image Echo Workstation local version can also be a client when it performs backup to Acronis Backup Server.
- **Server application** – the application to which the client tries to connect. This could be Acronis True Image Agent, Acronis Group Server, Acronis Backup Server.

2.2.4 Security parameters in Acronis Administrative Template

As stated above, encryption generally does not require setting up. However, connection to Acronis components of earlier versions will not be encrypted. To completely disable non-encrypted communication with some or all Acronis True Image Echo Workstation components, use the Administrative Template, provided by Acronis.

Through the Microsoft Group Policy mechanism, the template can be applied to a single computer as well as to a domain.

How to apply Acronis Administrative Template

1. Run Windows Group Policy Objects Editor (\WINDOWS\system32\gpedit.msc).
2. Open the Group Policy object you want to edit, and in the console tree right-click Administrative Templates.
3. Click Add/Remove Templates.
4. Click Add.
5. Browse to the Acronis Administrative Template
(\Program files\Common Files\Acronis\Agent \acronis_agent.adm or \Program files\Acronis\TrueImageConsole\acronis_agent.adm), and click Open.
6. Once the template is added, open it and edit the desired settings.



For detailed information about Windows GPO Editor please see:

<http://msdn2.microsoft.com/en-us/library/aa374163.aspx>

For detailed information about Group Policies please see:

<http://msdn2.microsoft.com/en-us/library/aa374177.aspx>

The Acronis Administrative Template contains the following settings.

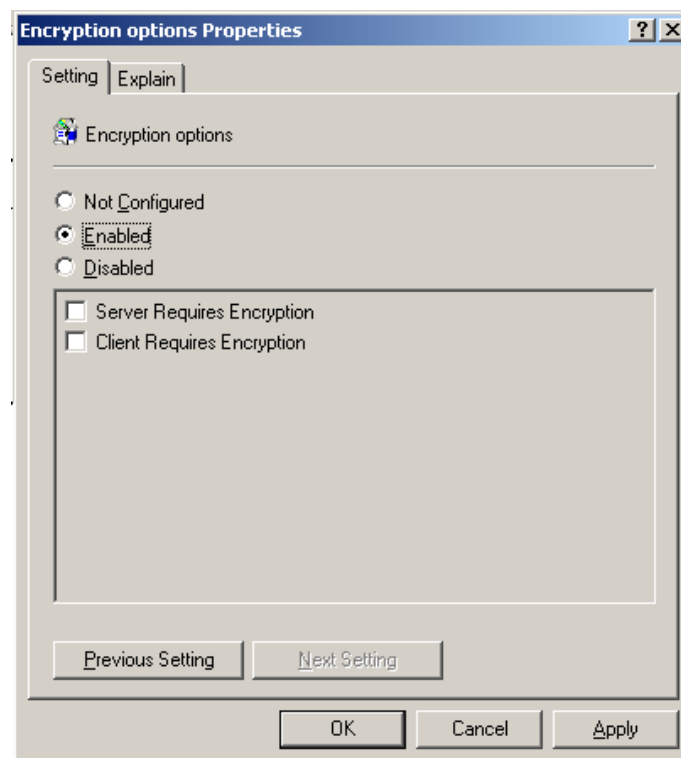
Encryption Options

- **Server Requires Encryption**

This option defines the server behavior in case the client does not support encryption. When enabled, connection to the client will be terminated. When disabled, the client will be allowed to establish non-encrypted connection.

- **Client Requires Encryption**

When connecting to server applications, the Acronis client applications always attempt to establish an encrypted connection. The Client Requires Encryption option defines the client behavior in case the server does not support encryption. When disabled, the non-encrypted connection will be established. When enabled, the connection will be terminated.



After applying the template or editing the encryption options, you should restart the Remote Agent(s).

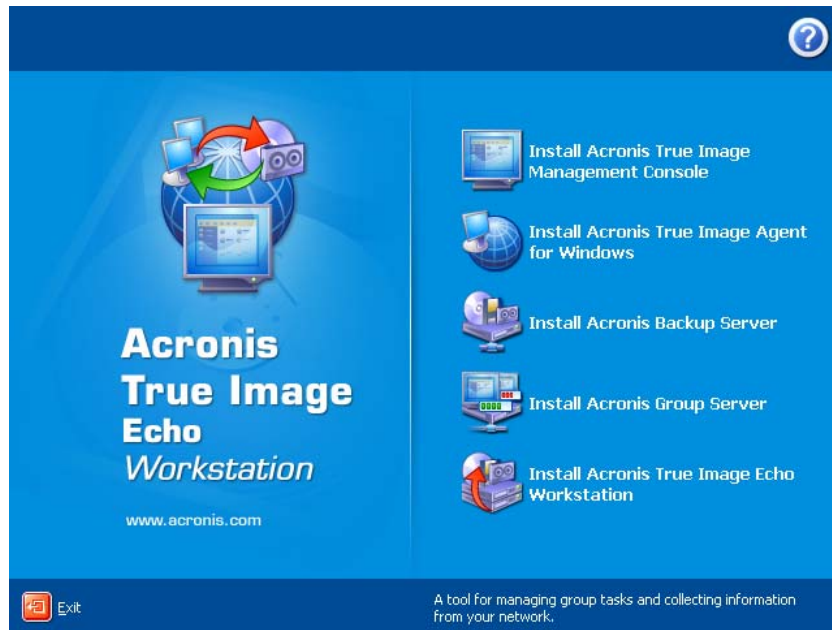
2.3 Installing Acronis True Image Echo Workstation components

To install Acronis True Image Echo Workstation components, run the Acronis True Image Echo Workstation setup file.



If you have the trial version of Acronis True Image Echo Workstation installed on your system, you must uninstall it before installing the commercial version of the product.

Select the program to install and follow instructions on the screen.



Acronis True Image Echo Workstation Install Window

It is recommended that you install Acronis True Image Management Console first. After that you will be able to install Acronis True Image Echo Workstation (local version) and Acronis True Image Agent for Windows remotely to networked computers.

2.3.1 Installation of Acronis True Image Echo Workstation local version and Acronis True Image Agent for Windows

For Acronis True Image Echo Workstation 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 Echo Workstation, 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*). 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.

The widely used **Bart PE** utility provides a Windows-like operating environment invoked via removable bootable media. 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 Echo Workstation into a 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 installed, Acronis True Image Echo Workstation (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 backups as virtual disks (see *11.2.2 Mounting an image*).

2.3.2 Installation of Acronis Group Server

The Acronis Group Server only can be installed locally on a computer by running the setup program.

When installing Acronis Group Server, you will be asked for credentials. The credentials you provide are used for running the Acronis Group Server service and also applied to all networked computers.

Enter the uniform account information discussed in *2.2.1 Credentials*. If you do not use a uniform account, provide credentials for each computer after the Acronis Group Server installation as described in point 4 of *4.4.1 Group status display*.

2.3.3 Acronis Backup Server installation and setup

The Acronis Backup Server only can be installed locally on a computer by running the setup program.

Before starting installation of this component, please read section *3.5 Acronis Backup Server* to get understanding of this component functionality and define the storage policy advantageous to your network.

We suggest that you start using Acronis Backup Server as follows:

1. Set up a machine with a system drive and a high capacity storage drive.
2. Install Acronis Backup Server on the system drive. Reboot on prompt.

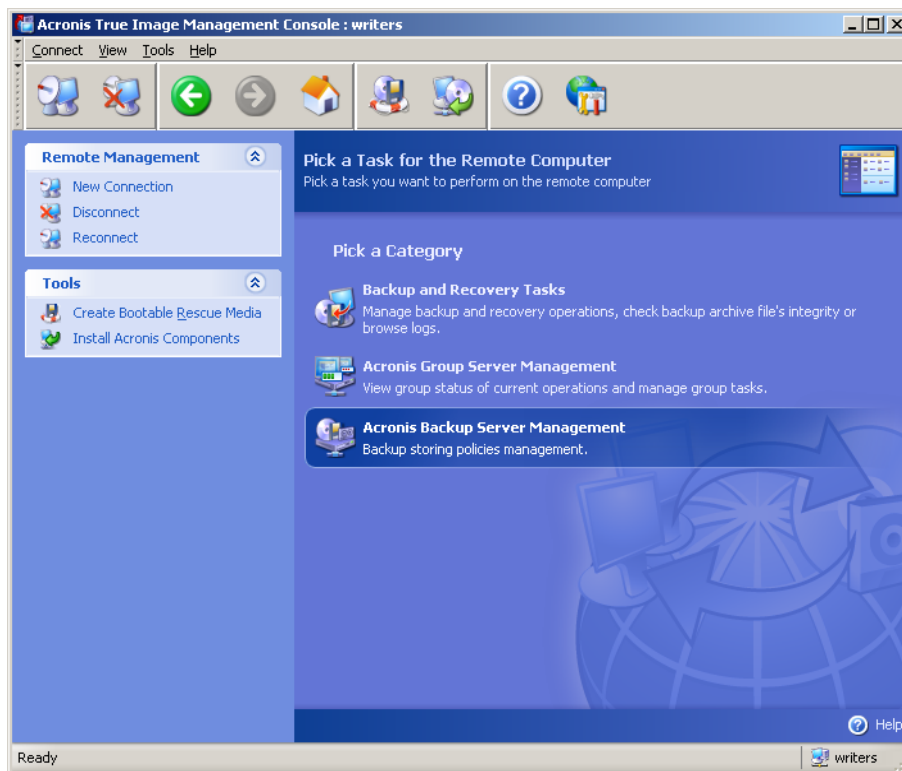


In Windows XP SP2 or Windows 2003 Server, the option **Control panel -> Windows Firewall -> Exceptions -> File and Printer Sharing** must be enabled. Otherwise remote users will not be able to back up on the backup server.

3. Connect the console to Acronis Backup Server.



When connecting to a **backup server inside a domain**, mind whether your domain or local account is saved on the backup server. If you used your local account to install the backup server, and then logged in Windows on the console computer using your domain account, enter the local user name along with the backup server name (for example, Server1\username). Otherwise the name will be identified as a domain one.



4. **Acronis Backup Server Management -> Specify Default Settings -> Set Backup Location ->** specify path to the storage drive. You can create a folder for the backup location on the storage drive. To see the folder in the tree and add it to the path, collapse and expand the drive.

5. Click Back -> **Configure Backup Locations** -> make sure that the new default location is created and delete the location in \Documents and Settings.

6. Set limitations to disk space and storage period for the location, if needed, according to the selected policy.

To do so, select **Configure Backup Locations -> select location -> Quotas and time limits**. The maximum backup location size can be set to the storage drive capacity minus the estimated size of the largest backup (some space must be reserved for the temporary file created at consolidation).

7. Set the default limitations for users/computers, if needed, according to the selected policy.

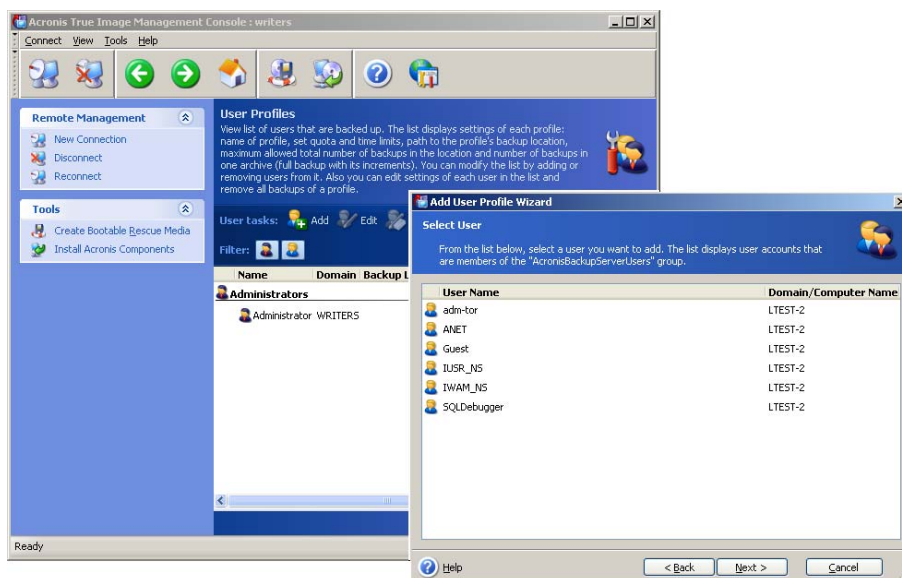
To do so, select **Acronis Backup Server Management -> Specify Default Settings -> Set Quotas and time limits**. The maximum disk space allowed for a user/computer can be set as the max location size divided by total number of users and computers. Generally, value of this setting can reach the maximum location size.

8. Read about administrators and users profiles in *3.5.3 Administrators and Users*. Define if you need more than one administrator on the backup server. If yes, add administrators as follows:

Add the person's local or domain account to the AcronisBackupServerUsers group on the backup server.

Click **Set up User profiles -> Add**.

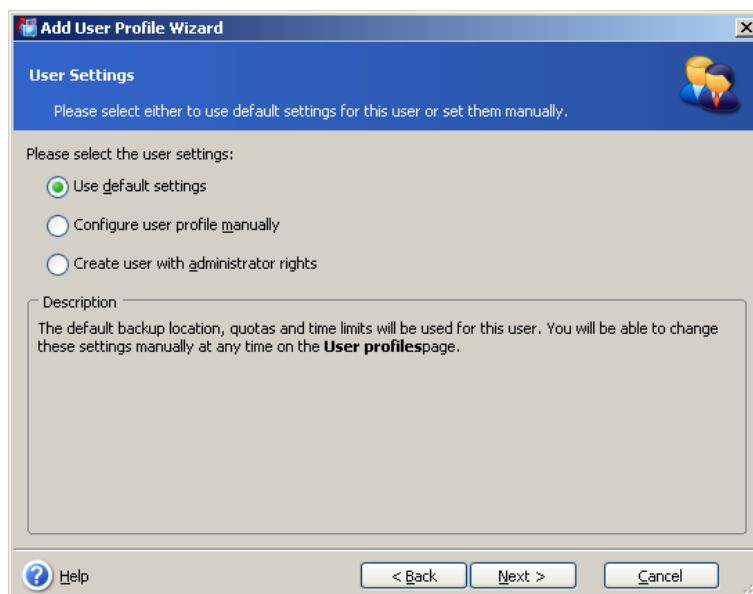
Choose the user name.



Select from the local backup server users or the domain users

Choose **Create user with administrator's rights**.

Click **Proceed**.



User or administrator?

9. Define which users will be allowed to back up data on the backup server. Add the users as follows:

Add the person's local or domain account to the AcronisBackupServerUsers group on the backup server.

Click **Set up User profiles -> Add**.

Choose the user name.

Choose **Use default settings**.

Click **Proceed**.

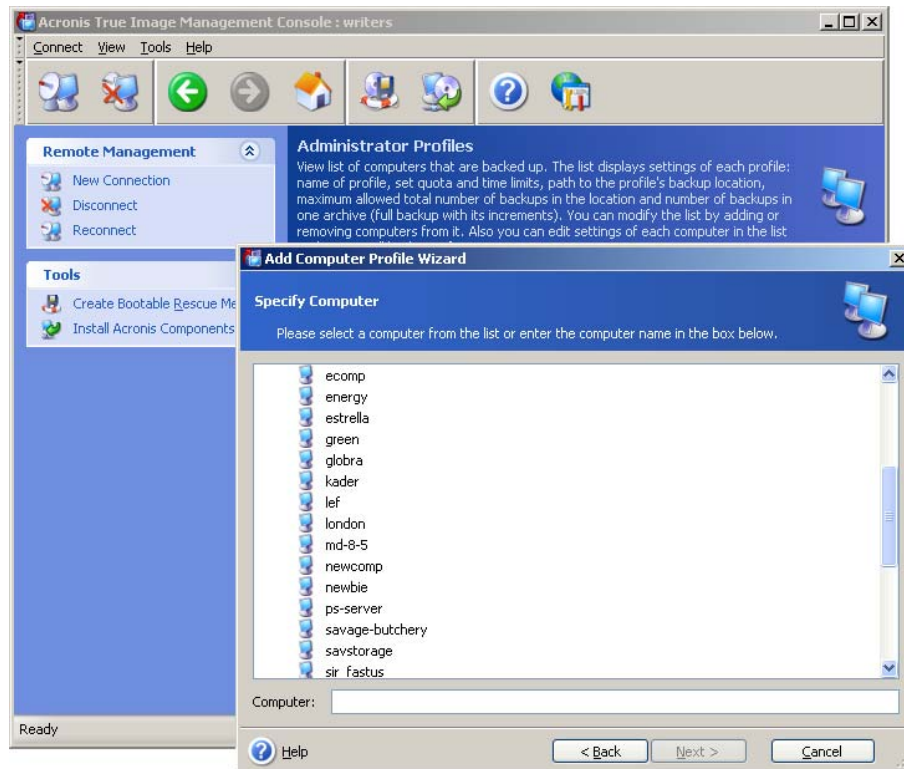
10. Define the computers which administrators will back up using Acronis True Image Agents. Add the computers as follows.

Click **Set up Administrator profiles -> Add**.

Choose the computer or enter its name.

Choose **Use default settings**.

Click **Proceed**.



Adding a computer to the administrator profile

11. Schedule a check for exceeding the quotas and time limits, if needed according to the selected policy.

To do so, select **Acronis Backup Server Management -> Specify Default Settings -> Schedule automatic consolidation and backup management**.

Choose **Periodically**.

Choose **Weekly**.

Schedule check to be performed once a week during off-peak time.

Click **Proceed**.

The backup server is ready to work. To perform backup using the Administrator profile, connect the console to the agent on a remote computer and create a standard backup task while selecting **Acronis Backup Servers -> backup server name -> Personal Backup Location** as backup destination. Or create a group task for several computers with the same destination.

Users can back up their data with local program versions while selecting the same destination.

2.3.4 Acronis Universal Restore installation

Acronis Universal Restore is an option for Acronis True Image Echo Workstation. It is purchased separately and installed from a separate setup file. Acronis Universal Restore has its own serial number that is required at installation.

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 Echo Workstation (local version)

Bootable Media Builder.

Acronis Universal Restore can be installed on a networked computer either locally, by running the setup program, or remotely, using one of remote installation services such as Systems Management Server (a component of Microsoft Windows NT BackOffice program package). Remote installation of Acronis Universal Restore with Acronis True Image Management Console is not supported.

After installation, Acronis Universal Restore automatically plugs in one or more of above program components. Acronis True Image Echo Workstation (local version) name, displayed in its main window, changes to **Acronis True Image Echo Workstation with Universal Restore**.

2.4 Extracting Acronis True Image Echo Workstation components

During Acronis True Image Management Console installation, all Acronis True Image Echo Workstation 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 Echo Workstation components on a local computer, you can save setup files for each Acronis True Image Echo Workstation component separately on a local or network drive. This will help when modifying or recovering the existing component installation on a local computer.

To save a component's setup file:

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

2.5 Running Acronis True Image Echo Workstation components

2.5.1 Running Acronis True Image Echo Workstation (local version)

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

If your operating system fails to load, 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 the computer bootup when you see a corresponding message that tells you to press that key. Acronis

True Image Echo Workstation 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 Echo Workstation version from the bootable media (created by you using Rescue Media Builder) or RIS-server. Then you will be able to restore the disk from a previously created image.

2.5.2 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**.

2.5.3 Running other Acronis components

Acronis True Image Agents, Acronis Backup Server and Acronis Group Server run as services immediately after installation and the consequent system reboot (if the latter is required). Later on they will automatically launch at every system restart. You can stop and start these programs in the same way as other services.

2.6 Removing Acronis True Image Echo Workstation components

You can remove any Acronis True Image Echo Workstation 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.

In case you remove Acronis True Image Agent or Acronis True Image Echo Workstation local version from the system, there is an option to keep the Acronis Secure Zone along with its contents (which will enable data recovery on booting from bootable media) or remove Acronis Secure Zone.

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, is compressed and stored.

Backing up disks and partitions is performed in a different way: Acronis True Image Echo Workstation saves a sector-based 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 Echo Workstation 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), root and the zero track of the hard disk with master boot record (MBR).



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

All Acronis True Image Echo Workstation archives files have a “.tib” extension by default.

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 *11.2.2 Mounting an image*) or start the image restoration and select **Restore specified files or folders**.

3.2 Full, incremental and differential backups

Acronis True Image Echo Workstation 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** only contains data changed since the last full or incremental backup creation. Therefore, it is smaller and takes less time to create. However, since it does not contain all data needed to restore an image, *all* the previous incremental backups *and* the initial full backup are required for restoration.

A **differential backup** creates an independent file containing all changes since the last full archive. Generally, data from a differential backup will be restored faster than an incremental backup, as it does not have to process through a long chain of previous backups.

A standalone, full backup could be an optimal solution if you often roll back the system to the initial state (for example, systems in a gaming club or Internet café where you need to undo changes made by the guests). In this case, you need not 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 most current 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.

An incremental backup is most useful when you need frequent backups and possibility to roll back to any one of multiple stored states. For example, let's say you create a full backup once a month. 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 just examples for your information. Feel free to make up your own backup policy in accordance with your specific tasks and conditions. Acronis True Image Echo Workstation 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 Echo Workstation 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 Active Restore features (see below). The three features, in combination, instantly make operational a system that fails to boot.

A consistent external copy of archives, saved on Acronis Secure Zone, can be created on a network share using dual destination backup feature. See details in *6.3.12 Dual destination backup*.

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 Echo Workstation uses the following approaches to clear space in the 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.
- If there is only one full backup left, and an incremental or differential backup is in progress, you will get an error message telling you there is a lack of available space. In that case, you will have to either re-create the full backup or increase the size of the Acronis Secure Zone.

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 is a good practice to check the zone free space periodically. To do so, start the **Manage Acronis Secure Zone** wizard and see the zone free space that is displayed on the wizard's second page.

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

In case you remove Acronis True Image Agent or Acronis True Image Echo Workstation local version from the system, there is an option to keep Acronis Secure Zone along with its contents (which will enable data recovery on booting from bootable media) or remove Acronis Secure Zone.



The Acronis Secure Zone should not be the only location where a backup is stored. Should the disk have a physical failure, the Acronis Secure Zone could be lost. The Acronis Secure Zone should only be one part of an overall backup strategy.

3.4 Acronis Startup Recovery Manager

3.4.1 How it works

The Acronis Startup Recovery Manager enables starting Acronis True Image Echo Workstation on a local computer without loading the operating system. If the operating system won't load, you can run Acronis True Image Echo Workstation by itself to restore damaged partitions. Unlike booting from the Acronis removable media or RIS server, you will not need a separate media or network connection to start Acronis True Image Echo Workstation.

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 Echo Workstation local version, or remotely, using Acronis True Image Management Console):

1. Install Acronis True Image Echo Workstation local version or Acronis True Image Agent on a computer.
2. Create Acronis Secure Zone on the computer hard disk (see *Chapter 9. Managing the 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.

Here's an example of how you would use this feature. If failure occurs on a 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 Echo Workstation 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 Echo Workstation 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

Acronis Backup Server is an application for centralized storage and management of enterprise backup archives in accordance with the policies, set by an administrator. It ensures optimal usage of storage resources 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.

For information on how to install and set up Acronis Backup Server, see *2.3.3 Acronis Backup Server installation and setup*. For information on how to manage Acronis Backup Server, see *4.5 Managing backup server*.

3.5.1 Backup locations

Backup server is a networked computer where Acronis Backup Server is installed. A backup location is a storage area for backups on a local backup server hard drive.

At installation, Acronis Backup Server creates one (default) backup location. The location has the following properties:

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

Maximum backup location size: Unlimited

Maximum storage period (days): Unlimited

All backup data destined to the backup server will be saved in the default backup location.

Because it may not be practical or efficient for you to store all backup data in one location, the backup server allows you to create as many locations as you need, each with its own properties. The three basic rules are:

- any location, except for the default one, must be assigned to at least one user or computer
- only one location can be assigned to a user or computer
- the default location may not be assigned to a user or computer. There must be a default backup location on a backup server though.

You can create a separate location for each user or computer while adding them to the backup server, distribute the users/computers between several locations, or assign the same location to all users/computers.

Maintaining multiple small backup locations on a single disk does not allow for tracking changes in total disk space usage. At the same time, manual management of thousands of archives in a location may be a serious problem. Practice is the best criterion for your choice.

You can move, clear or delete existing backup locations or edit their size limitations and storage period.

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, GB or TB
- 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 backups.



A storage period is the amount of time that is allotted for a user or the backup location to maintain a file.

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. After that a full backup and a set of subsequent incremental backups is created, then again a full backup and so on.



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.

An attempt to direct user/computer backup data to the backup server while space or number quota is exceeded will not succeed. Backup to the full location will also be prohibited.

An administrator can schedule a check of meeting the limitations. All archives on the backup server will be checked and, if the space quota is violated or the maximum number of backups is exceeded, the backups will be processed as follows:

- Acronis Backup Server will combine the first full backup with the next incremental one into one full backup which will be dated the later backup date. Then, if necessary, this backup will be combined with the next, until the occupied storage space (or number of backups) decreases to the preset limit. Thus, the archive integrity will not be affected, in spite of the fact that the oldest backups will be deleted. This procedure is called **automatic consolidation**.



The actual number of backups can exceed the **Maximum number of backups** by one. This enables the program to detect the fact of quota violation and start consolidation.

3.5.3 Administrators and Users

At installation, Acronis Backup Server creates the user group called AcronisBackupServerUsers:

Control Panel -> Administrative Tools -> Computer Management -> Local Users and Groups -> AcronisBackupServerUsers.

The person who installed the program becomes the administrator in this group. The administrator is automatically registered on the backup server.

Generally, there are two types of profiles on the backup server: Administrators and Users.

The **Administrators** profiles are designed to perform backups on remote computers with Acronis True Image Agents. Whatever computer the administrator backs up, backup data will be sent to the same location, assigned to the computer. Administrators can also manage archives on the backup server, including archives created via Users' profiles.

The **Users** profiles are designed to back up data from computers with Acronis True Image Echo Workstation local version. Whatever computer the user operates on, backup data will be sent to the same location assigned to that user.

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 consolidate any backup (except for the oldest one in the archive) manually with the preceding backup file. This operation deletes the preceding backup and sets concatenation between the backup being consolidated and the backup before the deleted one. Thus, the archive integrity will not be affected, in spite of the fact that one backup will be deleted. Data recovery from any of the remaining backups will be possible.

An archive can be exported from Acronis Backup Server to a local hard drive or network share or imported from external location to a computer's or user's backup location on the backup server.

3.6 Acronis Active Restore

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

3.6.1 Limitations in using Acronis Active Restore

1. Acronis Active Restore is currently available for images located in the Acronis Secure Zone only.
2. Acronis Active Restore does not support images of Windows Vista. If any Vista edition is detected in an image, the Active Restore option will not appear.
3. Acronis Active Restore does not work if the image contains dynamic disks and volumes.
4. Acronis Active Restore cannot be used if the image contains no operating system (a logical partition or disk image) or when restoring file archives.

3.6.2 How it works

When the restoration procedure is started, Acronis True Image Echo Workstation:

1. Finds the sectors in the image which contain system files, and restores these sectors first. First the OS is restored and can be started very quickly. 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. Next, the application writes on the hard disk its own drivers, which intercept system queries to the files. When the user attempts to open files or launch applications, the drivers receive the system queries and restore the sectors that are necessary for the requested operation.

3. At the same time, Acronis True Image Echo Workstation proceeds with the complete sector-by-sector image restoration in the background. However, the 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 10-20GB image (most common image size) takes about 10 minutes. The larger the image size, the more time you save.

3.6.3 How to use

To be able to use Acronis Active Restore, prepare your system this way: (you can do it either locally, using Acronis True Image Echo Workstation local version, or remotely using Acronis True Image Management Console):

1. Install Acronis True Image Echo Workstation local version or Acronis True Image Agent on the local computer.
2. Create the Acronis Secure Zone on the local computer hard disk (see *Chapter 9. Managing the 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 Echo Workstation (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 Active Restore, the current Acronis True Image Echo Workstation version always restores the entire system disk. Therefore, if your system disk consists of several partitions, all of them must be included in the image. Any partitions which are missing from 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 Active Restore** and in the next window click **Proceed**. In a few seconds the computer will reboot to the restored system. Log in and start work – no additional reboots or other actions are required.

You can perform Active Restore running Acronis True Image Echo Workstation in Windows operating systems as well. However, it is mandatory to have bootable media in case Windows cannot boot.

3.7 Acronis Universal Restore

3.7.1 Acronis Universal Restore purpose

A system disk image can be deployed easily on the hardware where it was created or to identical hardware. However, if you change a motherboard or use another processor version — a likely possibility in case of hardware failure — the restored system could be unbootable. An attempt to transfer the system to a new, much more powerful computer will usually produce the same unbootable result because the new hardware is incompatible with the most critical drivers included in the image.

Using Microsoft System Preparation Tool (Sysprep) does not solve this problem, because Sysprep permits replacing drivers only for Plug-and-Play devices (sound cards, network adapters, video cards etc.). As for system Hardware Abstraction Layer (HAL) and mass storage device drivers, they must be identical on the source and the 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 Hardware Abstraction Layer (HAL) and mass storage device drivers.

Acronis Universal Restore is applicable for:

1. Instant recovery of a failed system on different hardware
2. Hardware-independent cloning and deployment of operating systems
3. Real-to-virtual and virtual-to-real computer migration for system recovery, test and other purposes.

3.7.2 Acronis Universal Restore general principles

1. Automatic HAL and mass storage drivers selection

Acronis Universal Restore searches the Windows default driver storage folders (in the image being restored) for HAL and mass storage device drivers and installs drivers that better fit the target hardware. You can specify a custom driver repository (a folder or folders on a network drive or CD) which will also be used for drivers search.



The Windows default driver storage folder is determined in the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current version\DevicePath. This storage folder is usually WINDOWS/inf.

2. Manual selection of mass storage device driver

If the target hardware has a specific mass storage controller (such as a SCSI, RAID, or Fibre Channel adapter) for the hard disk, you can install the appropriate driver manually, bypassing the automatic driver search-and-install procedure.

3. Installing drivers for plug and play devices

Acronis Universal Restore relies on built-in plug and play discovery and configuration process to handle hardware differences in devices that are not critical for the system start, such as video, audio and USB. Windows takes control over this process during the logon phase, and if some of the new hardware is not detected, you will have a chance to install drivers for it later manually.

3.7.3 Acronis Universal Restore and Microsoft Sysprep

Acronis Universal Restore is *not* a system preparation tool. You can apply it to any system image created by Acronis products, including images prepared with Microsoft System Preparation Tool (Sysprep). The following is an example of using both tools on the same system.

Acronis Universal Restore does not strip security identifier (SID) and user profile settings in order to run the system immediately after recovery without re-joining the domain or re-mapping network user profiles. If you are going to change the above settings on a recovered system, you can prepare the system with Sysprep, image it and restore, if need be, using Acronis Universal Restore.

3.7.4 Limitations in using Acronis Universal Restore

1. The system recovered by Acronis Universal Restore might 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 only selected partitions but not the entire source disk



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 a partition other than the first, this can confuse the loader and prevent the restored system from startup.

To avoid the problem, we recommend that you image and restore the entire system disk.

2. The Acronis Universal Restore option does not work if a computer is booted with Acronis Startup Recovery Manager (using F11) or the backup image is located in Acronis Secure Zone. This is because Acronis Startup Recovery Manager and Acronis Secure Zone are primarily meant for instant data recovery on the same computer.

3.7.5 Getting Acronis Universal Restore

Acronis Universal Restore is an add-on to Acronis True Image Echo Workstation. It is purchased separately, has its own license, and is installed from a separate setup file.

Let's assume for a moment that you own Acronis True Image Echo Workstation but have not purchased Acronis Universal Restore. When you create a task for restoring a Windows system disk and select a target disk (either physical or virtual) in the Restore Data Wizard, the program compares crucial for the system start devices found in the image registry and the target computer registry. If the chipset, motherboard or mass storage device are different, and therefore there is a risk that the system cannot boot, you will be prompted whether you want to buy Acronis Universal Restore. To buy the option, follow the link: <http://www.acronis.com/enterprise/products/ATICW/universal-restore.html>

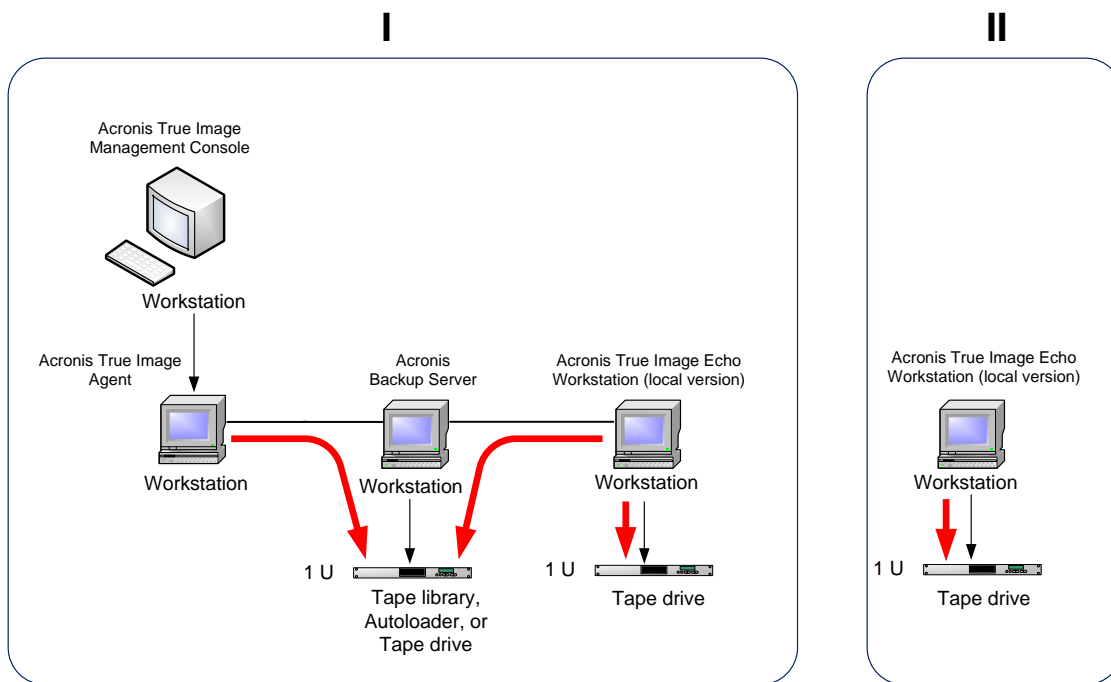
If you already have Acronis Universal Restore, the prompt will not come up and you will have an option to enable Acronis Universal Restore later in the Restore Data Wizard.

3.8 Backing up to tape libraries and tape drives

A tape library is a high-capacity storage device consisting of one or more tape drives and a loader that automatically selects and loads multiple tape cartridges. Tape libraries with only one drive and loader are known as autoloaders.

Acronis True Image Echo Workstation supports tape libraries, autoloaders, and SCSI tape drives as storage devices.

Tape libraries, autoloaders and tape drives are accessible through the Acronis Backup Server. Acronis True Image Echo Workstation local version can access tape drives only. The following diagram illustrates ways of access to tape devices for networks with (I) and without (II) backup server.



The devices must be locally attached to the computers. The devices attached to the Backup Server must work through Windows Removable Storage Management (RSM). Locally attached devices do not require RSM.

The following operations are available for backups stored on tape devices:

- Validation
- data recovery
- converting an image to virtual disk.

Limitations

Devices that use the Network Data Management Protocol (NDMP) are not supported.

Consolidation, mounting or exploring backups stored on tape devices is not supported.

Tapes created by a tape device attached to the Backup Server are not compatible with tapes created by a locally attached tape device

All backups stored on one tape must be of the same backup type - either image backups, or file-level backups, performing an image backup on the tape containing a file-level backup also is not supported.

Acronis True Image Echo Workstation does not support tape devices when working in preinstallation environment such as Win PE or Bart PE.

3.8.1 Backing up to a locally attached tape device

Backup to a locally attached tape device can be performed using either Acronis True Image Echo Workstation local version or bootable media.



Only SCSI tape drives are supported when backing up in this mode. Tape libraries and autoloaders are not supported.

When working with locally attached tape drives, you do not need the RSM service (opposing to the Backup Server, where you do need to use RSM for tape management). Acronis True Image Echo Workstation local version will disable the RSM service on your computer while backing up to a locally attached tape device.

To enable backup to a locally attached tape device with Acronis True Image Echo Workstation local version:

1. Install Acronis True Image Echo Workstation local version.
2. Attach the tape device to the computer.
3. If the tape contains data, its contents will be overwritten on prompt. You have an option to disable prompts, see *6.3.14 Additional settings*.
4. When creating a backup task, you will be able to select the tape device from the list of destination devices. Filenames for backups are not needed when backing up to tape.
5. As soon as the tape is full, a dialog window with a request to insert a new tape will appear.

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.

Limitations for a locally attached tape device

- A full backup can be stored on an empty tape only. If you use tape that already contains data, its contents will be overwritten.
- Acronis True Image Agent doesn't support a locally attached tape device. If you want to back up to tape via Acronis True Image Agent, select the tape device attached to the Backup Server as the backup location.
- A tape cannot store two and more archives: thus the following scenarios are not possible:
 - • Two full backups on one tape (only a full backup and its incremental backups\different backup)
 - • Two archives of different backup type, for example the first archive is a disk archive, and the second one is a file-level archive.

3.8.2 Understanding backup to tape devices attached to the Backup Server

Archives cataloguing

Acronis True Image Echo Workstation creates a dedicated database for archives and tapes cataloguing (\Program files\Common Files\Acronis\Fomatik\tape_archives.fdb.)

Each tape of an RSM-managed device has its own GUID stored in the Windows registry. Acronis True Image Echo Workstation creates its own ID for each tape, sets up the correspondence between this ID and the RSM GUID and stores that information along with information about the archive in its own database. Additionally, the program stores metadata on tape, so that identification information can be obtained when mounting a tape that is not registered in the database.

If the database is lost or not available (say, you detach the tape device and attach it to another computer or reinstall Windows) the necessary information is derived from the metadata saved on the tape and the database will be recreated on the new host using the

new host RSM. This operation is performed at first access to the tape device while setting up a backup, recovery or validation task. Therefore, under Windows the program knows which tape should be mounted even if the data is recovered on another machine.

When booted from Acronis rescue media or backing up to a locally attached tape device, Acronis True Image Echo Workstation uses another mechanism for access to tape devices since RSM is not available.

Moving tapes between tape devices

A tape that already has backups can be added to a tape device. When the tape device is selected in the recovery or validation wizard, the newly added tape is scanned by the RSM and then by Acronis and added to the Acronis database and the Acronis, or Import Media pool. The access to the archives on the tape becomes available.

However, Acronis will not scan the added tape for changes if the tape already is in the Acronis database. If you eject a tape, back up another machine on this tape and take the tape back to the first tape device, the second machine archive will not be discovered by Acronis and therefore cannot be restored by the first tape device. Please be aware of this limitation when using tapes between multiple computers.

Using RSM pools

At first backup to the tape device, Acronis True Image Echo Workstation takes a tape from the **Free** pool. The program creates the **Acronis** pool and puts the 1st tape in the pool. The tape stays mounted after writing a backup is completed. The next backups, regardless of their contents, will be placed on the same tape, unless the tape free space runs out.

When the 1st tape is full, the program looks for another cartridge in the **Free** pool and uses it without user intervention. If the **Free** pool is empty, a cartridge from the **Import media** pool is used through a prompt. (You have an option to disable prompts, see *6.3.14 Additional settings*.)

So, to fully automate changing tapes at backup, you must always have at least one tape in the **Free** pool (or a tape in the **Import media** pool and the prompt disabled.)

Overwriting old archives

You can move tapes with outdated archives from the **Acronis** pool to the **Free** pool periodically using the Removable storage snap-in. To do so:

1. Select Control panel -> Administrative tools -> Computer management -> Removable storage -> Media pools -> Acronis.
2. Right click on the tape in the Acronis pool, dismount the tape if it has a status Loaded and select **Free** from the context menu. The tape will be moved to the **Free** pool. After putting a tape in the **Free** pool RSM and then Acronis will rescan it and record it to the database with a new GUID.



A deleted archive is not necessarily deleted from the tape, it can be just marked as deleted in the catalogue.

Saving a full backup to a new tape

You can enable saving a **full** backup on a new tape even if the currently mounted tape is not full. To do so, dismount the current tape and eject it, add a new tape and move the tape to the **Free** pool using RSM. Incremental or differential backups cannot be performed in this way because access to the previous backups is required.

3.8.3 Backing up to a tape device through Acronis Backup Server

To enable backup to a tape device in the local network:

1. Install Acronis Backup Server on a computer accessible to all users.
2. Attach the tape device to that computer.
3. Move tapes from the **Unrecognized** or **Backup** pool to the **Free** pool using the Removable storage snap-in (Control panel -> Administrative tools -> Computer management -> Removable storage -> Media pools.)
4. Create local accounts on that computer for all users who will back up their data to the autoloader. Accounts must belong to the AcronisBackupServerUsers group and be the real accounts with which users log in Windows.
5. When creating backup tasks (if logged in Windows with the above accounts), users of Acronis True Image Echo Workstation local version will be able to select the tape device from the list of Backup Server locations.

The backup server administrator can create group or individual tasks for computers to back up their data to the tape device using Acronis True Image Management Console. Filenames for backups are not needed when backing up to tape.

Archives, created on tape devices through Acronis Backup Server, cannot be accessed by Acronis True Image Echo Workstation local and bootable versions and agents for validation, data recovery and converting images to virtual disks.

When the tape is full, you must dismount it first before ejecting.

You can attach the tape device to another Acronis Backup Server, if need be (say, the current backup server is down.) Before doing so, delete the Acronis database for tape devices on that computer, if there is one (\Program files\Common Files\Acronis\Fomatik\tape_archives.fdb.) This will allow the backup server to create the database for the newly attached tape device using metadata contained on tapes.



Acronis Backup Server does not allow for creating manageable backup locations on tape devices. This means that you cannot limit the number of backups or the period while the archives are stored on tape devices. This functionality is supported only on the backup server internal hard drives.

3.8.4 Restoring data from archives located on tape devices

Data recovery from archives located on tape devices is performed in the same way as with other storage devices.

When recovering, you start the restore wizard, select the local tape device or tape device under the backup server, select the archive and the backup to restore data from.

[Tape drive] You will be prompted to insert tapes required for restoring data from the selected backup.

[Tape library or autoloader] The program finds the tapes and inserts them automatically in the right order. A prompt comes up if the required tape is not found.



Archives created on tape devices through Acronis Backup Server cannot be accessed by a locally attached tape device in Acronis True Image Echo Workstation local version.



Implementation notice

Due to the wide variety of tape libraries and configuration complexity, for detailed information on how to implement Acronis True Image Echo Workstation with tape devices please contact Acronis support specialists.

3.9 Viewing disk and partition information

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

To the right are three icons: **Arrange Icons by**, **Choose Details** and **i (Display the properties of the selected item)**, the 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.

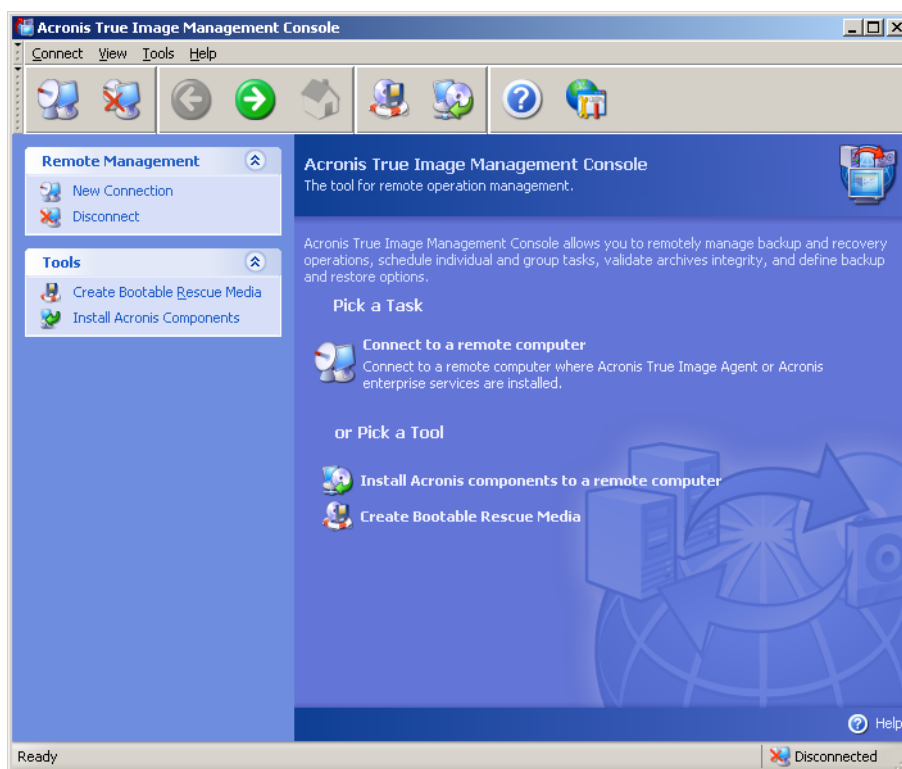
This window contains two panels. The left panel contains the properties tree and the right describes the selected property in detail. The disk information includes its physical parameters (connection type, device type, size, etc.); partition information includes both physical (sectors, location, etc.),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

You can change the width of a column by dragging its 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 for the managing of computer groups and corporate backup archives using Group and Backup Servers, as well as managing individual backup/restore tasks for every computer.



Acronis True Image Management Console main window

4.2 Installing/updating Acronis components on remote machines

Acronis True Image Management Console allows for group installation and updates of Acronis True Image Echo Workstation (local version) and Acronis True Image Agent for Windows on remote computers. To perform any of these operations, you will need administrator rights on the target machines.



Installation of Acronis components onto remote machines running all Windows Vista editions is not possible. You will have to install the components locally on such computers.



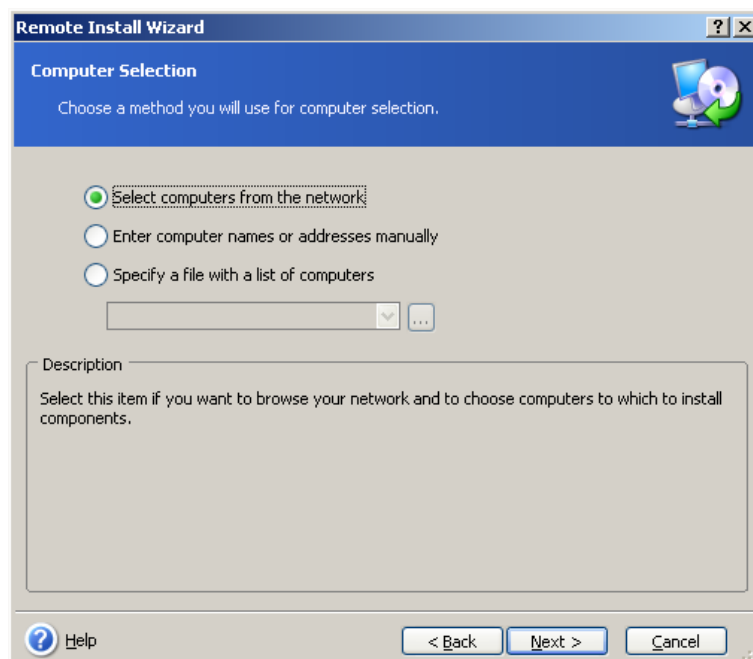
If the remote computer runs Windows XP, the option **Control panel -> Folder options -> View -> Use simple file sharing** must be disabled on that computer.



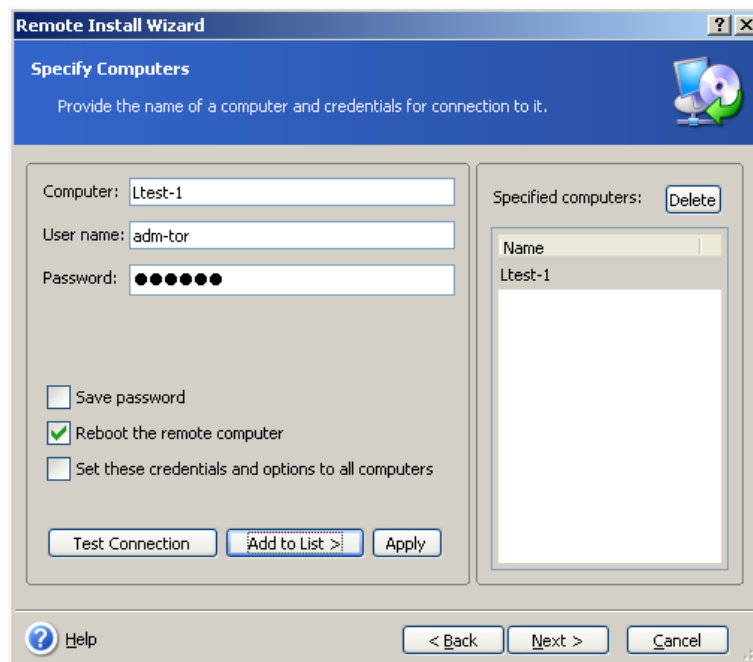
If the remote computer runs Windows XP with Service Pack 2, Service Pack 3 or Windows 2003 Server, the option **Control panel -> Windows Firewall -> Exceptions -> File and Printer Sharing** must be enabled on that computer.

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 *2.3 Installing Acronis True Image Echo Workstation components*.)
4. Select computers on which the Acronis component is to be installed. This can be done by:
 - browsing the network. When browsing the network, you can select entire workgroups or domains
 - typing the computers names or addresses (click **Next** then add computers to the list)
 - importing the computers list from .txt or .csv files.



5. Provide administrator username and password for each computer. If there is a universal administrator account on the network, enter the account credentials for one computer and set the option to apply it to all computers that you select. Domain administrator credentials and universal credentials for workgroups can be applied in this way.



If you do not specify credentials for all machines involved, or if the credentials are not valid for some machines, you will have an option to provide credentials during installation (there is an option **Other user** in the username/password error prompt.)

Most Acronis components require the system restart on their installation. To allow immediate remote computer reboot, check the **Reboot the remote computer** box. This option also can be applied to all computers or set to each machine individually.

6. The summary window displays a list of computers where the Acronis component will be installed.

7. Once the installation starts, the program displays the operation progress and the name of the computer on which the component is being installed.

To update an Acronis component on a remote computer, perform the same procedure.

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:

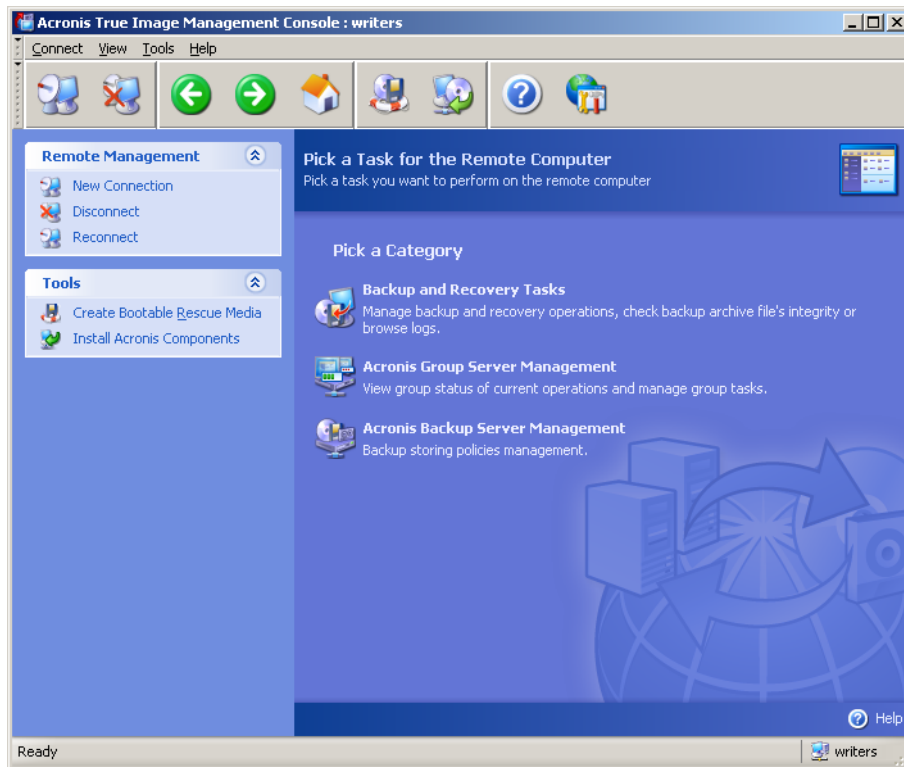
1. Click **Connect to a remote computer** in the center of Acronis True Image Management Console main window or on the toolbar, or select **New connection** from the sidebar or the **Connect** menu.
2. Enter the computer network name, IP address or select it using **Browse...** button. **Browse...** will open a list, including all computers controllable with Acronis True Image Management Console.
3. Enter administrator or backup operator username and password.



When connecting to a **backup server inside a domain**, mind whether your domain or local account is registered on the backup server. If you entered Windows on a network computer using your domain account while your local account is registered, enter the local user name along with the backup server name (for example, Server1\username).

Otherwise the name will be identified as a domain one.

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



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** (using the Acronis True Image Agent), **Acronis Group Server Management** and **Acronis Backup Server Management**.

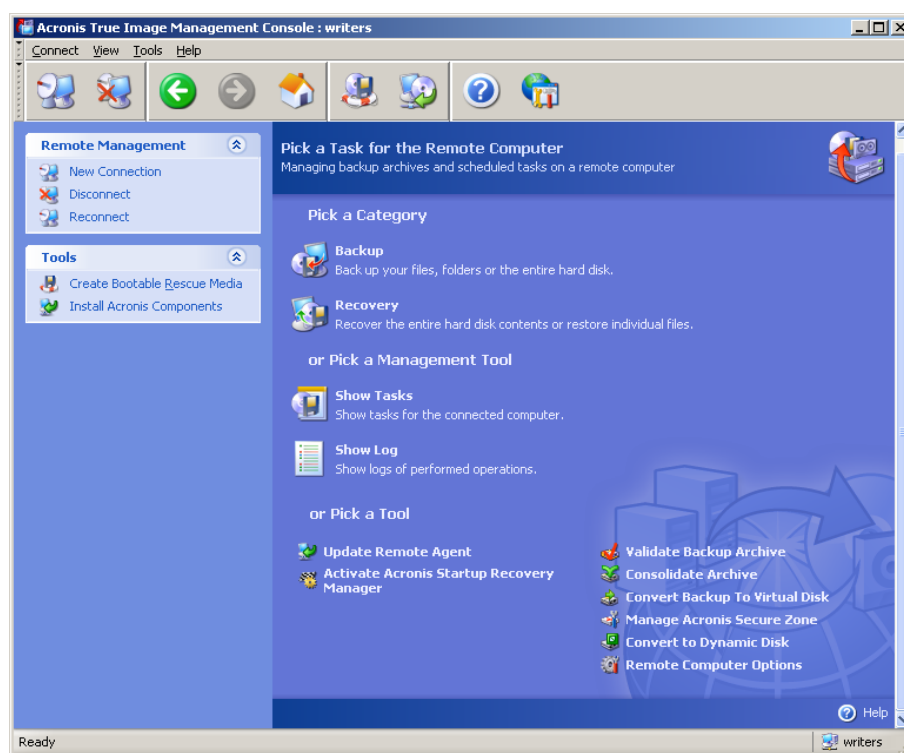
While you are operating on a remote computer, the computer could reboot or the connection to the computer could be broken for other reasons. This will result in operations failure, such as hiding of the remote computer file system in wizards, or operation may hang. Use **Reconnect** on the sidebar to test whether the computer is available again or eliminate any malfunction that persists.

The console automatically attempts to reconnect to the last connected machine every 30 sec. To change the time interval between the attempts, select **Tools -> Options -> Network -> Reconnect options**.

When the console is disconnected, Reconnect provides a handy one-click connection to the most recently accessed machine.

4.3.2 Backup and recovery tasks

After clicking on **Backup and Recovery Tasks**, the program window will appear like the graphic below:



You can perform the following operations on the remote computer.

Operation

How to access

Back up and Recover

Back up 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*.

Browse logs of Acronis True Image Agent operation

Click **Show Log**. See details in *12.3 Viewing logs*.

Set up default backup or 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*.

Set up default parameters for sending notifications about Acronis True Image Echo Workstation operation and tracing this operation in the Windows Application Event Log

Click **Remote Computer Options**, select **Notifications** or **Event tracing** and make settings. See details in *Chapter 12. Notifications and event tracing*.

Scheduling Tasks

- | | |
|--|---|
| Schedule backup and archive validation operations | Click Show tasks to navigate to the Manage Computer Tasks window. Click Create then follow the wizard's instructions. See details in <i>Chapter 8. Scheduling tasks</i> . |
| Run, stop, edit, clone, rename, delete backup and archive validation tasks | Click Show tasks to navigate to the Manage Computer Tasks window. See details in <i>8.2 Managing scheduled tasks</i> . |

Archives Management

- | | |
|--|---|
| 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 <i>11.1 Validating backup archives</i> . |
| Consolidate backup files in an archive | Click Consolidate archive , then follow the Wizard's instructions. See details in <i>11.3 Consolidating backup</i> . |
| Convert disk images to virtual disk files of the type you select (.vmdk, .vhd, .hdd) | Click Convert backup to Virtual Disk and follow the wizard's instructions. See details in <i>13. 4 Converting disk images to virtual disks</i> |

Hard Disk Management

- | | |
|--|--|
| Manage Acronis Secure Zone (create, delete, resize, remove or change password) | Click Manage Acronis Secure Zone , then follow the wizard's instructions. See details in <i>Chapter 9. Managing the Acronis Secure Zone</i> . |
| Activate Acronis Startup Recovery Manager | Click Activate Acronis Startup Recovery Manager , then follow the wizard's instructions. See details in <i>3.4 Acronis Startup Recovery Manager</i> . |

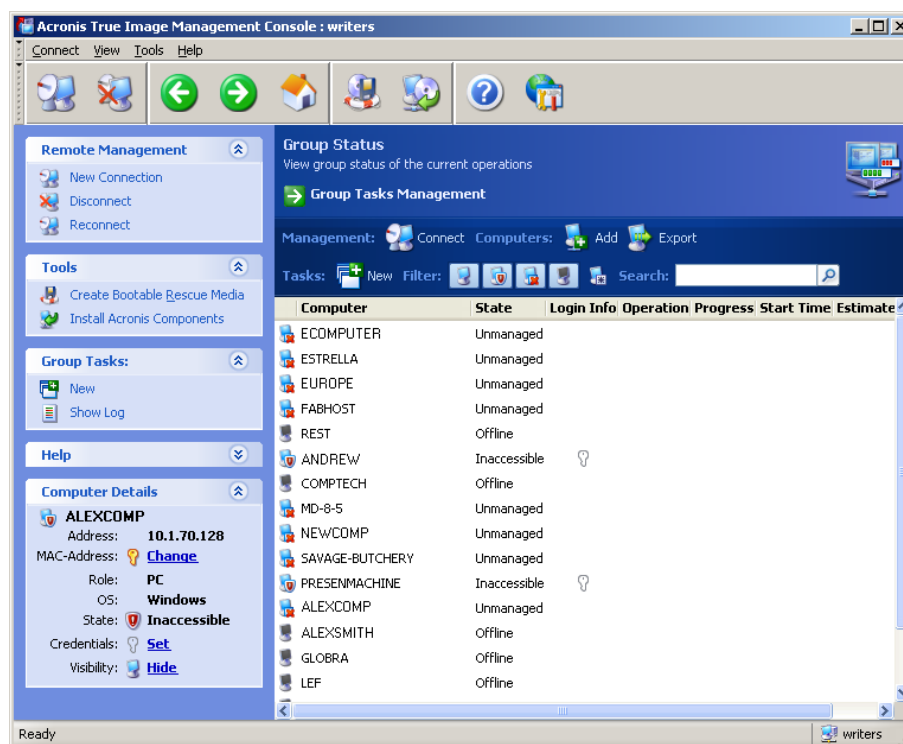
Other Tools

- | | |
|--|---|
| Create bootable rescue media, its ISO or RIS package | See <i>Chapter 10. Creating bootable media</i> . |
| Update the remote agent | Click Update the remote agent , then follow the Wizard's instructions. The procedure is the same as described in <i>4.2 Installing/updating Acronis components on remote machine</i> |
- 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 status display

When connected to a computer where Acronis Group Server is installed, click **Acronis Group Server management** to display the following window.



Here you can monitor states of Acronis True Image Echo Workstation 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

Offline - the remote computer is not connected to the network or is 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 the remote machine.

Use **Search** to find a computer in the list quickly.

To see details of the computer in brief (the computer role, operating system and IP address), click 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 name.

You can also search computers by their IP. To use this function you should proceed to **Tools->Options->Network->Computers Discovery** and specify the search parameters in the "Search for computers whose IP match the mask" and/or in the "Search

for computers in the following domain" fields. If you do not remember the correct IP or you want to expand the search results to several computers, you can use the IP masks. To define the range of necessary digits, for example, 192.168.1.12 - 192.168.1.19, the IP mask has to include patterns as in 192.168.1.[12-19]. If you use several masks, for example for the 192.168.2.12 - 192.168.5.25 range, you have to separate them with the vertical line as in 192.168.2.[12-255]|192.168.[3-4].*|192.168.5.[0-25].

In this window you can also:

1. **Filter out** from the list offline, inaccessible or unmanaged computers or filter out online computers to see those that cannot be managed (use buttons in the **Filter** group).
2. **Import computers** into the group server in case they are not discovered automatically due to network behavior. It makes sense to install Acronis components on these computers first so that you will be able to create tasks for these computers.

To add a single computer:

- click **Add** on the toolbar
- type in the computer name or IP address.

To add computers from Active directory:

- click **Add** on the toolbar
- type in the exact domain names

or otherwise type in the name of the domain controller and when the active directory is expanded, tick off the desired computers or the entire directory.

To add multiple computers from a file:

- prepare a .txt or .csv file, listing semicolon-separated computers names and IP addresses as follows: Name1; IP1; Name2; IP2;...
- click **Add** on the toolbar
- specify path to the above file.

3. **Export computers** from the group server to a .txt or .csv file that can be used by other application or new versions of Acronis Group Server. To do so:

- click **Export** on the toolbar
- specify name of the file and a path to a folder where you want to create it.

4. Set and test credentials for access to each computer. To do so, select the computer, then select on the sidebar **Computer details** -> Credentials: **Set**, type username and password and click **Test connection**. The program will display the test result. Key icons for successfully tested connections are colored gold.

5. Set (or change) the MAC address for each computer. To do so, select the computer, then select on the sidebar **Computer details** -> MAC address: **Set** or **Change** and type the hex MAC address as XXXXXXXXXXXX or XX-XX-XX-XX-XX. The program will test the MAC address for validity and display the test result.

6. Hide computers that you do not wish to browse or make a hidden computer visible. To hide a computer, select it, then select on the sidebar **Computer details** -> Visibility: **Hide**. To make a hidden computer visible (and monitored), enable Show hidden computers in the Filter group, select the hidden computer, then select on the sidebar **Computer details** -> Visibility: **Unhide**.

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

8. **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**.

9. Switch to the **Group tasks management** window for managing group tasks.

4.4.2 Creating new group tasks

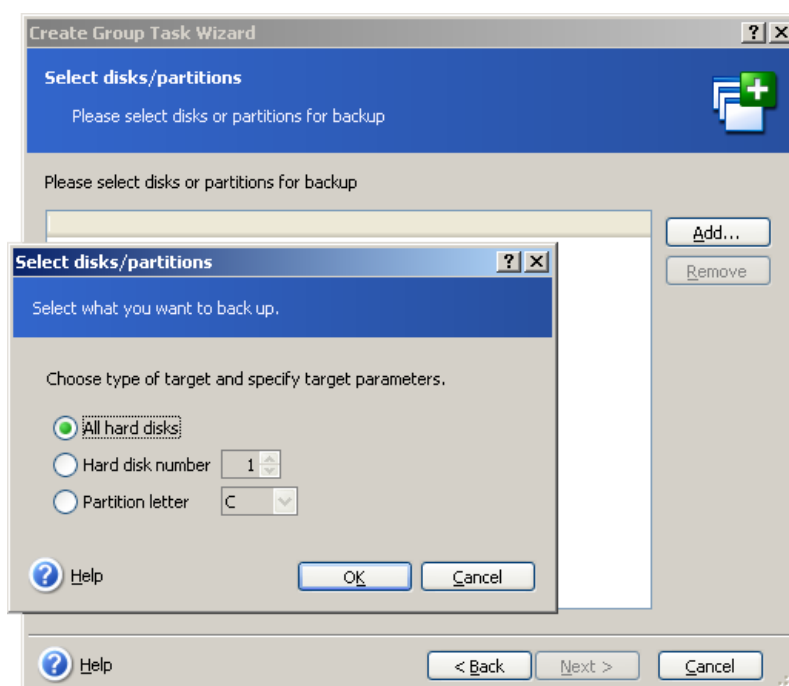
You can create a disk/partition backup task or archive validation task for several remote computers at once. File-level backup for groups of computers is unavailable.

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

2. Select the type of the task: backup or validation.

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

4. For the backup task only: 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

5. Specify the paths for the backup archives. To place every archive on its local computer, specify **Local path** or select **Acronis Secure Zone**, if there is such a zone on every remote computer. For more information about the 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 the name input field will assign to each archive the respective computer's name.

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

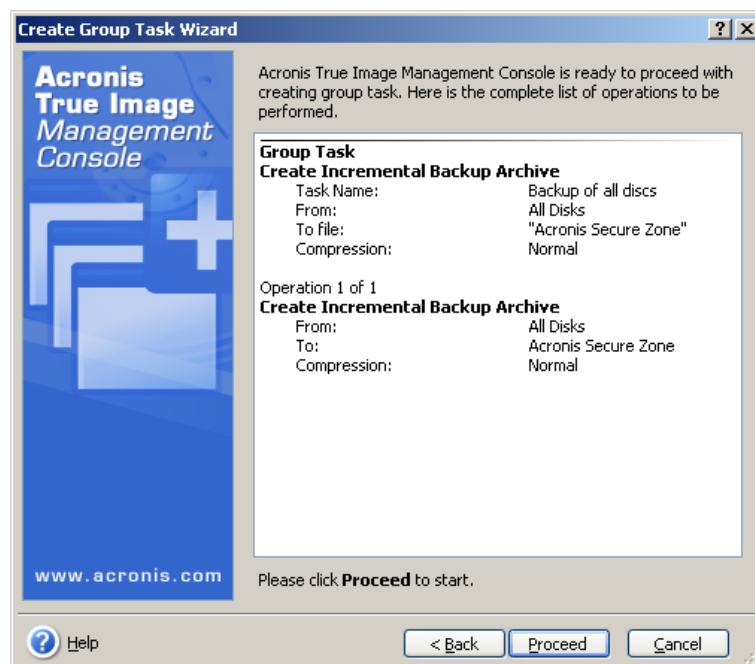
7. Provide a name for the group task. The name will be displayed in the **Group Tasks Management** window (see below) to allow quick task identification.

8. 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.

9. If, for any reason (traffic limitation, for example), you do not want the task to start on all computers simultaneously, set the **Start time shift** parameter. The task will start on all computers in turn, with the 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.

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

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



Group task summary

12. 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 complete, 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, mouse over the task name.

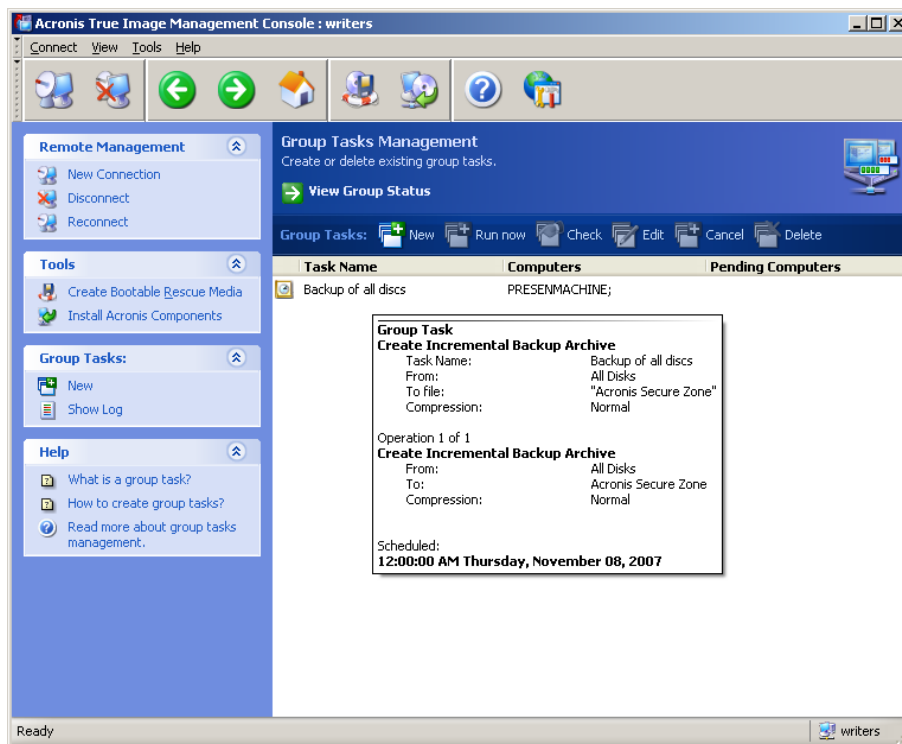
To create new or delete existing backup task, use the **New** and **Delete** items on the **Group tasks** toolbar.

To edit a task, select it and click **Edit**. Editing is performed in the same way as creation, however, the earlier selected options will be set, so you have to enter only the changes.

Deleting or editing a task does not affect the current task execution. A task, that has been edited or deleted while running, will come to an end without any changes. The changes you made will be applied when execution is completed.



In addition to editing tasks for groups, you can edit individual tasks produced by the group task on each computer involved. To do so, connect the console to the desired computer. For details, see *8.2 Managing scheduled tasks*.



To stop or restart the task execution, use the **Stop** or **Restart** toolbar items. The task schedule, if created, remains valid.

For a group task that is not currently being executed on either computer, the following operations are also available:

Run now - an instant task start command. The task schedule, if created, remains valid.

Check – the group server will connect in turn to all computers involved in the group task and check if the child tasks are intact on the computers so that the group task can run effectively. The result will be displayed.

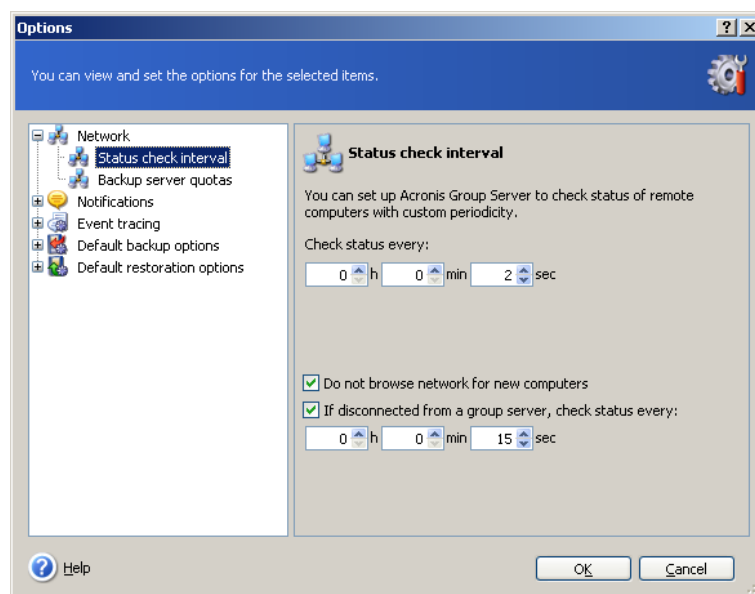
When managing a group task, enter the same username and password you entered when created the task.

4.4.4 Acronis Group Server options

Acronis Group Server regularly polls computers included in its database for their status (Ready, Offline and so on, according to *4.4.1 Group status display*.) The default interval between enquires is 2 seconds. You have an option to set the status refresh rate based on your network requirements.

There is usually no need to refresh the view at all when the console is disconnected from the group server. A separate option allows you to disable the polling on console disconnection or set a wider interval between packets.

There is also an option to stop scanning network for newly connected computers. This can speed up operations with the computers already discovered. After the scanning is disabled, Acronis Group Server stops sending the packets, but the response may come to the packets already sent. Therefore, some computers may be added to the computer list after scanning is disabled. This is not a malfunction.

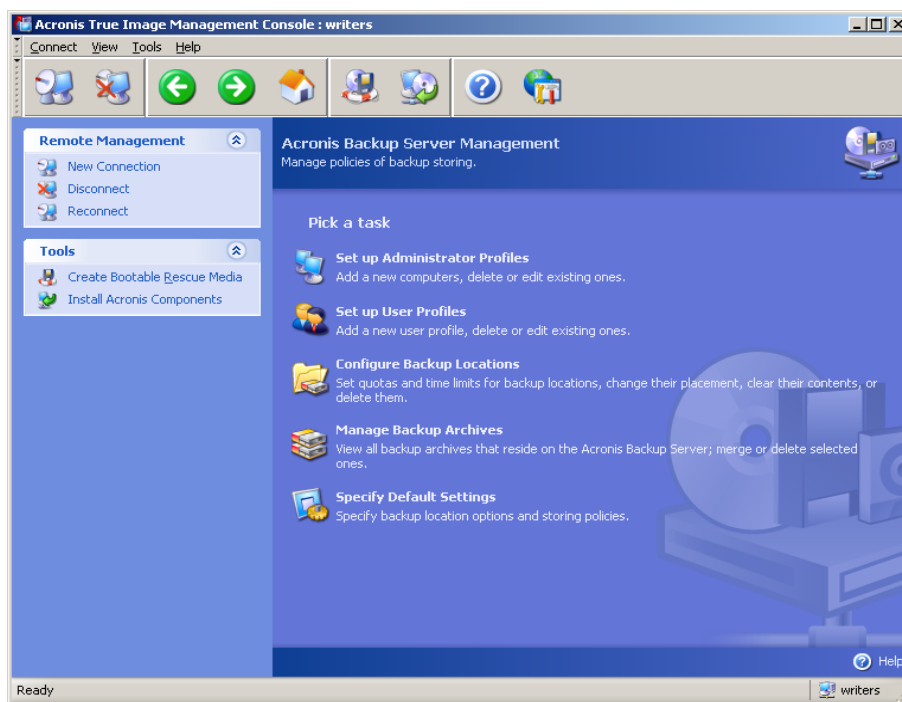


To adjust the status refresh rate, connect the console to the computer where Acronis Group Server is installed and select **Tools -> Options -> Network -> Status check interval**.

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 application.

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



When connecting to a **backup server inside a domain**, be aware whether your domain or local account is registered on the backup server. If you entered Windows on a network computer using your domain account while your local account is registered, enter the local user name along with the backup server name (for example, Server1\username). Otherwise the name will be identified as a domain one.

4.5.1 Default settings

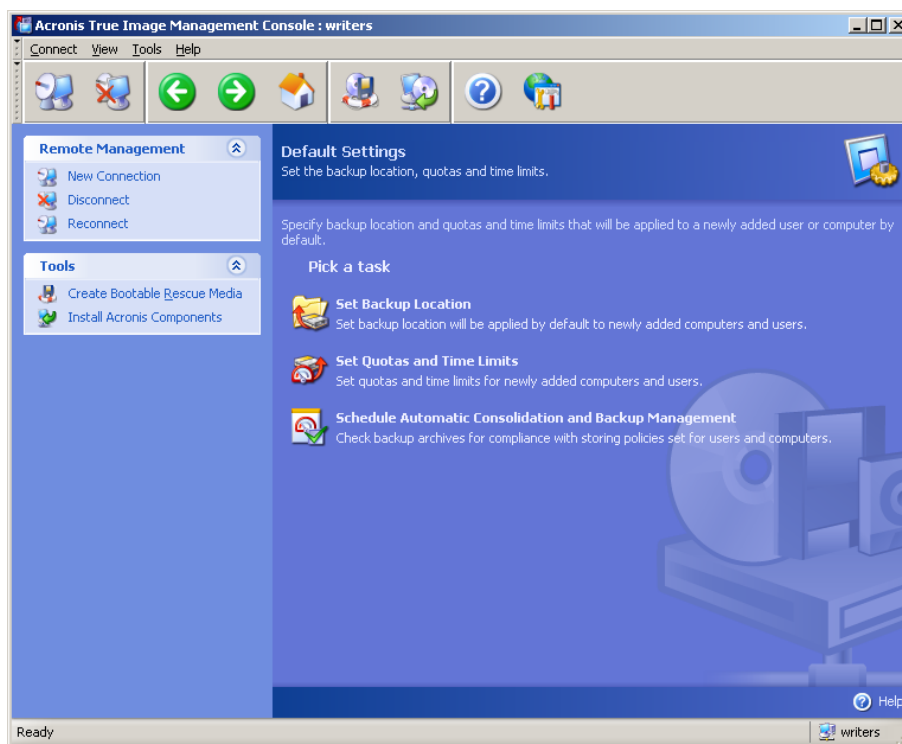
Each user or computer, added to Acronis Backup Server database, is associated with the default backup location and the default user/computer quotas and time limits.

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.

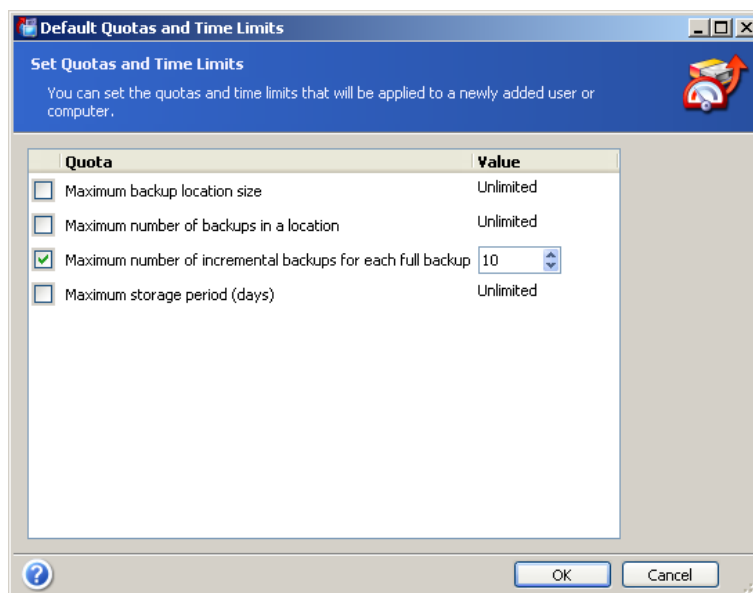
This folder is a default backup location.

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.



The default quotas/time limits are preset to **Unlimited**, except for **Maximum number of incremental backups for each full backup**, 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).

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 makes no sense if you have not changed at least one of the preset **Unlimited** values for quotas/time limits.

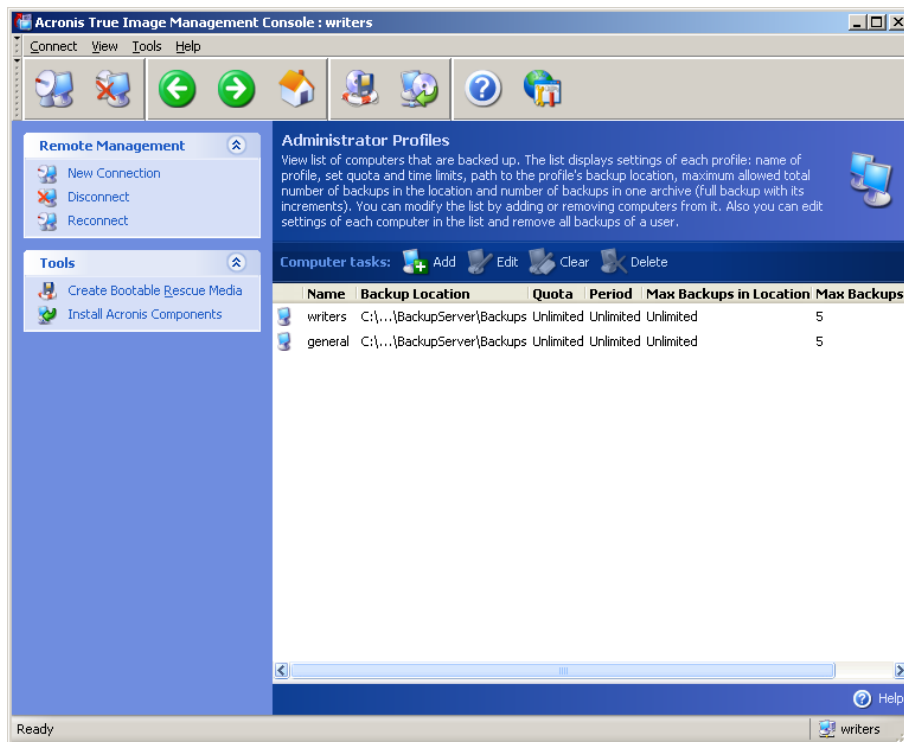


The actual number of backups created in a backup location can exceed the **Maximum number of backups** by one. This enables the program to detect the fact of exceeding and start consolidation. Backup to the full location will be prohibited until the consolidation takes place.

4.5.2 Set up Administrator profiles

Add a remote computer to Acronis Backup Server database if you want to be able to remotely back up data from that networked computer where Acronis True Image Agent is installed. 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 this 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 folder.

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 can be time-consuming so schedule it for the off-peak period.

4.5.3 Adding Users and Administrators to the Acronis Backup Server database

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

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

To enable any other user to back up data from any networked computer where Acronis True Image Echo Workstation 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's local or domain account to the AcronisBackupServerUsers group. Then click **Set up User profiles -> Add User**.

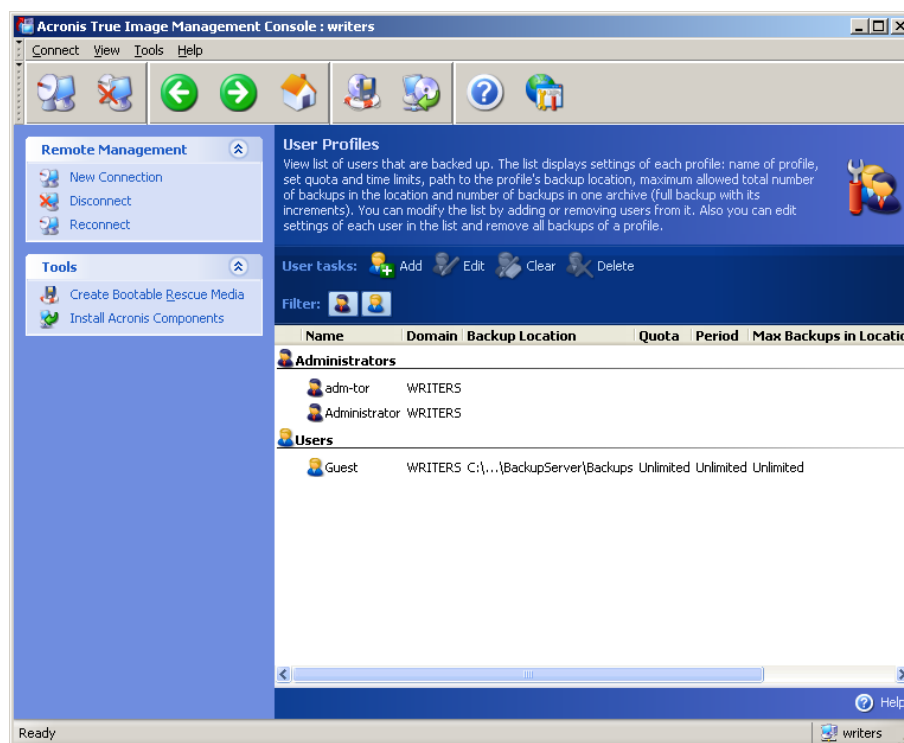
The **Add User Profile Wizard** will offer you a choice of adding the new user name from the list of domain users, or entering it manually. In some cases, when the list of domain users is excessively big, the manual way of entering the new user name will prove quicker, but you have to know the exact user name.



If you click **Next**, you will go to the window where you can enter the user name manually, if you don't know the correct user name, you will be able to return to the previous window and pick the other option.



If you opted for picking the user name out of the domain user list, you will skip the above window and proceed to the other windows where you will 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 specific 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's local or domain account to the 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, the administrator is not assigned a

backup location, quotas and time limits like common users are and uses the administrator profile for both remotely and locally controlled backups.

4.5.4 Changing User profiles

You might need to change a user profile that is 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 can 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 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 profile and click **Clear**, all archives created by this user will be deleted. However, this operation will not work for the administrators' profiles.

If you select a user profile and click **Delete**, this will disable backup to the 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.

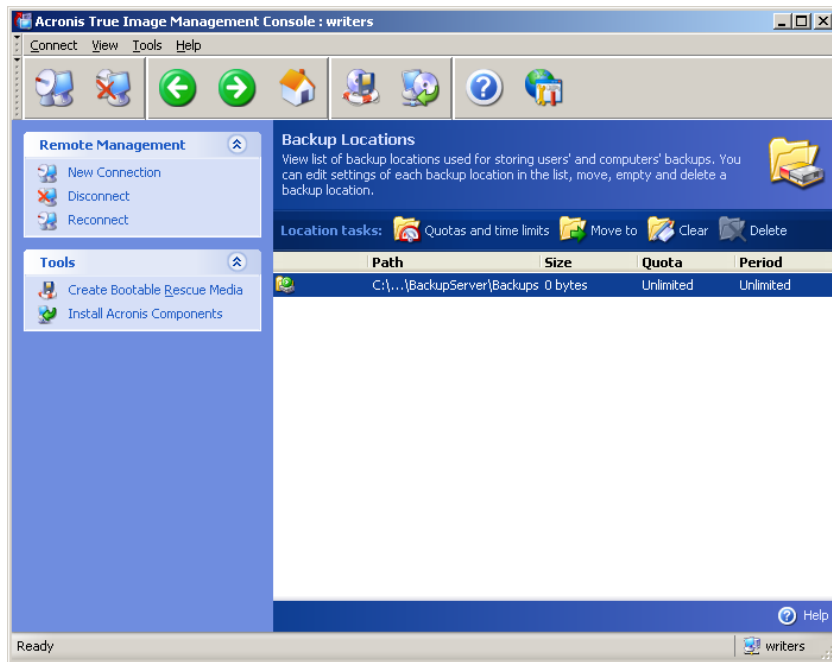
Deleting an administrator profile will not result in deleting any archives. The person whose profile is deleted just loses the right to back up to the backup server and to manage the backup server.



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 **Quotas and Time Limits** 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 can 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.

To delete all archives stored in a backup location, select the location and click **Clear**.

To delete a backup location, select the location and click **Delete**. This will delete all archives stored in this location and redirect the associated computer/user's backups to the default backup location.

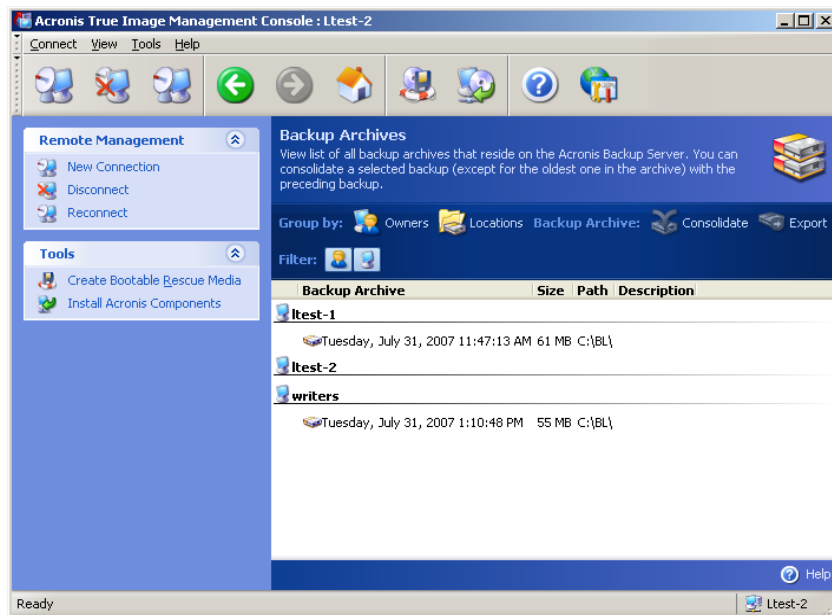


The default backup location cannot be deleted. If you try to do so, the program will clean the default backup location and issue an appropriate message. To delete the location completely, first reassign the default backup location by selecting **Specify Default Settings -> Set backup location**.

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. This operation deletes the preceding backup and sets concatenation between the backup being consolidated and the backup before the deleted one. Thus, the archive integrity will not be affected, in spite of the fact that one backup will be deleted. Data recovery from any of the remaining backups will be possible.
4. Export an archive from Acronis Backup Server to a local hard drive or network share. To do so, select any backup belonging to the archive and click **Export**. Then provide name for the archive copy and a path to the location where the copy will be created.
5. Import an archive from external location to a computer's or user's backup location on the backup server. To do so, use **Import** on the toolbar.



Editing images, mounted in R/W mode, results in creating incremental backups, that are a kind of offshoots of the incremental chain. Such backups are always excluded from the archive being imported.

4.5.7 Limiting access to Acronis Backup Server

To access the Acronis Backup Server options, connect the console to the backup server and select **Tools -> Options** from the menu.

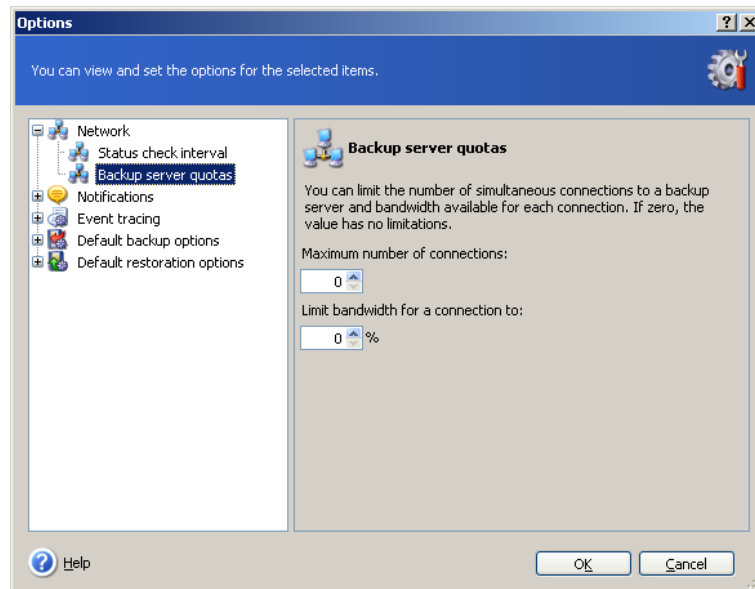
1. Maximum number of connections

This comes in handy when you want to back up a group of computers quickly and not allow users to access the backup server at the time. Generally, limiting number of tasks simultaneously processed by Acronis Backup Server may speed up each taken separately backup procedure at the expense of its possible delay.

If maximum number of connections is set, then some agents or local Acronis True Image Echo Workstation versions may be unable to access the server immediately after starting

their task. They will be trying to connect to the server every 5 seconds until the connection is allowed. Therefore, the real backup start time may differ from the scheduled one. If it is not practical or efficient for you, be aware of this setting when creating group tasks so that number of computers in the group does not exceed the limit you set.

By default, the number of connections is unlimited. This corresponds to setting "0". The console connection to Acronis Backup Server is not counted.



2. Limit bandwidth for a connection to:

Limiting bandwidth for each connection helps equalize the server usage among simultaneously running tasks. Practice is the best way to determine the correct limit. In most cases you can leave it as is.

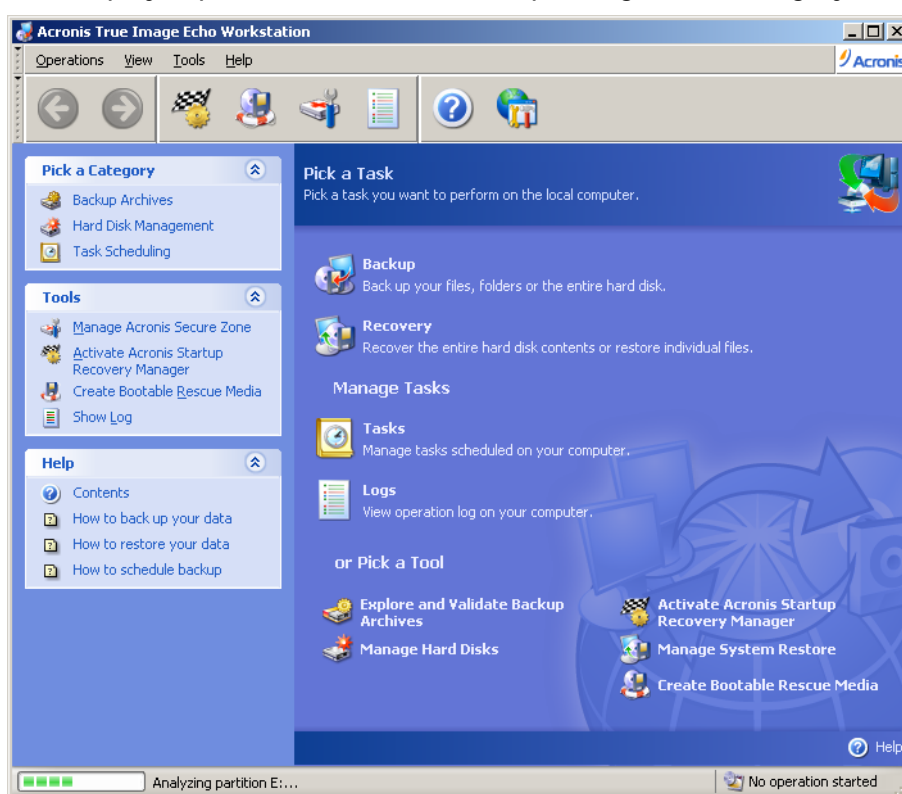
By default, bandwidth per connection is not limited. This corresponds to setting "0".

Chapter 5. Using Acronis True Image Echo Workstation (local version)

Acronis True Image Echo Workstation (local version) supports the GUI mode, the command-line mode, and can be used to execute XML scripts. Here we describe the operations available in the GUI mode, which provides the widest functionality. For console commands and scripting please see *Chapter 16. Command-line mode and scripting*.

5.1 Main program window

The main program window contains the menu, the toolbar, the sidebar and the main area. The sidebar features a pane for selecting task category, the **Tools** and **Help** panes. The main area displays operation icons or tasks depending on the category selected.



By default, the program displays operations included in the **Backup and Recovery** category. Operation icons are divided into three groups.

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

- **Backup** – create a backup archive
- **Recovery** – restore data from a previously created archive

The **Manage Tasks** group contains the following operations:

- **Tasks** – schedule backup or archive validation tasks on your computer and manage them
- **Logs** – open the Log Viewer window

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

-
- **Explore and Validate Backup Archives** – explore file-level archives, mount disk/partition images as virtual drives, run the archive integrity checking procedure
 - **Manage Hard Disks** – clone disk (i.e. transfer the OS, applications and data from the old disk to the new one) or mark out partitions on a new hard disk added for data storage with the OS and applications kept on the old one, convert basic disks to dynamic and create dynamic volumes
 - **Activate Acronis Startup Recovery Manager** – activate the boot restoration manager (F11 key)
 - **Manage System Restore** – turn on/off Microsoft Windows System Restore tool and set its options directly from Acronis True Image Echo Workstation
 - **Create Bootable Rescue Media** – run the bootable media creation procedure

Program menu

The program menu bar 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:

- **Toolbars** – contains commands that control toolbar icons
- **Common Task Bar** – enables/disables the sidebar
- **Status Bar** – enables/disables the status bar

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

- **Manage Acronis Secure Zone** – create, delete and resize a special hidden partition for storing archives (Acronis Secure Zone)
- **Activate Acronis Startup Recovery Manager** – activate the boot restoration manager (F11 key)
- **Explore Backup Archive** – explore file-level archives or mount disk/partition images as virtual drives
- **Validate Backup Archive** – run the archive integrity checking procedure
- **Consolidate archive** – applicable for archives containing more than one backups. This will create a consistent copy of the archive with an option to exclude backups that are no more needed
- **Convert Backup to Virtual Disk** - convert a disk image, created with the program (.tib), to a virtual disk file of the type you select (.vmdk, .vhd, .hdd)
- **Create Bootable Rescue Media** – run the bootable media creation procedure
- **Dynamic Volume Creation Wizard** – create dynamic volumes on basic or dynamic disks
- **Show Log** – open the Log Viewer window
- **Options** – open a window for editing default backup/restore options, setting text appearance (fonts), configuring e-mail or Windows pop-up notifications etc.

The **Help** menu is used to view help and obtain information about Acronis True Image Echo Workstation.

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.

Status bar

There is a status bar divided into two parts at the bottom of the main window. 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 log window.

Taskbar notification area icon

During most of the operations, a special indicator icon appears in the Windows taskbar notification area. 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.

Operation	How to access
Back up and Recover	
Back up and restore data, including system disks/partitions	Click Backup or Recovery , then follow the wizard's instructions. See details in <i>Chapter 6. Creating backup archives</i> and <i>Chapter 7. Restoring the backup data</i> .
Browse logs of Acronis True Image Echo Workstation operation	Click Logs in the Manage Tasks group or select the Show Log tool on the sidebar to navigate to the Event Log window. See details in <i>12.3 Viewing logs</i> .
Set up default backup or 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 <i>6.3 Setting backup options</i> and <i>7.4 Setting restore options</i> .
Set up default parameters for sending notifications about Acronis True Image Echo Workstation operation and tracing this operation in Windows Application Event Log	Select Tools -> Options -> Notifications or Event tracing and make settings. See details in <i>Chapter 12. Notifications and event tracing</i> .
Scheduling Tasks	
Schedule backup and archive validation operations	Click Tasks in the Manage Tasks group or select the Task Scheduling category on the sidebar to navigate to the Scheduled Tasks window. Then click the Create button on the toolbar and follow the wizard's instructions. See details in <i>Chapter 8. Scheduling tasks</i> .

Run, stop, edit, clone, rename, delete backup and archive validation tasks	Click Tasks in the Manage Tasks group or select the Task Scheduling category on the sidebar to navigate to the Scheduled Tasks window. See details in <i>8.2 Managing scheduled tasks</i> .
--	--

Archives Management

Explore any archive's contents and restore individual files from any archive	Select Tools -> Explore Backup Archive and follow the wizard's instructions. See details in <i>11.2.1 Exploring an archive</i>
Validate backup archives wherever they reside, be it local, network or removable media	Select Tools -> Validate Backup Archive , then follow the wizard's instructions. See details in <i>11.1 Validating backup archives</i> .
Consolidate backup files inside an archive	Select Tools -> Consolidate archive , then follow the Wizard's instructions. See details in <i>11.3 Consolidating backup</i> .
Convert disk images to virtual disk files of the type you select (.vmdk, .vhd, .hdd)	Select Tools -> Convert backup to Virtual Disk and follow the wizard's instructions. See details in <i>13. 4 Converting disk images to virtual disks</i> .
Mount partitions' images to explore and modify their contents, or to restore individual files	Select Operations -> Mount Image and follow the wizard's instructions. See details in <i>11.2.2 Mounting an image</i> .
Unmount previously mounted partition images	Select Operations -> Unmount Image and follow the wizard's instructions. See details in <i>11.2.3 Unmounting an image</i> .

Hard Disk Management

Manage Acronis Secure Zone (create, delete, resize, remove or change password)	Click Manage Acronis Secure Zone , then follow the wizard's instructions. See details in <i>Chapter 9. Managing the Acronis Secure Zone</i> .
Activate Acronis Startup Recovery Manager	Click Activate Acronis Startup Recovery Manager , then follow the wizard's instructions. See details in <i>3.4 Acronis Startup Recovery Manager</i> .
Create a dynamic volume	Select Tools -> Dynamic volume creation wizard , then follow the Wizard's instructions. See details in <i>7.5.1 Creating dynamic volumes</i> .
Transfer the system to a new hard disk	See <i>Chapter 14. Transferring the system to a new disk</i> .
Format partitions on a new hard disk	See <i>Chapter 15. Adding a new hard disk</i> .

Other Tools

Create bootable rescue media, its ISO or RIS package See *Chapter 10. Creating bootable media.*

Turn on/off Windows System Restore tool See *12.5 Managing System Restore.*

Some of the above operations can be executed in command-line mode. For more information on Acronis True Image Echo Workstation command-line mode see *16.1 Working in the command-line mode.*

Chapter 6. Creating backup archives

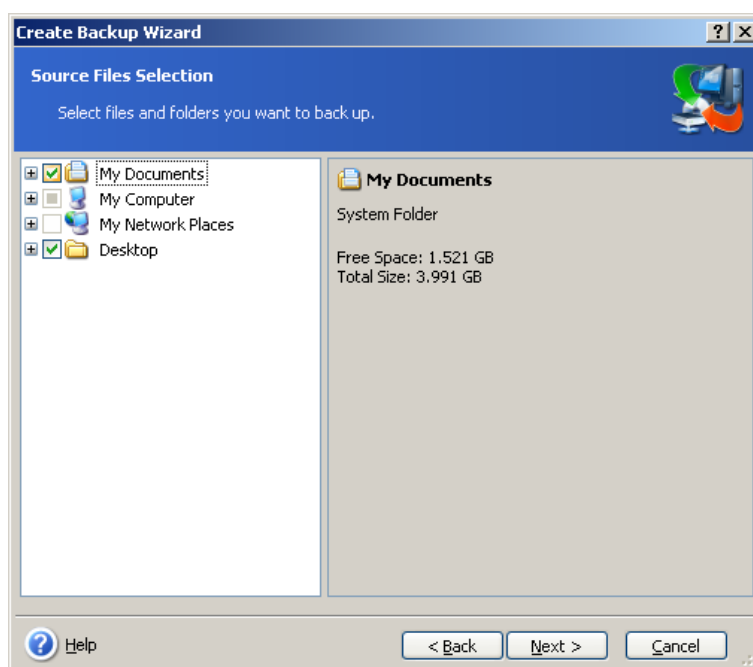
To be able to restore the lost data or roll back your system to a predetermined state, you should first create a data or entire system backup file.

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)

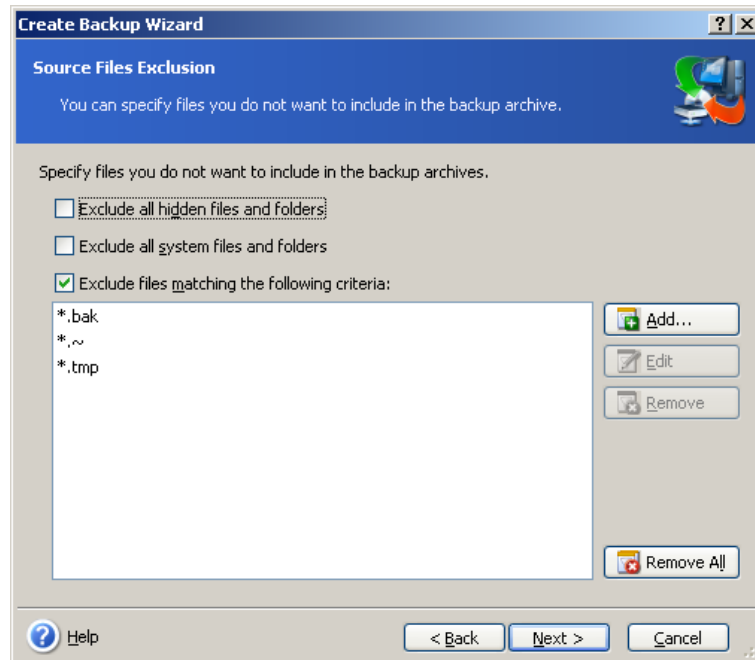
1. Start the **Create Backup Wizard** by clicking on the backup operation icon in the main program window.
2. Select **My Data**.
3. From the tree pane, select files and folders to back up. You can select a random set of files, folders, partitions, disks and even computers.



In order to restore your operating system, you must image the system disk or partition; a file-based backup is not sufficient for the operating system restore.

4. You can exclude specific files from a backup by setting filters for the types of files you do not wish to back up. For example, you may want to exclude hidden and system files and folders or files with **.~, .tmp and .bak** extensions.

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



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

5. Select the name and location of the archive.

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 full backup, it will be overwritten.

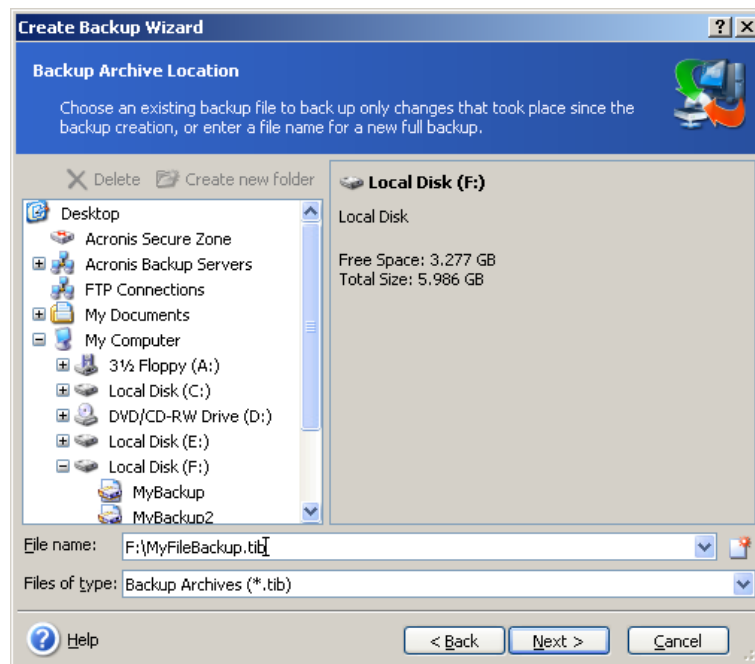
Including [date] in the backup file name will add to the name the time and date of the backup creation formatted as <DD-Month-YYYY HH:MM:SS>. Example: C:\MyBackup[date].tib.

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 with the basic full backup, 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 the existing differential backups. Either way, the program will create a new differential backup.



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, but won’t be useful if the computer is destroyed in a fire or flood. 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*) or Acronis Backup Server (see details in *3.5 Acronis Backup Server*) for storing backups. In those cases, you need not provide the file name.

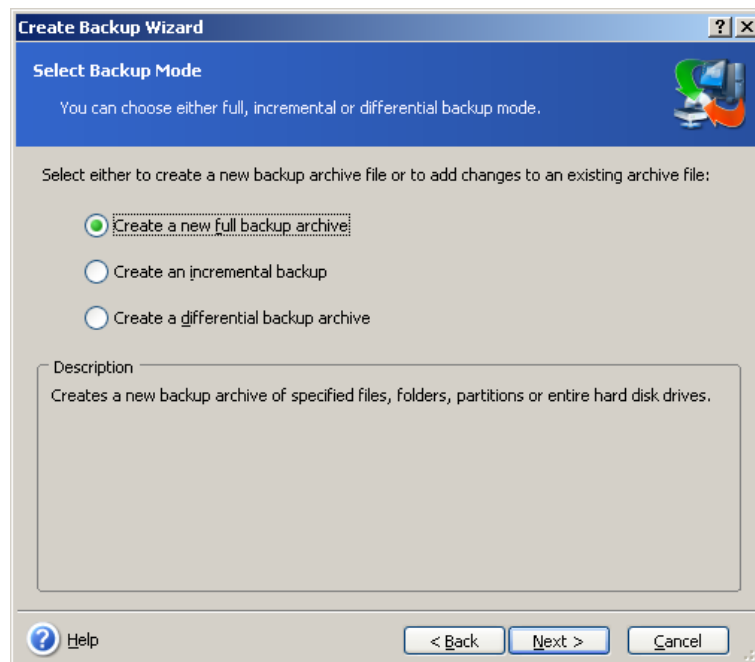
When backing up to Acronis Secure Zone, you have an option of dual destination backup. If enabled, the program will automatically place a copy of your backup archives on a local drive or network share as well as Acronis Secure Zone. See details in *6.3.12 Dual destination backup*.

Dynamic volumes are fully supported as a backup destination place. Acronis True Image Echo Workstation can access backup archives, created on dynamic volumes, in standalone (rescue) mode as well as under Windows control.



See notes and recommendations for using the FTP server in *1.4.2 Supported storage media*.

6. If your choice was not Acronis Backup Server, 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*).



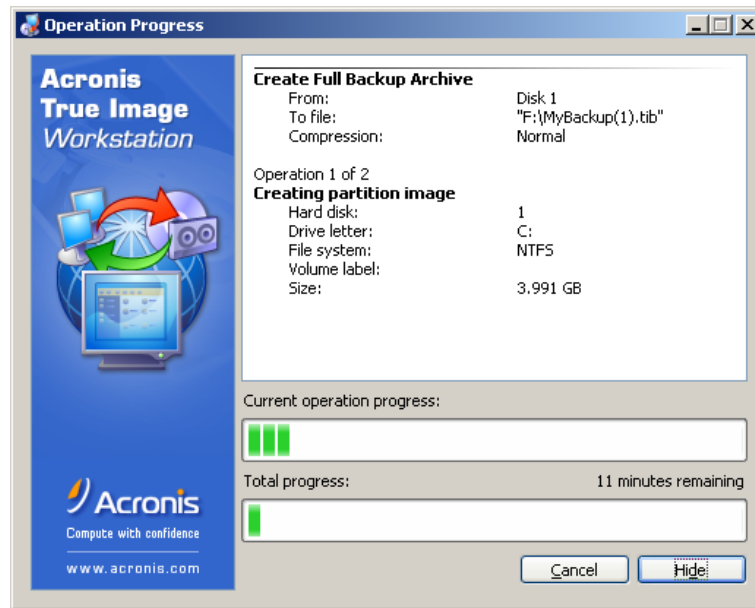
7. Select the backup options (that is, backup file splitting, compression level, password protection, pre/post backup commands etc.). You may select **Use default options** or **Set the options manually**. If the latter is the case, the settings will be applied only to the current backup task. Alternatively,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

8. 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.

9. 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.

10. (For Acronis True Image Echo Workstation local version only) The task progress will be shown in a special window. You can stop the procedure by clicking **Cancel**.

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



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 menu that appears. For information on how to set the default priority, see *6.3.6 Backup performance*.

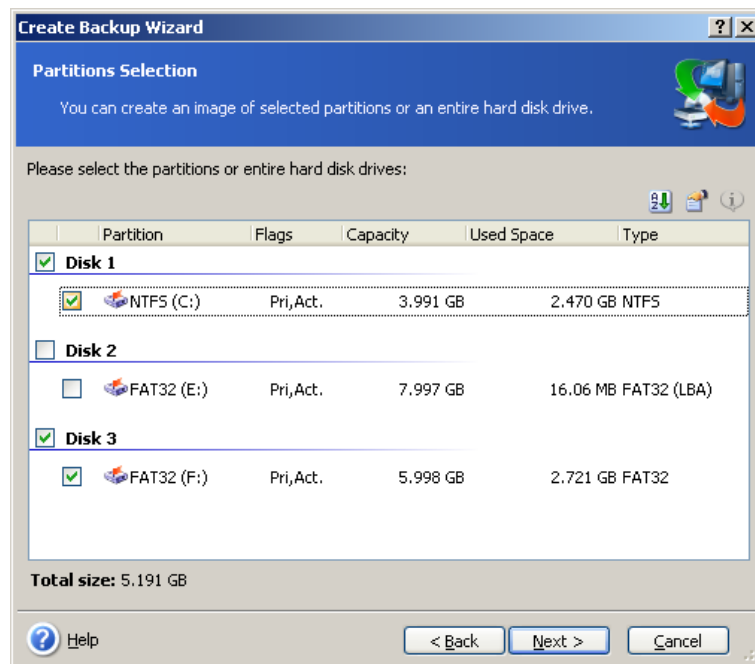
11. You may want to see the log when the task is completed. To view the log, click the **Show Operation Logs** button on the toolbar.



If you burn an archive to multiple 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. Start the **Create Backup Wizard** by clicking on the backup operation icon in the main program window.
2. Select **My Computer**.
3. Select disks, partitions or dynamic volumes to back up. You can select a random set of disks, partitions and dynamic volumes.



4. Select the name and location of the archive.

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 full backup, it will be overwritten.

Including [date] in the backup file name will add to the name the time and date of the backup creation formatted as <DD-Month-YYYY HH:MM:SS>. Example: C:\MyBackup[date].tib.

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 with the basic full backup, 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 the existing differential backups. Either way, the program will create a new differential backup.

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*) or Acronis Backup Server (see details in 3.5 *Acronis Backup Server*) for storing backups. In those cases, you need not provide the file name.

When backing up to Acronis Secure Zone, you have an option of dual destination backup. If enabled, the program will automatically place a copy of your backup archives on a local drive or network share. See details in 6.3.12 *Dual destination backup*.

Dynamic volumes are fully supported as a backup destination place. Acronis True Image Echo Workstation can access backup archives, created on dynamic volumes, in standalone (rescue) mode as well as under Windows control.



See notes and recommendations for using the FTP server in *1.4.2 Supported storage media*.

5. If your choice was not Acronis Backup Server, 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*).

6. 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 the defaults. See *6.3 Setting backup options* for more information.

7. Provide a comment for the archive. This can help prevent you from restoring the wrong disk or partition. However, you also 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.

8. 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.

9. (For Acronis True Image Echo Workstation local version only) The task progress will be shown in a special window. You can stop the procedure by clicking **Cancel**.

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



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 menu that appears. For information on how to set the default priority, see *6.3.6 Backup performance*.

10. 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.



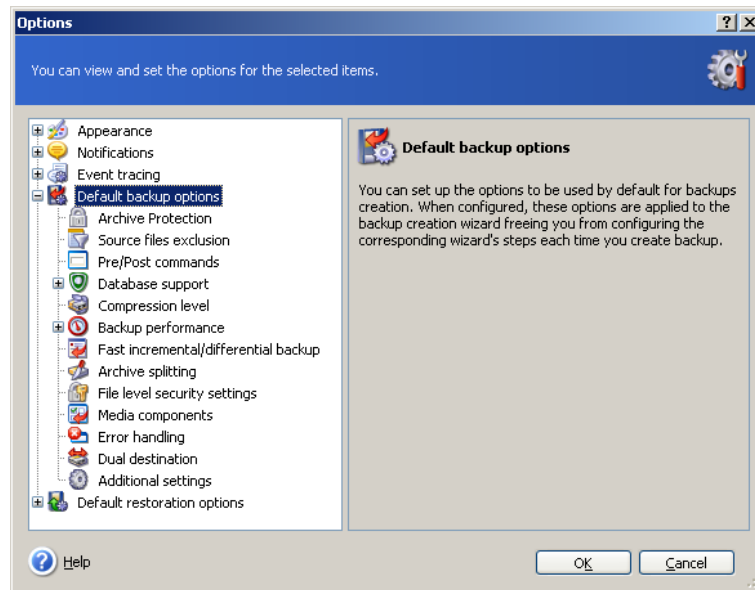
If you burn an archive to multiple removable media, be sure to number them, since you will have to insert them in order during the restoration.

6.3 Setting backup options

To view or edit the default backup options in Acronis True Image Echo Workstation 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

Password

The preset is **no password**.

An archive can be protected with a password. To protect the archive data from being accessed 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 Echo Workstation will ask for the password in a special window, allowing access only to authorized users.

Passwords cannot be set for archives created in the Acronis Secure Zone. To protect such archives, set a password for the zone itself.

Encryption

The preset is **128 bit**.

Once the password has been set, you can choose to encrypt the backup for advanced security with industry-standard AES cryptographic algorithm. The password is used to generate a key which may differ in length. There are 4 choices: no encryption, 128, 192 and 256-bit encryption. The more the key size, the longer time to cipher and the greater is your data security.

6.3.2 Source files exclusion

By default, **all files from the selected folders will be included in the archive**.

You can set default filters for the specific types of files you do not wish to back up. 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**. **My???.exe** will exclude 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.

The program does not support interactive commands, i.e. commands that require user input (for example, "pause".)

The backup process will run concurrently with your commands if you uncheck the **Do not perform operations until the commands execution is complete** box, which is checked by default.

6.3.4 Database support

Database servers, such as MS SQL Server and MS Exchange, can be problematic to backup, partially due to open files and indexes and partially due to rapid data changes. Therefore it is usually recommended that the database be suspended just before the backup (data capture). You can suspend the database and clear all caches to ensure that all transactions are completed at the moment of data capture. If it become necessary to restore a damaged database, it will be restored completely and be ready to access after recovery.

1. Before/after data capture commands

The transactions completion can be ensured by 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 msxchangesa /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 the *data capture* process, which takes seconds, while

the entire backup procedure may take much longer, depending on the amount of data to be imaged. Therefore, the database idle time will be minimal.

Before/after data capture commands can also be used for other purposes. You may want to suspend an application other than a database, for example.

The backup process will run concurrently with your commands if you uncheck the **Do not perform operations until the commands execution is complete** box, which is checked by default.

2. Multi-volume snapshot

The preset is **disabled**.

Enable the **Multi-volume snapshot** feature if you are going to back up data located on multiple volumes and you must preserve its consistency (such as a database spanned across the volumes). In this case, a single snapshot for all volumes is created, which will be used for backup creation. When disabled, snapshots for volumes will be taken one by one.

6.3.5 Compression level

The preset is **Normal**.

The data will be copied without any compression, which may significantly increase the backup file size, if you select **None** as the compression level. 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, such as .jpg, .pdf or .mp3. However, formats such as .doc or .xls will compress more than other file types.

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 preset is **Low**.

The priority of any process running in a system determines the amount of CPU usage and system resources allocated to that process. Decreasing the backup priority will free more resources for other CPU tasks. Increasing the backup priority 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

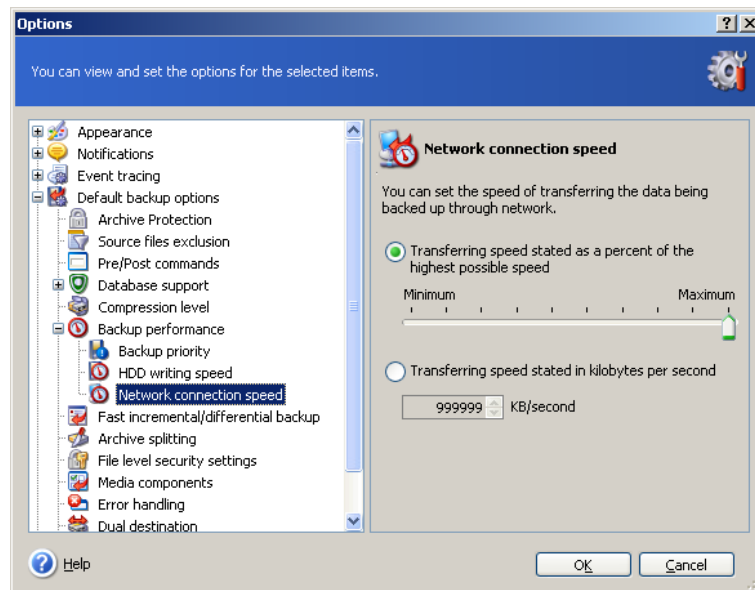
The preset is **Maximum**.

Backing up in the background to an internal hard disk (for example, to the Acronis Secure Zone) may slow other programs' performance because of the large amounts of data transferred to the disk. You can limit the hard disk usage by Acronis True Image Echo

Workstation to the desired level. To set the desired HDD writing speed for data being backed up, drag the slider or enter the writing speed in kilobytes per second.

3. Network connection speed

The preset is **Maximum**.



If you frequently backup data to network drives, think of limiting the network usage used by Acronis True Image Echo Workstation. To set the desired data transfer speed, drag the slider or enter the bandwidth limit for transferring backup data in kilobytes per second. This setting is also applied to an FTP connection, if an FTP server is selected as backup destination device.

6.3.7 Fast incremental/differential backup

The preset is **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 Echo Workstation 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 an FTP server (data recovery directly from an FTP server requires the archive to be split into files no more than 2GB in size).

The preset is **Automatic**. With this setting, Acronis True Image Echo Workstation will act as follows:

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

The program will automatically split the backup into several files if the storage disk has enough space, but its file system does not allow the estimated file size.



FAT16 and FAT32 file systems have a 4GB file size limit. However, the existing hard drive's capacity can reach as much as 2TB. 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 backup 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 Echo Workstation 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 a backup directly on CD-R/RW or DVD±R/RW generally will 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 the user account, specified in the permissions, you may not be able to read or modify this file.

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

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 - the files will inherit the permissions from the parent folder.

In archives, store encrypted files in decrypted state

The preset is **disabled**.

Simply ignore this option if you do not use the encryption feature available in Windows XP. (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 preset is **disabled**.

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

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

The **Acronis One-Click Restore** is a minimal addition to the image archive, stored on removable media, allowing one-click disk recovery from this archive. This means that at boot from the media and clicking “restore” all the data contained in the image will be silently restored.



Because the one-click approach does not presume user selections, such as selecting partitions to restore, Acronis One-Click Restore always restores the entire disk. Therefore, if your disk consists of several partitions and you are planning to use Acronis One-Click Restore, all the partitions must be included in the image. Any partitions missing from the image will be lost.

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

The **Advanced** tab lets you select full, safe or both Acronis True Image Echo Workstation loader versions. The safe version does not have USB, PC card or SCSI drivers and is useful only in cases where 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.

6.3.11 Error handling

1. Ignore bad sectors

The preset is **disabled**.

With the default setting, the program will display a pop-up window each time it comes across a bad sector and ask for user decision whether to continue or stop the backup procedure. In order to back up the valid information on a rapidly dying disk, enable ignoring bad sectors. The rest of the data will be backed up and you will be able to mount the image and extract valid files to another disk.

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

The preset is **disabled**.

Corporate administrators need an option to continue a back up despite any errors that might occur without the system popping up an error box. Details of the operation, including errors, if any, could be found in the operation log.

With the silent mode enabled, the program will not display interactive windows. Instead, it will automatically handle situations requiring user intervention such as running out disk space (except for handling bad sectors, which is defined as a separate option.) No prompts will be displayed, including those for removable media or overwriting data on a tape. If an operation cannot continue without user action, it will fail.

Therefore, enable this feature if you do not want unattended backup operations hang on pop-ups and errors.

3. If an error occurs, re-attempt in (minutes)

The preset is **enabled**.

When the backup destination location on the network is not available or not reachable, the program will attempt to reach the location at the specified time interval.

6.3.12 Dual destination backup

The preset is **disabled**.

If enabled, the program will automatically place a copy of each backup being created locally to a separate location on a local drive or network share. The consistency of the additional archive copy is maintained automatically. After a backup is saved to the main location, the program compares the updated archive contents to the copy contents, and if some backups are missing from the copy, they will be copied to the external location along with the new backup.

In addition to enhancing the archive security provided with replication, this feature allows traveling users to keep a consistent copy of the laptop data both on the laptop and the corporate server. When the remote destination for the creation of the archive copy is not available, e.g. due to the network absence, the program will back up data to the local destination alone. When connected again, all changes made to the archive will be transferred to the copy during the first backup operation.

The feature provides quick desktop backup to the internal drive as an intermediate step before saving the ready backup on the network. This comes in handy in cases of slow or busy networks and time-consuming backup procedures. Disconnection during the copy transfer will not affect the backup procedure as opposed to backing up directly to the remote location.



If saving a backup copy to ASZ please note: even when a password is set for the Acronis Secure Zone, the copy archive will not be protected with the password.

6.3.13 Wake On LAN

This option is available only for tasks created by the Acronis Group Server.

The preset is **Enable Wake On LAN**.

With this setting, Acronis Group Server will send a magic packet to the remote computer network interface card (NIC) before starting backup. (A magic packet is a packet that contains 16 contiguous copies of the receiving NIC's Ethernet address.) This will power on the computer for running the backup task. Once the backup procedure is over, the computer can go to sleep if it times out.

Before using the feature, make sure that Wake On LAN is enabled both on the computers that you intend to back up and the Acronis Group Server.

To enable the Wake On LAN feature on a computer to be backed up:

1. Enter the computer BIOS and set Power -> Wake On PCI PME -> Power On.
2. Set the NIC properties on the computer as follows.

Control Panel -> System -> Device Manager -> Network adapters -> select the NIC -> Properties -> Advanced:

Enable PME -> Enabled

Wake On Link Settings -> OS Controlled

Wake On Settings -> Wake On Magic Packet.

3. Find out the computer MAC address (Local Area Connection -> Status -> Support -> Details -> Physical Address.)

4. Repeat steps 1-3 for all computers you wish to wake on LAN.

To enable the Wake On LAN option on the Acronis Group Server:

1. Find the computer to be backed up in the list of computers.

2. Select the computer and enter its MAC address in the Acronis Group Server (sidebar -> Computer details -> MAC address: Set -> type the hex MAC address as XXXXXXXXXXXX or XX-XX-XX-XX-XX -> click OK). The program will test the MAC address for validity and display the test result.

3. Repeat steps 1-2 for all computers you wish to wake on LAN.

4. Schedule a group backup task for the above computers. When setting the backup options, ensure that the **Wake On LAN** option is enabled. Any computer that is asleep as the task starts will be powered on for running the task.

6.3.14 Additional settings

1. Validate backup archive upon operation completion

The preset is **disabled**.

The program will check integrity of the just created or supplemented archive immediately after backup when enabled.



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

2. Overwrite data on a tape without user confirmation

The preset is **enabled**.

When pulling a tape from the Imported media pool, Acronis True Image Echo Workstation 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 preset is **enabled**.

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

4. Reset archive bit

The preset is **disabled**. The option relates only to file-level backup.

In Windows operating systems, each file has an attribute **File is ready for archiving**, available at selecting file -> **Properties** -> **General** -> **Advanced** -> **Archive and Index attributes**. This attribute, also known as archive bit, is set by the operating system each time the file is changed and can be reset by backup applications each time they include the file in a backup copy. Archive bit value is used by various applications such as databases.

With **Reset archive bit** enabled, Acronis True Image Echo Workstation will reset archive bits of all files being backed up. Acronis True Image Echo Workstation itself does not use the archive bit value. When performing incremental or differential backup, it determines whether a file has changed by the file size and the date/time when the file was last saved.

Chapter 7. Restoring the backup data

7.1 Considerations before recovery

7.1.1 Restore under Windows or boot from CD?

As mentioned above (see *2.5.1 Running Acronis True Image Echo Workstation (local version)*), Acronis True Image Echo Workstation can be run in several ways. We recommend that you first try to restore data running Acronis True Image Echo Workstation 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 Echo Workstation 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 Echo Workstation might sometimes differ from the way Windows identifies drives. For example, the D: drive identified in the standalone Acronis True Image Echo Workstation might correspond to the E: drive in Windows.

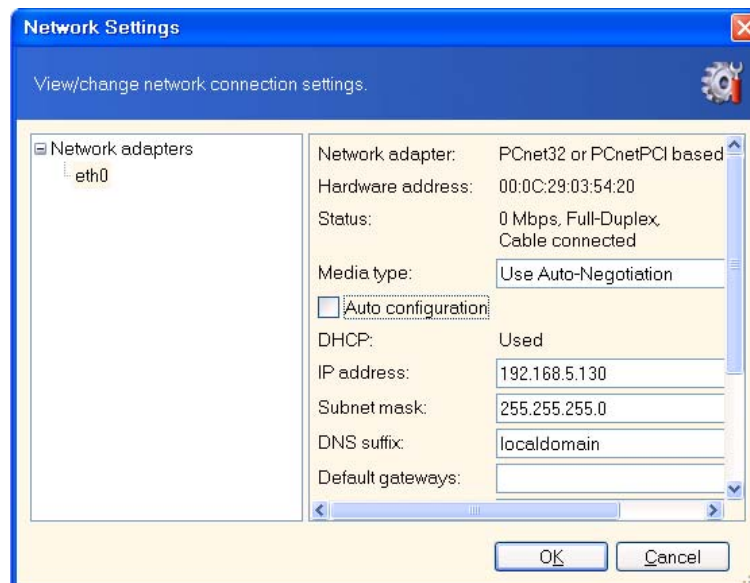


If a backup image is located on bootable media, you might have a choice of using Acronis One-Click Restore. This operation always restores the entire physical disk. Therefore, if your disk consists of several partitions, the partitions that are missing from the image will be lost. Please make sure that the image contains all disk partitions or you do not need the partitions that are not imaged before using Acronis One-Click Restore. For more information on Acronis One-Click Restore, see *6.3.10 Media components*.

7.1.2 Network settings in rescue mode

When booted from removable media, RIS server or by Startup Recovery Manager, Acronis True Image Echo Workstation may not detect the network. This can occur if there is no DHCP server in your network or if your computer address was not identified automatically for some reason.

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



7.1.3 Recovering dynamic volumes

Dynamic volumes are volumes located on dynamic disks, i.e. disks managed by Windows Logical Disk Manager (LDM). For more information on dynamic disks, please refer to your Windows documentation.

Acronis True Image Echo Workstation can back up and recover dynamic volumes.

A dynamic volume can be recovered over the same volume or unallocated space of a dynamic group. If recovered over another volume, the target volume's contents will be overwritten with the image contents, but the type or other properties of the target volume will not be changed.

To restore a dynamic volume exactly as it is, prepare a target dynamic group without volumes. In case you want to restore a dynamic volume in place of some volumes already existing on the target disks, delete the original volumes using third-party tools, such as the Windows Disk Management tool.

Dynamic volume contents alone can be recovered onto a basic or dynamic volume without changing the target volume type. Acronis True Image Echo Workstation local version has the **Create dynamic volume** tool so that you be able to prepare the desired volumes on the target disk.

Backward conversion of dynamic volume to basic disks can be performed, if need be, using the **Add new disk** operation (see *Chapter 15. Adding a new hard disk*).

With these tools, anywhere-to-anywhere data recovery becomes available, in terms of basic disks and dynamic volumes of any type (simple, spanned, striped, mirrored or RAID 5). The tools are available in bootable program version. Having booted the Acronis environment, you can easily prepare the desired dynamic group on bare metal or a computer with non-Windows operating system.

For how to use the above tools see *7.5 Creating dynamic disks and volumes*.

7.2 Restoring files and folders from file archives

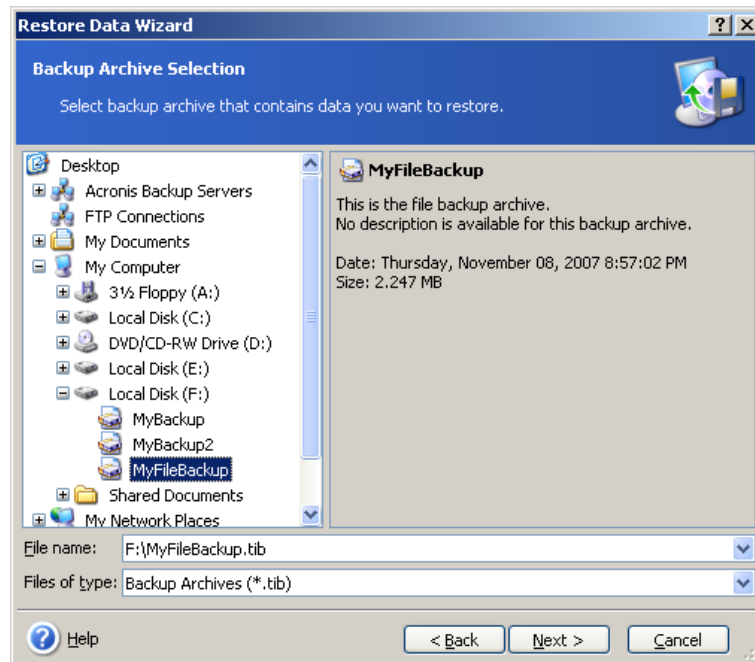
Here we describe how to restore files/folders from a file backup archive. You can restore the desired files/folders from a disk/partition image as well. To do so, mount the image

(see 11.2.2 *Mounting an image*) or start the image restoration and select **Restore specified files or folders** (see 7.3 *Restoring disks/partitions or files from images*).



To restore files and folders from an XFS, JFS, or ReiserFS image, mount it under Linux and copy the necessary files and folders.

1. Start the **Restore Data Wizard** by clicking on the restore operation icon in the main program window.
2. 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 an FTP server requires the archive to consist of files no more than 2GB in size. If you suspect 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. See notes and recommendations for supporting FTP server in 1.4.2 *Supported storage media*.

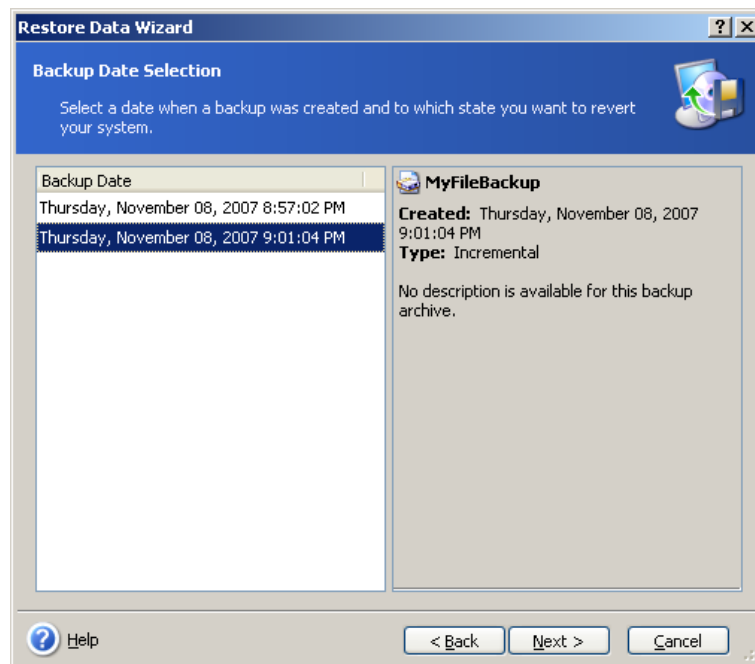
If you added a comment to the archive, it will be displayed to the right of the drives tree. If the archive was protected with a password, Acronis True Image Echo Workstation will ask for it. The comment and the **Next** button will be unavailable until you enter the correct password.

3. If the selected archive contains incremental backups, Acronis True Image Echo Workstation will suggest that you select one of successive incremental backups by its creation date/time. Thus, you can return the files/folders to a specific time and date.



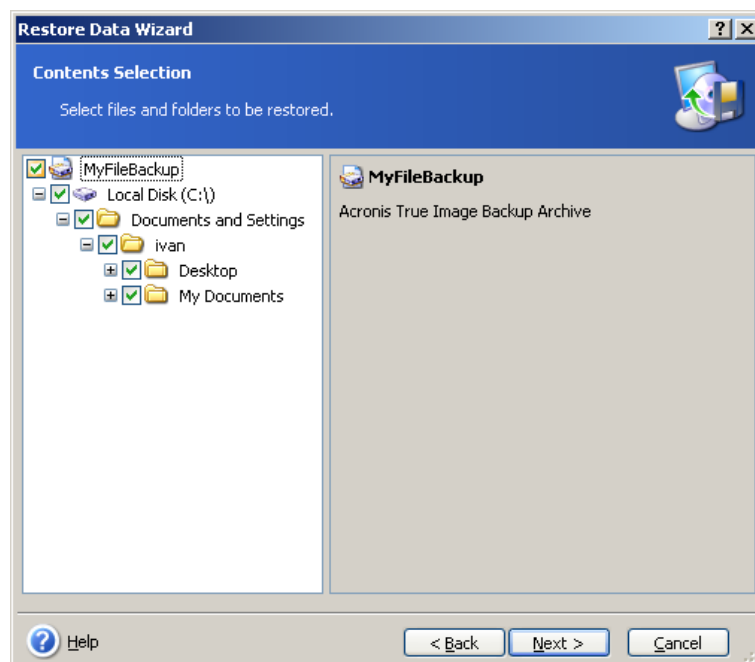
To restore data from an incremental backup, you must have all previous incremental backups and the initial full backup. If any of successive backups is missing, restoration is not possible.

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



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

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



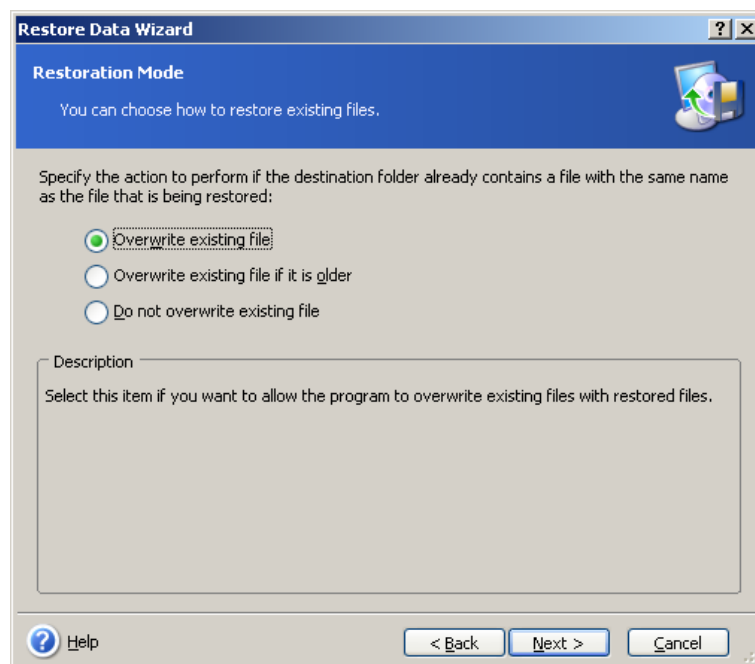
6. Select the options for the restoration process (that is, pre/post restoration commands, restoration process priority, file-level security settings etc.). You may **Use default options** or **Set the options manually**. If you set options manually, the settings will be applied only to the current restore 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.

7. Set filters for the specific types of files that are not to be restored. 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**. **My???.exe** 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 *7.4.1 Files to exclude from restoration*.

8. 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 be 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.

9. 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.

10. (For Acronis True Image Echo Workstation local or bootable version) The task progress will be shown in a special window. You can stop the procedure by clicking **Cancel**. Please keep in mind that the aborted procedure 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 Echo Workstation 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

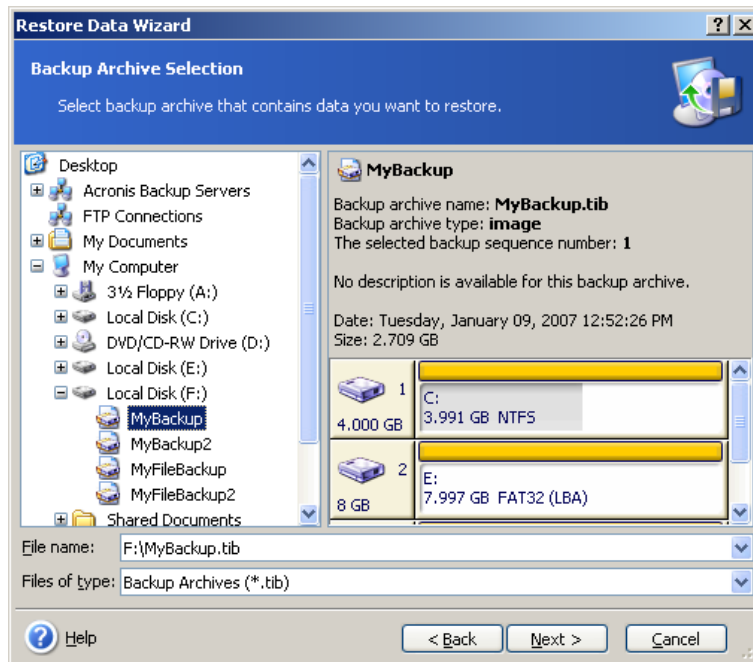
not be blocked, close applications that use this partition (disk) and start over. If you can not determine which applications use the partition (disk), close them all.

7.3.1 Starting the Restore Data Wizard

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

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 an FTP server requires the archive to be split into files no more than 2GB in size. If you suspect 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. See notes and recommendations for supporting FTP server in *1.4.2 Supported storage media*.

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 Echo Workstation will ask for it. The partitions layout, the comment and the **Next** button will be unavailable until you enter the correct password.

2. If the selected archive contains incremental backups, Acronis True Image Echo Workstation will suggest that you select one of successive incremental backups by its creation date/time. Thus, you can return the disk data to a certain moment.

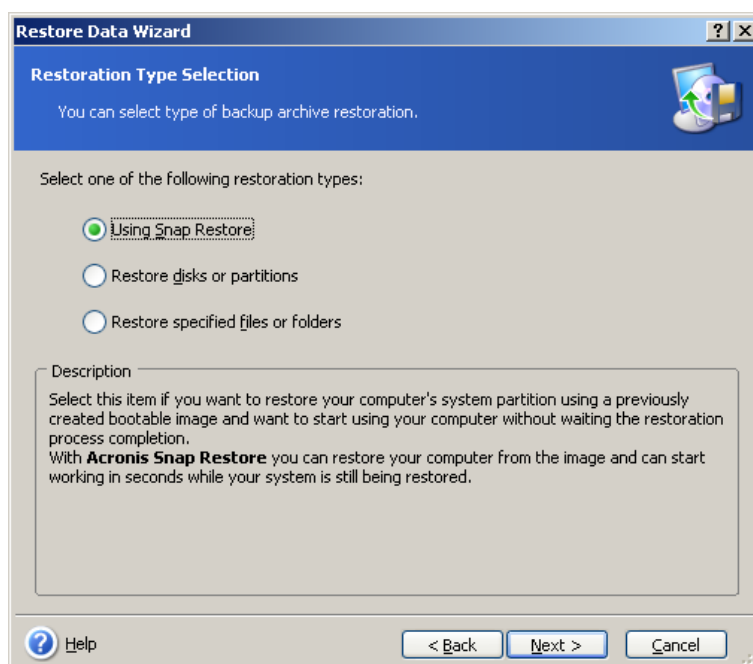


To restore data from an incremental backup, you must have all previous incremental backups and the initial full backup. If any of successive backups is missing, restoration is not possible.

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

7.3.3 Restoration type selection

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 want to restore files instead of disk/partition, uncheck the unnecessary folders. Otherwise you will restore a lot of extra 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 Active Restore

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



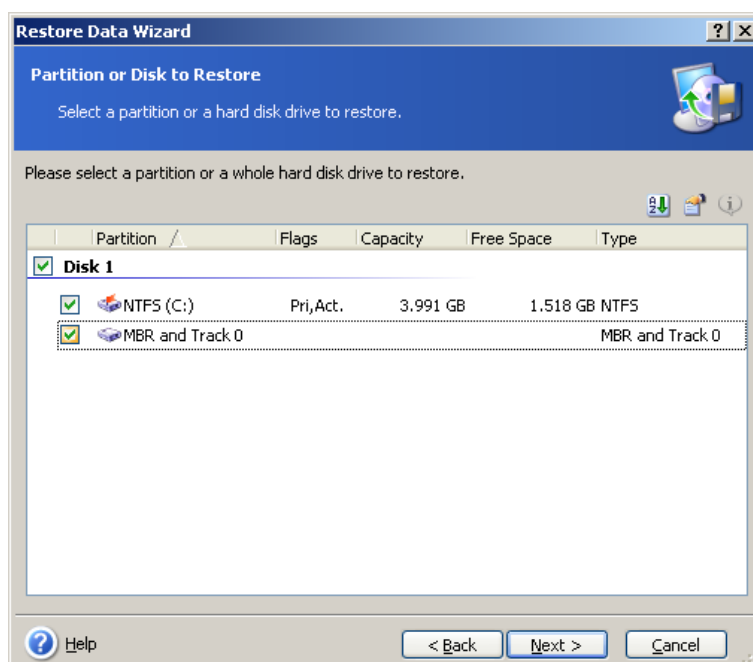
When performing Active Restore, the Acronis True Image Echo Workstation always restores the entire system disk. Therefore, if your disk consists of several partitions, the partitions which are missing from the image will be lost. Please make sure that the image contains all disk partitions or you do not need the partitions that are not imaged before using Acronis Active Restore.

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 not be possible when using Acronis Active Restore.

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

7.3.4 Selecting a disk/partition to restore

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



Disks and partitions images contain a copy of track 0 along with the MBR (Master Boot Record). It appears in this window in a separate line. You can choose whether to restore MBR and track 0 by checking the respective box. Restore the MBR if it is critical to your system boot.

7.3.5 Selecting a target disk/partition

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



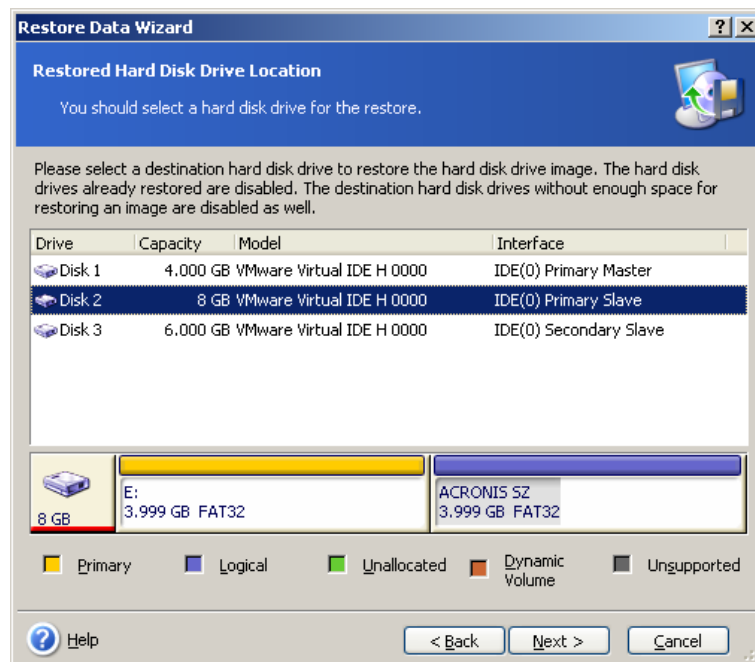
All the data stored on the target partition will be replaced by the image data, so be careful and watch for non-backed-up data that you might need.

When restoring a Windows system disk and select a target disk, the program compares critical for the system start devices, found in the image registry and the target computer registry.

If the chipset, motherboard or mass storage device are different, there is a risk that the system will not be able to boot. Then you will be prompted whether you want to buy **Acronis Universal Restore**. To find out more about this option, see [3.7 Acronis Universal Restore](#). To buy the option, follow the link.

If you already have Acronis Universal Restore, the prompt will not come up and you will have an option to enable Acronis Universal Restore later in the Restore Data Wizard.

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



If there are partitions on the target disk, you will be prompted by the **Nonempty Destination Hard Disk Drive** window stating that the destination disk contains partitions, perhaps with data.

You will have to select between:

- **Yes, I want to delete all the partitions on the destination hard disk before restoring** – all existing partitions will be deleted and all their data will be lost.
- **No, I do not want to delete partitions** – no existing partition will be deleted, discontinuing the recovery operation. You will be able to cancel the operation or return to select another disk.



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

To continue, select the first choice and click **Next**. You will be taken directly to step *7.3.10 Restoring several disks or partitions at once*.

7.3.6 Changing the restored partition type

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

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

If you are restoring a system partition to the new (or the same) disk and want to load 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 likely you will need only the data. In this case, you can restore the partition as **Logical** to access the data only.

By default, the original partition type is selected.



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

7.3.7 Changing the restored partition file system

You can change the partition file system during its restoration, although it is seldom required. Acronis True Image Echo Workstation can make the following file system conversions: **FAT 16 -> FAT 32** and **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 4GB, so you will not be able to restore a 4GB 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.

7.3.8 Changing the restored partition size and location

You can resize and relocate a partition by dragging it or its borders with a mouse or by entering corresponding values in 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.

7.3.9 Assigning a letter to the restored partition

Acronis True Image Echo Workstation 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.

7.3.10 Restoring several disks or partitions at once

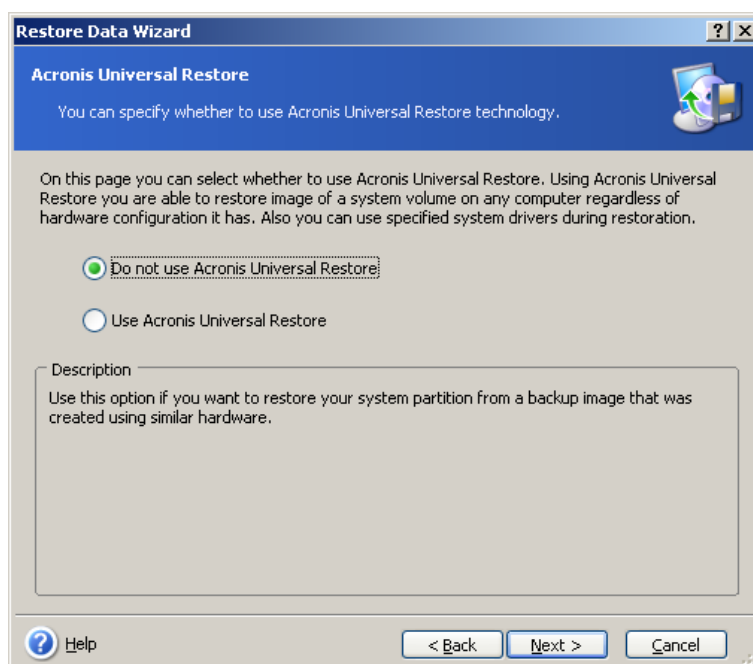
During a single session, you can restore several partitions or disks, one by one, by selecting one disk and setting its parameters first and then repeating these actions for every partition or disk to be restored.

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, do not set this switch.

7.3.11 Using Acronis Universal Restore

Acronis Universal Restore is an add-on to Acronis True Image Echo Workstation. It is purchased separately and installed from a separate setup file. The following is true for Acronis True Image Echo Workstation installations including Acronis Universal Restore.

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



2. If the target hardware has a specific mass storage controller (such as a SCSI, RAID, or Fibre Channel adapter) for the hard disk, you can install the appropriate driver manually, bypassing the automatic driver search-and-install procedure.

Use this option only if the automatic search-and-install procedure was unsuccessful.

Acronis Universal Restore uses three sources for drivers:

-
- the driver repository - a folder or folders on a network drive or CD specified in restore options. If you have not specified the driver repository in advance, you can do it at next step.
 - the mass storage device driver specified by the user at the current step
 - the Windows default driver storage folders (in the image being restored).

The program will find the most suitable drivers of all available drivers and install them into the restored system. However, the driver defined by the user, will have the priority. It will be installed, with appropriate warnings, even if the program finds the better driver.



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 **Specifying Mass Storage Drivers** window. Use drivers bundled with your virtual machine software or download the latest drivers versions from the software manufacturer website.

7.3.12 Setting restore options

Select the options for the restoration process (that is, pre/post restoration commands, restoration process priority etc.). You may **Use default options** or **Set the options manually**. If you set the options manually, 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.

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 Echo Workstation local or standalone version) The task progress will be shown in a special window.

You can stop the procedure by clicking **Cancel**. However, it is critical to note that the target partition will be deleted and its space unallocated – the same result you will get if the restoration is unsuccessful. To recover the “lost” partition, you will have to restore it from the image again.

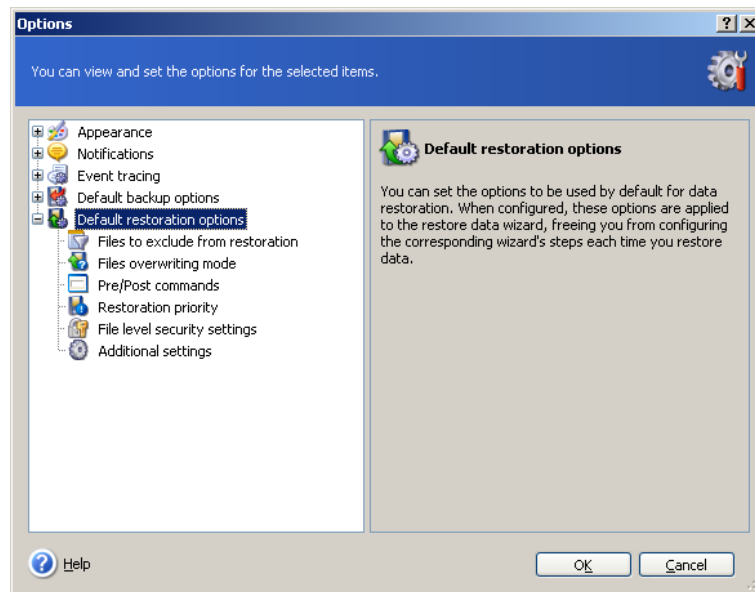
If Acronis Universal Restore finds no Hardware Abstraction Layer (HAL) or mass storage devices drivers compatible with the new hardware in all available sources, you will be prompted to browse to a network share drive or insert a floppy disk or CD with the necessary drivers. Upon starting Windows, it will initialize the standard 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 Echo Workstation local version, select **Tools -> Options -> Default Restoration Options** from the main program menu.

To do the same remotely, connect the 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 exclude from restoration

The preset is **Restore all files**.

You can set the default filters for the specific types of files that are not to be restored. Use the common Windows masking rules. For example, to exclude all files with extension .exe, add ***.exe**. **My???.exe** will exclude 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 be 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.

The program does not support interactive commands, i.e. commands that require user input (for example, “pause”).)

The backup process will run concurrently with your commands if you uncheck the **Do not perform operations until the commands execution is complete** box, which is checked by default.

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 preset is **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.

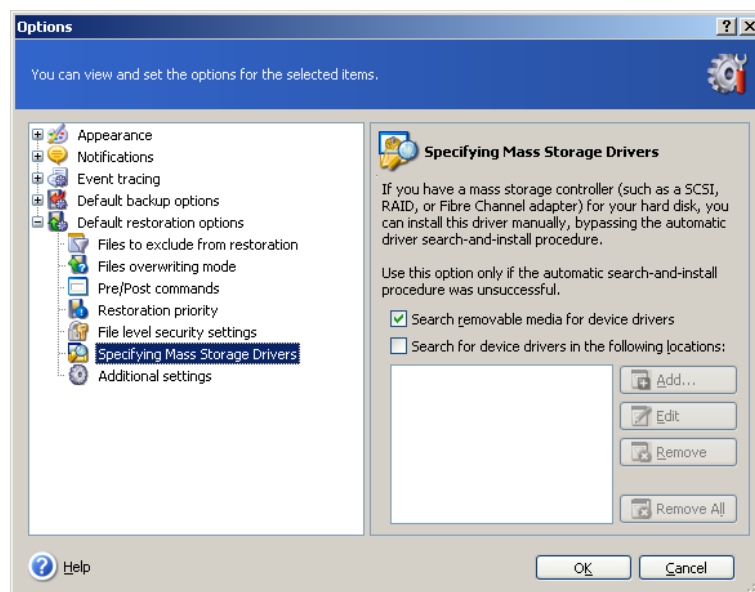
This option is effective only when restoring files from file/folders archives.

7.4.6 Specifying mass storage drivers

This option appears only in those computers’ options, where Acronis Universal Restore is installed.



Acronis Universal Restore is an option to Acronis True Image Echo Workstation. It should be purchased separately and installed from a separate setup file. For more information see 3.7 *Acronis Universal Restore*.



Here you can specify a path to the driver repository on a network drive or CD where Acronis Universal Restore will search for drivers at restoring a system disk on dissimilar hardware. If several paths are specified, the program will scan all locations and choose the most suitable driver.

7.4.7 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 Echo Workstation can check its integrity. If you suspect that the archive might have been corrupted, select **Validate backup archive before restoration**.



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

3. Having restored a disk/partition from an image, Acronis True Image Echo Workstation can check the integrity of the 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.

4. Restore file and folders without full path

The preset is **disabled**.

When enabled, files and folders are restored directly to the folder that you specified as a target folder. When disabled, the full path to the files and folders that exists in the backup will be reproduced within the target folder.

5. Change SID after restoration is finished

The preset is **disabled**.

Acronis True Image Echo Workstation can generate a unique security identifier (SID) for the restored system. You do not need a new SID when restoring a system on the same computer where the image was taken from or when creating a full duplicate that will replace the original system. Generate a new SID if the original and the restored systems will work concurrently in the same workgroup or domain.

6. The bootable Acronis True Image Echo Workstation version has also an option that after the restoration is finished, the computer reboots and starts the newly restored OS without any user interaction. If this option is set, post operation commands will not be executed. Include the reboot command in your batch file if you need these commands to be executed.

7.4.8 Error handling

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

The preset is **disabled**.

With the silent mode enabled, the program will not display interactive windows. Instead, it will automatically handle situations requiring user intervention. No prompts will be displayed, including those for inserting removable media or the next tape. If an operation cannot continue without user action, it will fail. Details of the operation, including errors, if any, could be found in the operation log.

2. If an error occurs, re-attempt in (minutes)

The preset is **enabled**.

When the backup location on the network is not available or not reachable, the program will attempt to reach the location at the specified time interval.

7.5 Creating dynamic disks and volumes

Acronis True Image Echo Workstation must obtain **exclusive access** to the disks to perform operations with disks and volumes. This means no other applications can access it at that time. Please close all other applications that use the disks (such as Windows Disk Management) before starting the disk conversion and dynamic volume creation wizards.

7.5.1 Creating dynamic volumes

This operation is available only in Acronis True Image Echo Workstation local version, including bootable version of this component. Having booted to the Acronis environment, you can easily prepare the desired dynamic group on bare metal or a computer with a non-Windows operating system.

The operation supports both dynamic disks and MBR or GPT basic disks. Basic disks will be converted to dynamic.



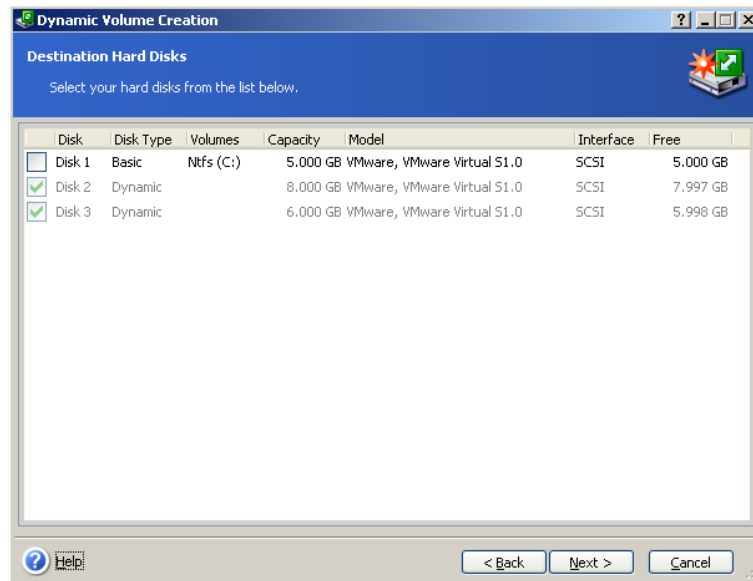
All data contained on the basic disk and the basic disk partitioning will be lost. On dynamic disks, only unallocated space will be used for the new volume.

An MBR basic disk must have at least 1MB of free space at the end of the disk for the dynamic disk database.

To create a dynamic volume:

1. Close all applications that use the disk(s) on which the volume is to be created.
2. Start the Dynamic Volume Creation Wizard by selecting **Tools -> Create Dynamic Volume** in the main program menu.
3. Select basic, dynamic or newly connected disks on which the dynamic volume will be created. Dynamic disks are selected by default. You can deselect any, if need be, later in the wizard.

If you tick off disks other than dynamic, these will be converted to dynamic disks and included in the dynamic group. However, this will be done when the operation starts. While you are using the wizard, no changes are made to disks.



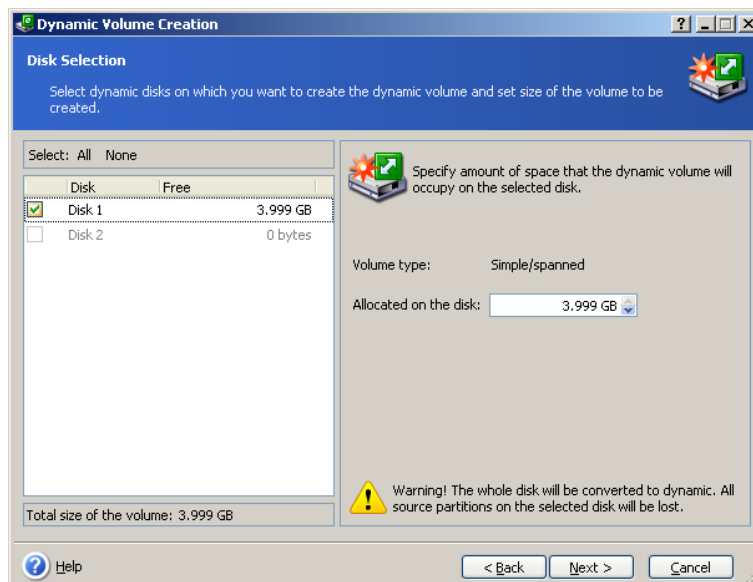
4. Select the type of dynamic volume that will be created: simple/spanned, striped, mirrored or RAID 5.

5. Specify amount of space that the dynamic volume will occupy on each of the selected disks. The value you set is adjusted to the selected volume type.

For a spanned volume, amount of space on each disk is selected independently. If only one disk is selected, a simple volume is created.

Striped, mirrored and RAID 5 volumes imply even distribution of data between disks. Therefore, the volume must occupy the same space on each disk. If you set different values, your latest setting will be applied to all the disks. If the set value is more than unallocated space on any disk, the minimal available space amount will be applied to all the disks. The resulting volume size is displayed under the disk selection field.

At this step, you can deselect disks that you do not want to be included in the volume.



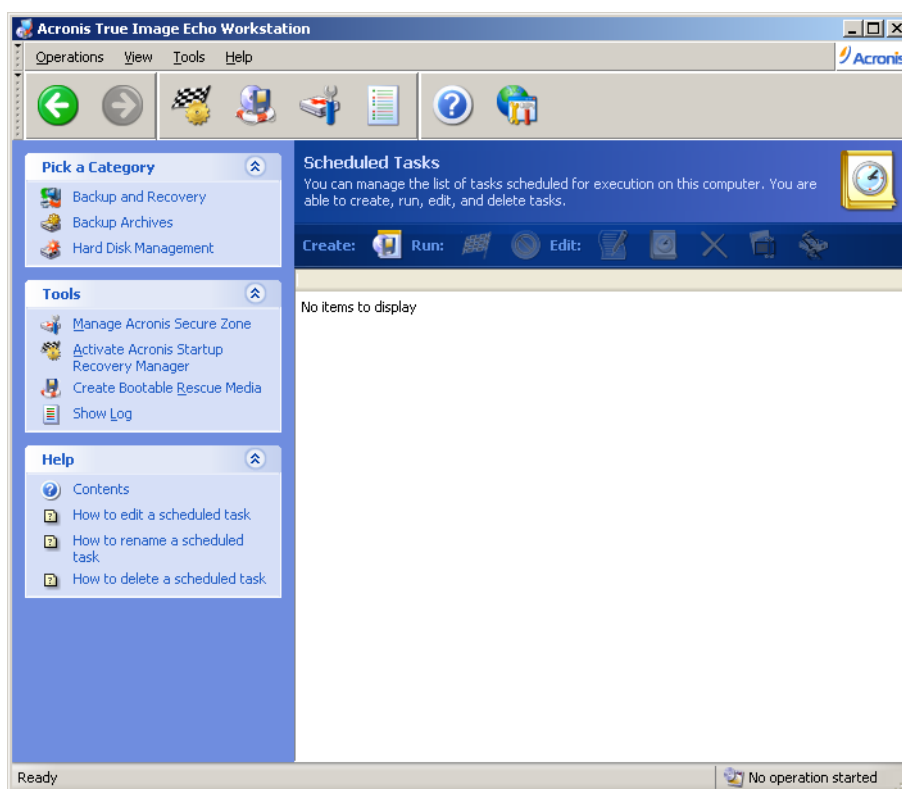
6. Click **Proceed** in the summary window.

On completion of operations, the dynamic volumes are unformatted and have no letters assigned. You will be able to assign the letters using Windows Disk Management tool after restoring Windows on the created volumes.

Chapter 8. Scheduling tasks

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

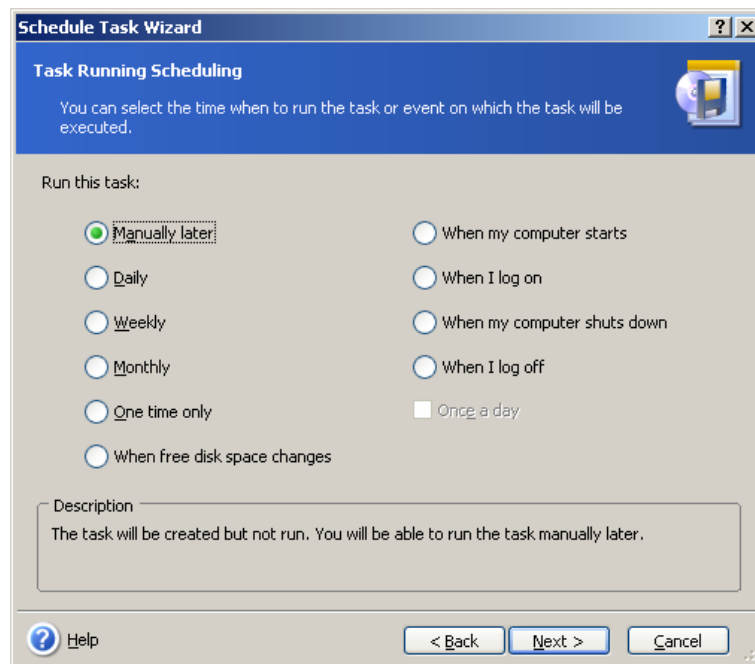
You can create more than one independently scheduled task. For example, you can back up your current project daily and back up the application disk once a week.



All the scheduled tasks appear in the **Scheduled Tasks** window, where you can start, stop, edit, delete and rename them. To navigate to the **Scheduled Tasks** window, click **Tasks** in the **Manage Tasks** group or select the **Task Scheduling** category on the sidebar.

8.1 Creating scheduled tasks

1. To start the **Schedule Task Wizard**, click **Create** on the **Scheduled Tasks** window toolbar or select **Operations -> Schedule Task** from the main menu.
2. Choose the **Backup** or **Validate** operation. If the latter is the case, choose the archive in the next window and you will be taken straight to step 4.
3. If backup is your choice, 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, enter a user name and a password for the drive access.
4. Set the task execution periodicity.



- **Manually later** – the task will be saved, but not launched automatically. You will be able to launch it later by clicking **Run** in the **Scheduled Tasks** window
- **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 the 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
- **Free disk space change** – the task will be executed when the free disk space changes by the specified amount
- **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 computer 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. Specify the task start time and other schedule parameters, according to the selected periodicity (see 8.1.1 - 8.1.5).

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

The screenshot shows the 'Schedule Task Wizard' window, specifically the 'User Information' step. The window has a blue header bar with the title 'Schedule Task Wizard' and a question mark icon. Below the header, the text 'User Information' is displayed, followed by the instruction 'Select the user name and password.' A small icon of a person is shown to the right. The main area contains a paragraph: 'Enter the name and password of a user. The task will run as if it was started by that user. Please note that the domain name must be specified if the user is a member of a domain.' Below this, there are three input fields: 'Enter the user name:' with the text 'administrator' entered; 'Enter the password:' with seven black dots; and 'Confirm password:' with seven black dots. At the bottom, there is a note: 'If a password is not entered, the scheduled tasks might not run.' The bottom of the window features a 'Help' button with a question mark icon, and three navigation buttons: '< Back', 'Next >', and 'Cancel'.

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

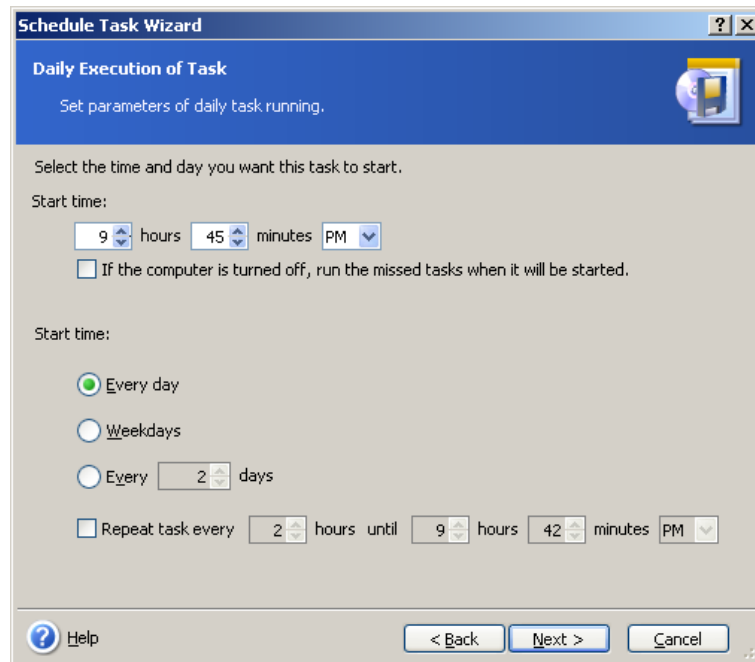
7. At the final step, the task configuration is displayed. Up to this point, you can click **Back** to make changes in the created task. If you click **Cancel**, all settings will be lost. Click **Finish** to save the task.

8. The task schedule and default name appear in the **Scheduled Tasks** window. You can rename the task, if need be.

8.1.1 Setting up daily execution

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

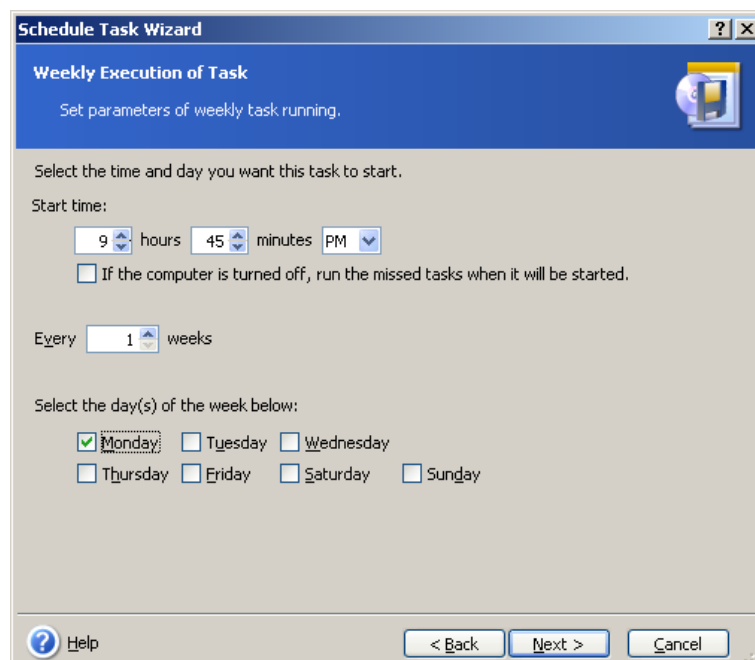
- **Every day**
- **Weekdays**
- **Every x days** – once in several days (specify the interval).
- **Repeat task every** – set this if the task must be performed several times a day.



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

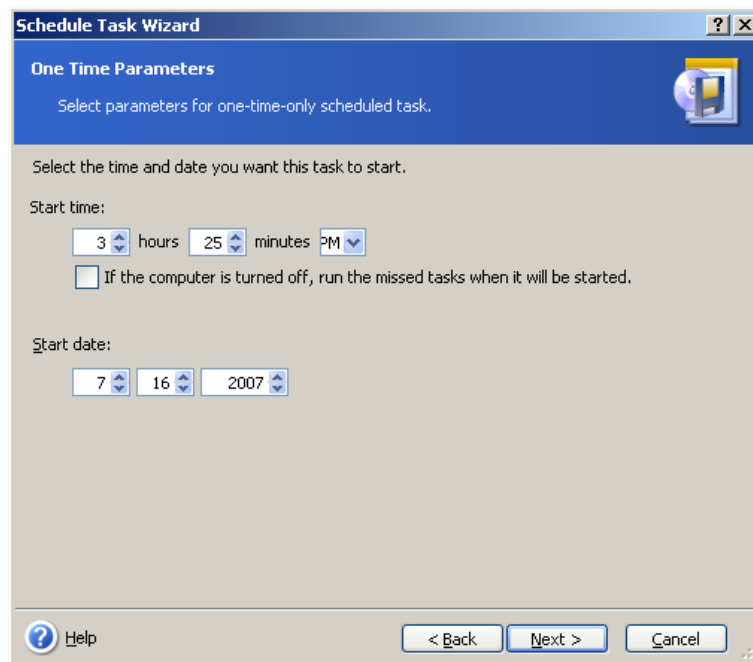
- **Day** – on the specified date
- **The <specify a day>** – on the specified day (e.g. on second Tuesday or fourth Friday); select this from the drop-down lists.

The screenshot shows the 'Schedule Task Wizard' dialog box, specifically the 'Monthly Execution of Task' step. The title bar reads 'Schedule Task Wizard'. The main heading is 'Monthly Execution of Task' with a subtext 'Set parameters of monthly task running.' Below this, it says 'Select the time and day you want this task to start.' There are two 'Start time:' labels. The first one is followed by a time picker showing '9' hours, '45' minutes, and 'PM'. Below this is a checkbox labeled 'If the computer is turned off, run the missed tasks when it will be started.' The second 'Start time:' label is followed by two radio buttons: 'Day' (unselected) and 'The' (selected). The 'The' radio button is followed by two drop-down menus: the first shows 'First' and the second shows 'Monday'. At the bottom, there are three buttons: 'Help' (with a question mark icon), '< Back', 'Next >', and 'Cancel'.

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

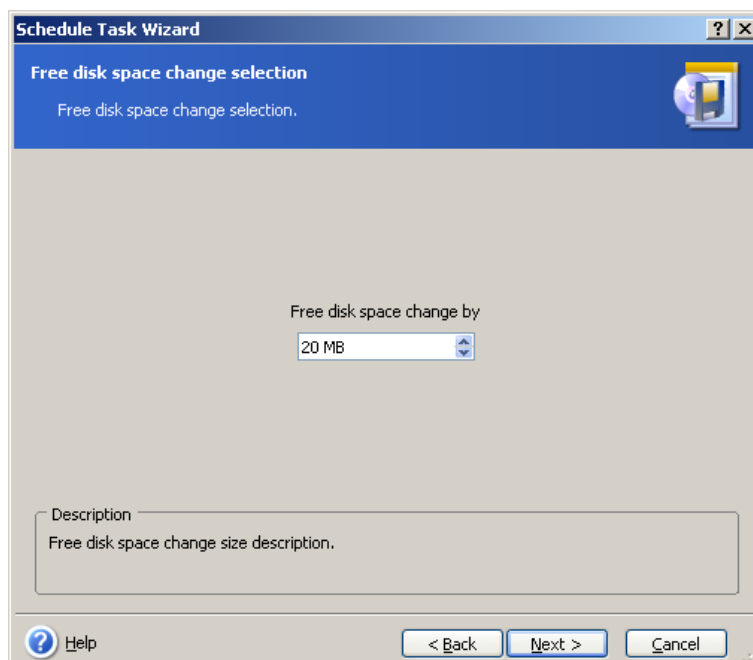
If you select the one-time execution, set the **Start time** and date on which to execute the task:



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.

8.1.5 Setting up event-driven execution

Execution on increasing or decreasing free space on a disk. The task will be started when the free space on the either disk selected for the backup changes by the specified value. The preset is 20MB.



8.2 Managing scheduled tasks

The task Status, Schedule, Last Run Time and Last Result are shown in the **Scheduled Tasks** 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** on the toolbar.

If you want to change only the task start trigger (time or event), click **Schedule** on the toolbar. Then you will have to perform only scheduling steps, leaving other settings the same.

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

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

In Acronis True Image Echo Workstation local version there is an option to duplicate a task so that you need program it only once. Select the task and click **Clone** on the toolbar. Pass through the same wizard as when editing a task and make changes if necessary. As opposed to editing, the result will be saved as a separate task. You will have the option to rename the clone for better identification.

Chapter 9. Managing the Acronis Secure Zone

The Acronis Secure Zone is a hidden partition for storing archives on the computer system itself. It is necessary for using Acronis Startup Recovery Manager. For more information about these functions, see *3.3 Acronis Secure Zone* and *3.4 Acronis Startup Recovery Manager*.

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 manage it (resize or change the password) or delete. If there is no zone, you'll be prompted to create it.

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

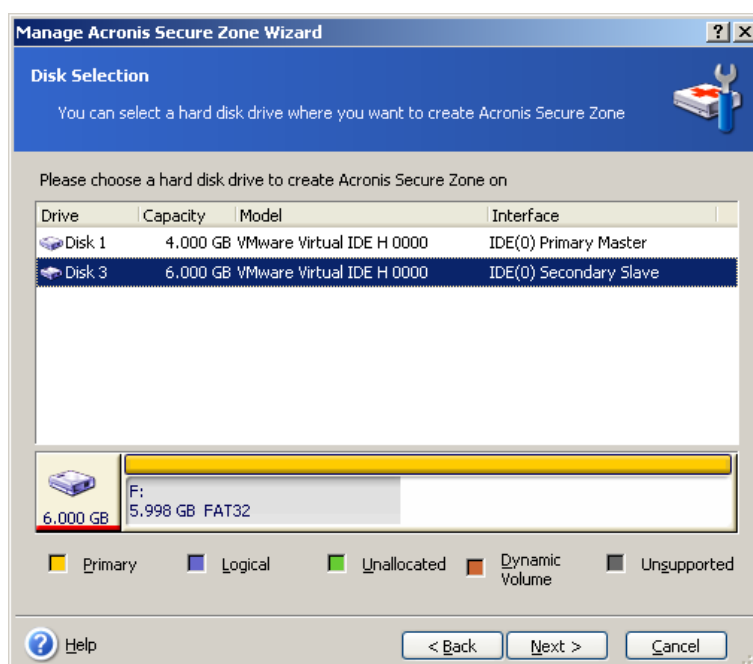
9.1 Creating Acronis Secure Zone

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

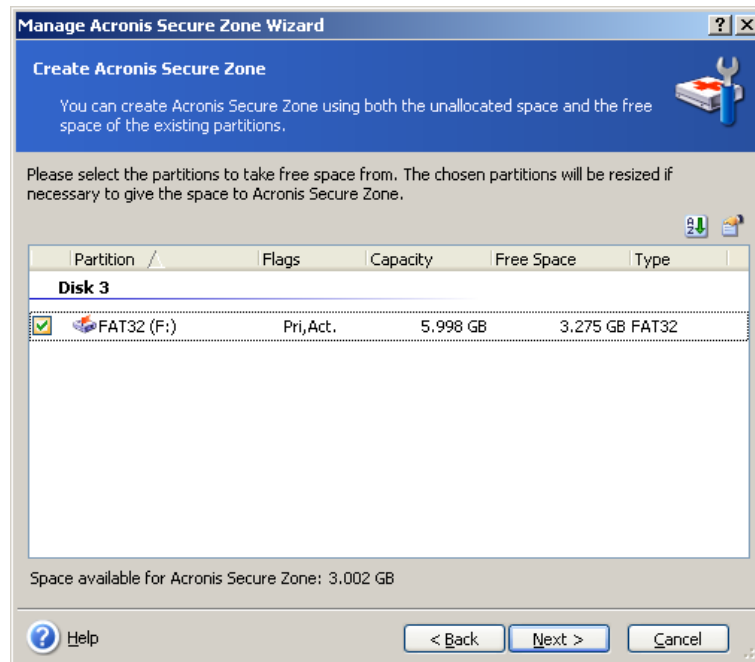
A computer can have only one Acronis Secure Zone. To create a zone on another disk, you must first delete an existing zone.

1. Before creating a zone, you may want to estimate its size. To do so, start a backup and select all data you are going to copy into it. At the **Set Backup Options** step, choose **Set the options manually**, then set the compression level. You will see the estimated full backup size (for disk/partition backup) or the approximate compression ratio (for file-level backup) with which you can calculate the estimated full backup size. Multiply this by about 1.5 to be able to create incremental or differential backups.

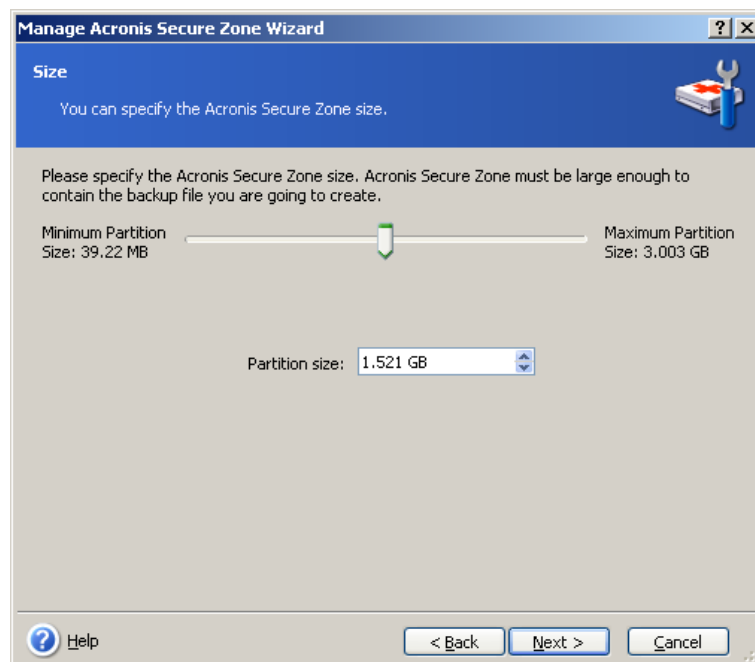
2. If there are several disks installed, select one on which to create Acronis Secure Zone.



3. Select the partitions from which space will be used to create the zone.



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



The minimum size is approximately 35MB, depending on the geometry of the hard disk. The maximum size is equal to the disk's unallocated space plus the total free space on all partitions selected at the previous step.

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



Please keep in mind that reducing a system partition to the minimum size might prevent your operating system from booting.

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



Acronis True Image Echo Workstation repair or update will not affect the password. However, if the program is removed and then installed again while keeping the Acronis Secure Zone on the disk, the password for the zone will be reset.

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

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

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

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

9.2 Resizing the 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 could 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 to select the size.

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



Please keep in mind that reducing a system partition to the minimum size may prevent your operating system from booting.

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

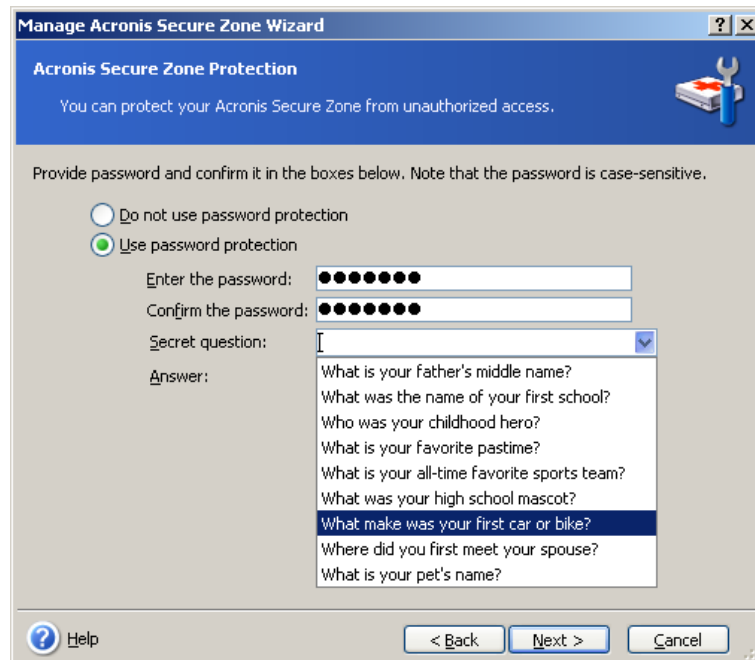
5. Next you will see a list of briefly described operations to be performed on partitions (disks).

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

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

9.3 Changing the password for Acronis Secure Zone

1. When prompted by the wizard, select **Manage Acronis Secure Zone**.
2. Select **Change password**.



3. Enter the new password and confirm it or select **Do not use password protection**. You can also select a secret question that will be asked in case you forget the password.
4. To perform the password change operation, click **Proceed** in the final wizard window.

9.4 Deleting Acronis Secure Zone

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

There is an option to keep Acronis Secure Zone along with its contents (which will enable data recovery on booting from bootable media) or remove Acronis Secure Zone if you remove Acronis True Image Agent or Acronis True Image Echo Workstation local version from the system. To delete the zone without uninstalling the program, proceed as follows.

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 zone. If you select several partitions, the space will be distributed proportionally to each partition.
3. Next, you will see a list of briefly described operations to be performed on partitions (disks).

After you click **Proceed**, Acronis True Image Echo Workstation 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.

Chapter 10. Creating bootable media

10.1 Creating Acronis rescue media

You can run Acronis True Image Echo Workstation 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 Echo Workstation version.

Because Acronis True Image Echo Workstation is available only as a download, you must create bootable media using the Bootable Media Builder. For this, you will need a blank CD-R/RW, DVD±R/RW, several formatted diskettes (the wizard will tell you the exact number), or any other media your computer can boot from, such as a Zip drive.

Acronis True Image Echo Workstation also has 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 Acronis True Image Echo Workstation from the RIS package.

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



This feature is available both in Acronis True Image Echo Workstation 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 Echo Workstation 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 Echo Workstation 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 Echo Workstation 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 Echo Workstation offers the following components:

- Acronis True Image Echo Workstation full version

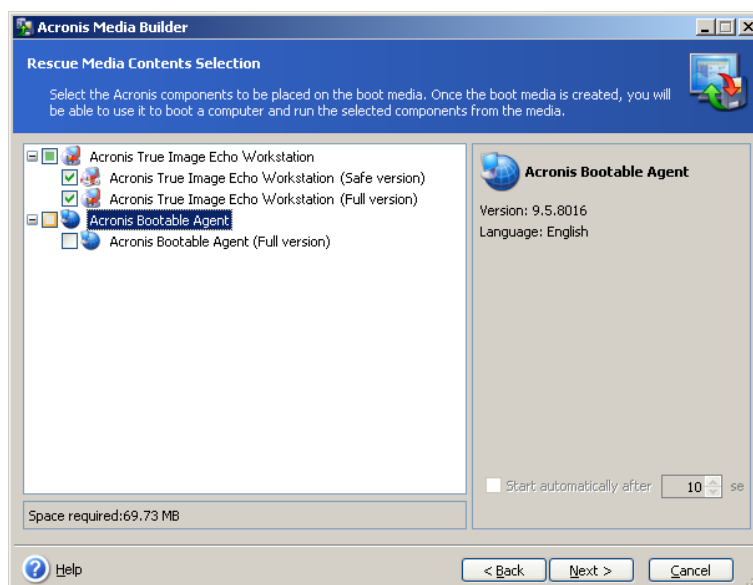
Includes support of USB, PC Card and SCSI interfaces along with the storage devices connected via them, and therefore is highly recommended.

- Acronis True Image Echo Workstation 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.



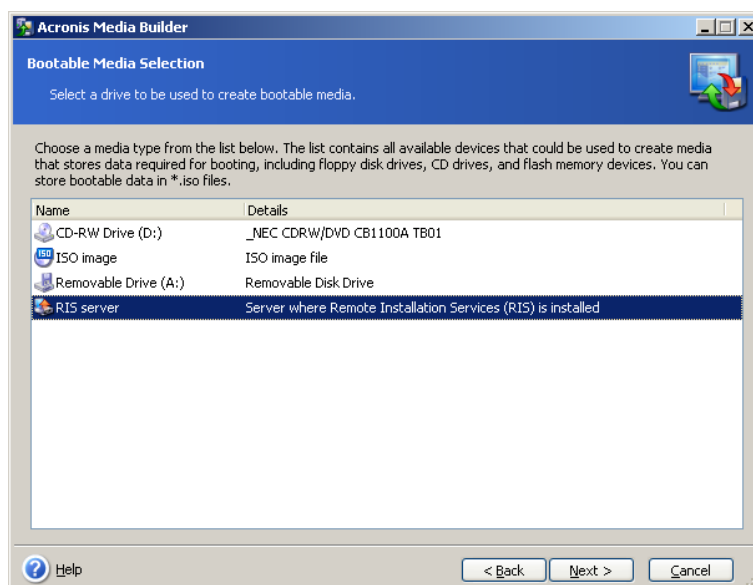
To find more about components of other Acronis products, see the respective user guides.

The **Start automatically after** parameter specifies the timeout interval for the boot menu. If this parameter is not specified, at booting a computer the program will display the boot menu and wait for someone to select whether to boot the OS or the Acronis component. If you set 10 sec for Acronis Bootable Agent, for example, the agent will launch in 10 seconds after the menu is displayed. This enables fully remote operations if you are booting from a RIS server.

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



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 Echo Workstation. To write another component, start the 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 in which 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, mark it and keep it in a safe place.

10.2 Creating a Win PE ISO with Acronis True Image Echo Workstation

Windows Preinstallation Environment (Win PE) is a minimal Windows system based on the Windows XP Professional and the Windows Server 2003 kernels. Win PE is commonly used by OEMs and corporations for deployment, test, diagnostic and system repair purposes. Using Acronis True Image Echo Workstation in Windows Preinstallation Environment allows a combination of Acronis True Image Echo Workstation and Win PE facilities and provides more functionality than using only-Acronis bootable media. The Acronis Universal Restore add-on to Acronis True Image Echo Workstation, if installed, will also be included in the ISO image.

To add the Acronis True Image Echo Workstation plug-in to your Win PE distribution:

1. Make sure that **Acronis Bart PE plug-in** is installed on the computer (the default path is \Program Files\Acronis\TrueImageEchoWorkstation\BartPE). If not, run Acronis True Image Echo Workstation setup file, choose **Modify** and install the Acronis Bart PE plug-in.

Acronis Win PE ISO Builder locates the Acronis Bart PE plug-in using the registry key **HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\TrueImageEchoWorkstation\Settings\BartPE**, created at the time of installation. If you moved the Bart PE plug-in to another folder after installation, change the key accordingly. If the above key is missing, the builder does not work.

2. Insert your Win PE distribution CD into the media drive of the computer. If you have a distribution copy on the hard disk, copy the path to it. The distribution files must be unpacked and allocated in a separate folder.

3. Select Programs -> Acronis -> Acronis True Image Echo Workstation -> Acronis Win PE ISO Builder.

4. Specify a source folder for building Win PE ISO, i.e. the media drive with Win PE distribution or a folder with the distribution copy.

5. Locate a folder where you want to create Win PE ISO and provide the name for the ISO file.

6. Check your settings in the summary screen and click **Proceed**.

7. Use any third-party tool that will burn ISO images to CD or DVD.



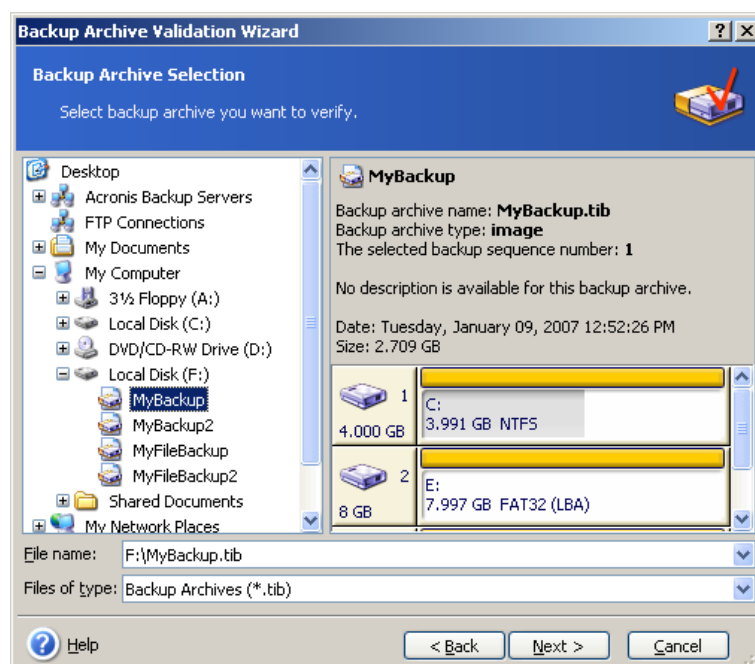
Media based on Win PE 2.0 and including Acronis True Image Echo Workstation requires at least 768MB RAM to work.

Chapter 11. Operations with archives

11.1 Validating backup archives

You can check the integrity of an archive to be certain that the archive is not damaged. Here's how to run a one-time validation task. For how to schedule regular archive validation, see *8.1 Creating scheduled tasks*.

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



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



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



Please note: if you are logged in as an administrator and decide to validate the Backup Server archives, the validation operation will affect all the archives created by all the accounts at the Backup Server, which can be a very time-consuming process.

11.2 Exploring archives and mounting images

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

This feature is available in Acronis True Image Echo Workstation local version only. Mounting images using Acronis True Image Management Console is not supported.

Archives located on an Acronis Backup Server or an FTP server cannot be explored or mounted.

Both operations are performed through the **Backup Archives** category.

Exploring images and file-level archives lets you view their contents and copy the selected files to the hard disk.

Mounting images as virtual drives lets 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

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

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

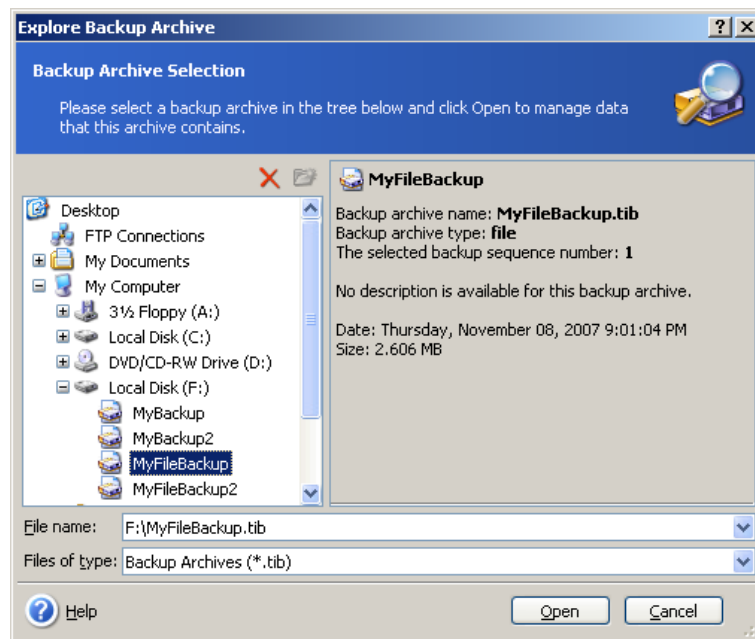


Acronis True Image Echo Workstation can mount or explore an image archive only if all its volumes reside in the same directory. If your archive spans several CD-R/RW discs and you want to mount the image, copy all volumes to a hard disk drive or network drive.

11.2.1 Exploring an archive

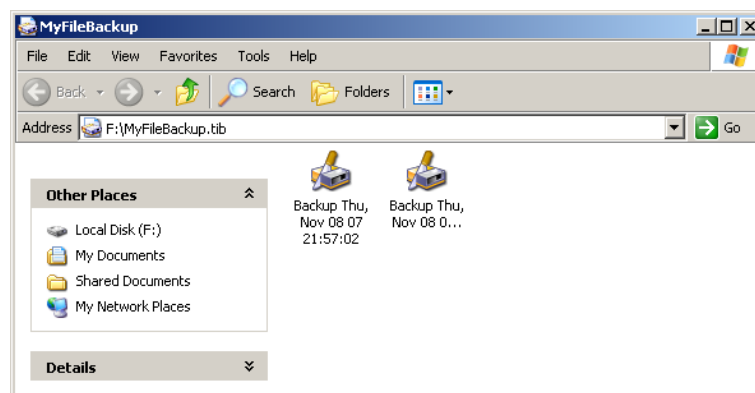
1. Click **Explore and Validate Backup Archives** in the **Tools** group or select the **Backup Archives** category on the sidebar to navigate to the Manage Backup Archives window. Then select **Explore Backup Archive**. Or, you can select **Tools -> Explore Backup Archive** in the main program menu.

2. Select an archive from the drive tree and click **Open**. If the archive is located in Acronis Secure Zone, select it to choose the archive at the next step. The explore operation does not support Acronis Backup Server, so backup servers are not displayed in the tree.



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 Echo Workstation will ask for it. Further steps will not be enabled until you enter the correct password.

3. The program opens a Windows Explorer window displaying the archive contents. If you selected an archive containing incremental or differential backups, Acronis True Image Echo Workstation will suggest that you select one of the successive backups by its creation date/time. This allows you to explore the data state for a given point in time.



To explore an incremental backup, you must have all previous incremental backups and the initial full backup. If any successive backups are missing, exploring is not possible.

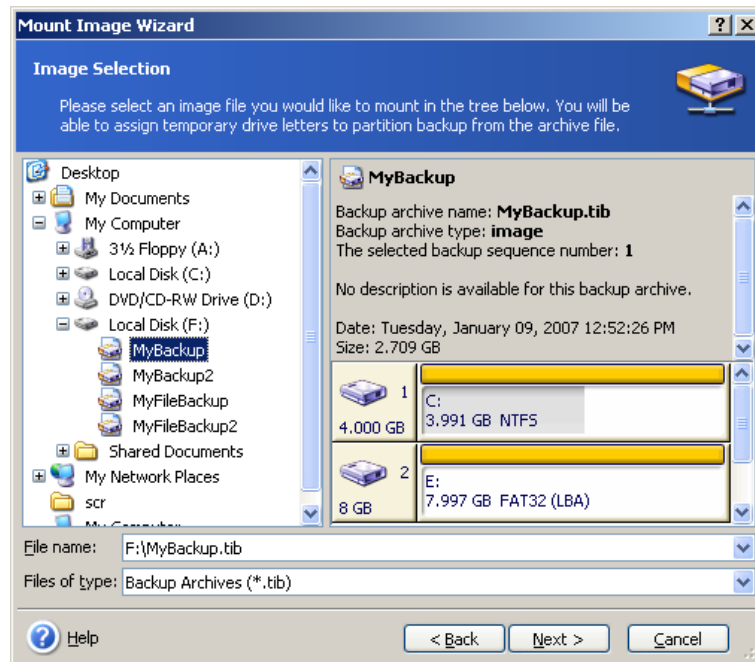
To explore a differential backup, you must have the initial full backup as well.

Double-click the backup icon to view the data saved in the backup. You can copy and paste or drag-and-drop any file or folder from the backup being explored to any hard disk folder.

11.2.2 Mounting an image

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

2. Select the archive from the drives tree. If the archive is located in the Acronis Secure Zone, select it to choose the archive. The mount operation does not support Acronis Backup Server, so backup servers are not displayed in the tree.



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 Echo Workstation will ask for it. Neither the partitions layout, nor the **Next** button will be enabled until you enter the correct password.

3. If you selected an archive containing incremental images, Acronis True Image Echo Workstation will suggest that you select one of the successive incremental images by its creation date/time. This allows you to explore the partition state for a given point in time.

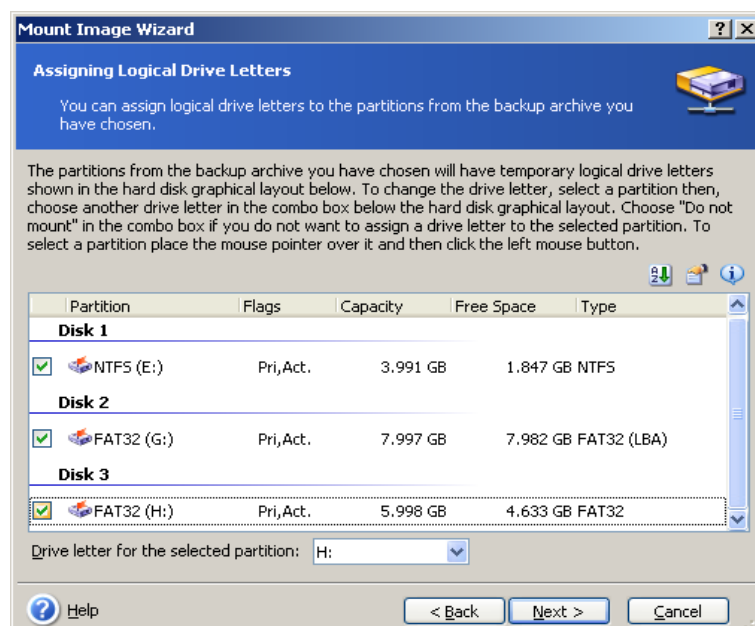


To mount an incremental image, you must have all previous incremental images and the initial full image. If any of the successive images are missing, mounting is not possible.

To explore a differential backup, you must have the initial full backup as well.

4. Select a partition to mount. (Note that you cannot mount the entire disk.)

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



-
5. Select whether you want to mount image in **Read-only** or **Read/Write** mode.
 6. 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.
 7. The program displays a summary containing a single operation. Click **Proceed** to connect the selected partition image as a virtual disk.
 8. 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 physical disk.

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

11.2.3 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 computer 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**.

11.3 Consolidating backups

The file name-based consolidation allows deleting the backups that you do not need any more from any archive while keeping the archive consistency. The operation is somewhat similar to consolidating backups on the Acronis Backup Server. In either case, you can delete from an archive, if need be, the base full backup. The program will create another full backup in place of the oldest remaining backup. The difference is as follows:

1. On the backup server, backups are deleted permanently. File name-based consolidation creates a consistent copy of the archive that does not contain deleted backups, but the source archive stays as is unless you delete it. This requires more disk space but ensures security of the archive in case the consolidation fails because of power failure or lack of disk space.
2. On the backup server, you only can consolidate two backups in one. File name-based consolidation keeps whichever backups you choose and deletes any backups that are not selected.

Consolidation can be performed both using the Acronis True Image Management Console connected to Acronis True Image Agent and with Acronis True Image Echo Workstation local version. The bootable program version also supports consolidation.

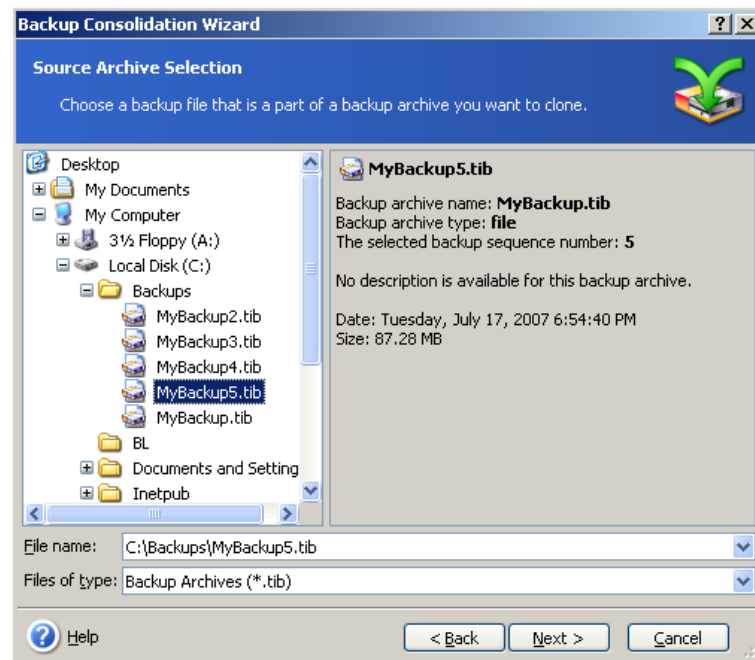
To consolidate backups in the archive:

1. Do one of the following:

Connect the console to the computer where Acronis True Image Agent is installed, select **Backup and Recovery tasks** and click **Consolidate Archive**.

In Acronis True Image Echo Workstation local version, start the **Backup Consolidation Wizard** by selecting **Tools -> Consolidate archive** in the main program menu.

2. Select the archive from the drives tree. The file name based consolidation does not support Acronis Backup Server and Acronis Secure Zone, so these are not displayed in the tree.

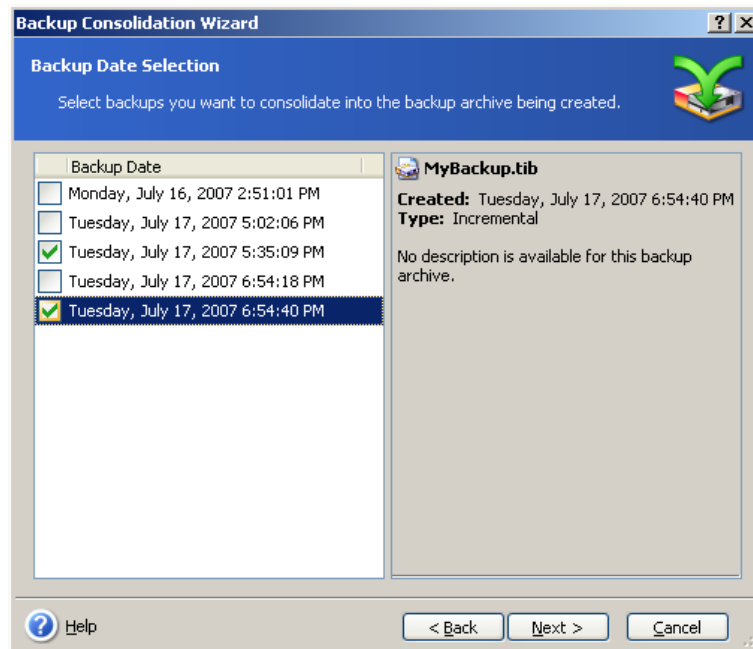


An archive MyBackup consisting of one full (MyBackup) and four incremental backups (MyBackup2-5) is selected

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

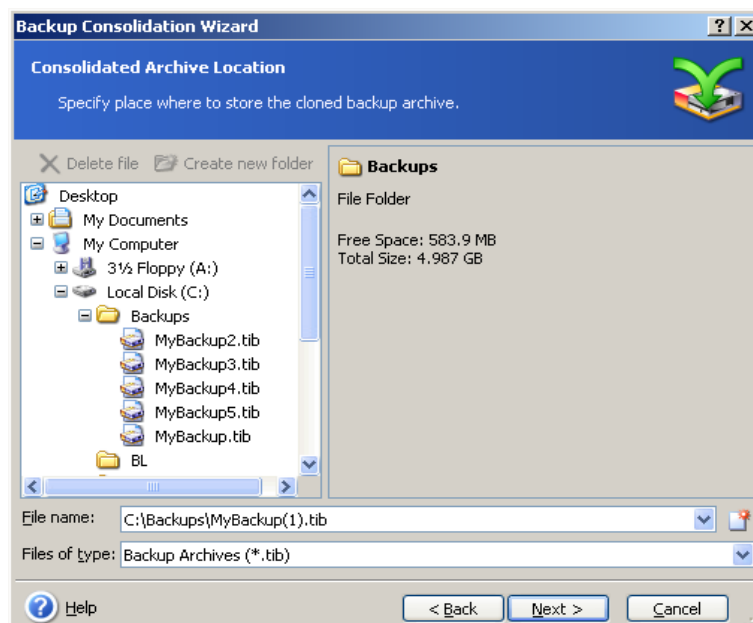


Editing images, mounted in R/W mode, results in creating incremental backups, that are a kind of offshoots of the incremental chain. Therefore, they cannot be consolidated and always will be excluded from the archive copy.



The clone archive will consist of MyBackup3 and MyBackup5, however, their numbers will be zero (no number) and 2. MyBackup3 will change into a full backup

4. Choose location and name for the archive copy. By default, the program suggests the same location and the source archive name with (1) added.

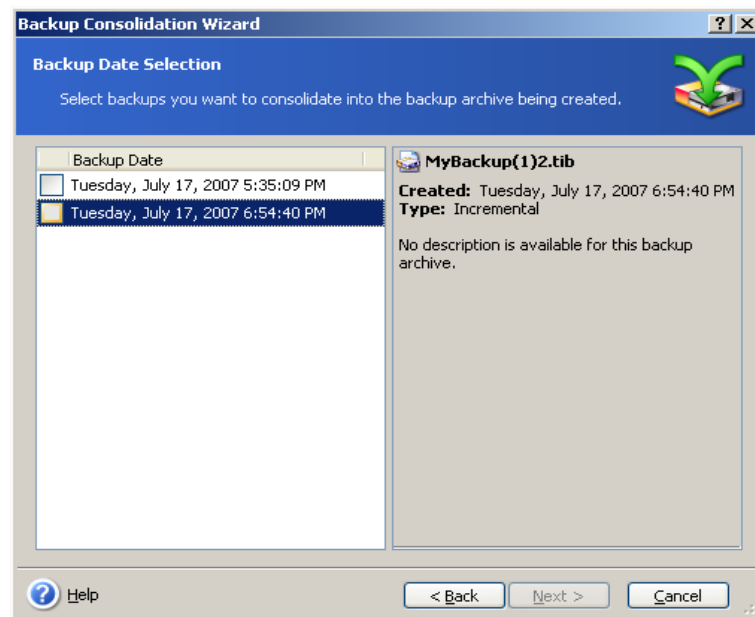


New archive will be created in the same folder and named MyBackup(1)

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

In our example, when consolidation is completed, the folder Backups will contain two archives MyBackup and MyBackup(1). The first is the source archive, the second is the copy consisting of MyBackup(1) and MyBackup(1)2.

MyBackup(1) is a full backup containing data as of Tuesday, July 17, 2007, 5:35:09 PM. MyBackup(1)2 is an incremental backup containing data as of Tuesday, July 17, 2007, 6:54:40 PM. You can make sure of this by starting the consolidation wizard again, selecting the archive MyBackup(1) and proceeding to the next window.



The resulting archive contents

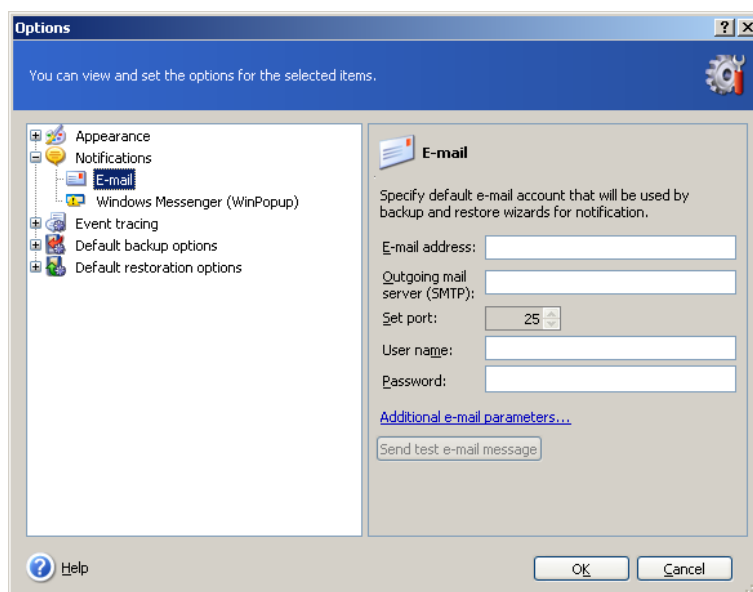
Chapter 12. Notifications and event tracing

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

12.1 Email notification

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



Provide the e-mail address to which notifications will be sent. You can enter several addresses separated by semicolons.

Provide the outgoing SMTP server name. A user name and a password might also be needed if the SMTP server requires authentication.

Some Internet service providers require authentication on the incoming mail server before being allowed to send anything. If this is your case, click **Advanced** and tick off **Log on to incoming mail server** and provide the server name.

Filling up the **From** and **Subject** fields will help the e-mail client program filter notifications to the appropriate folder. If the From field is left blank, messages will be constructed as if they are from the destination address.

Below, in this window, you can choose whether you want to get notifications:

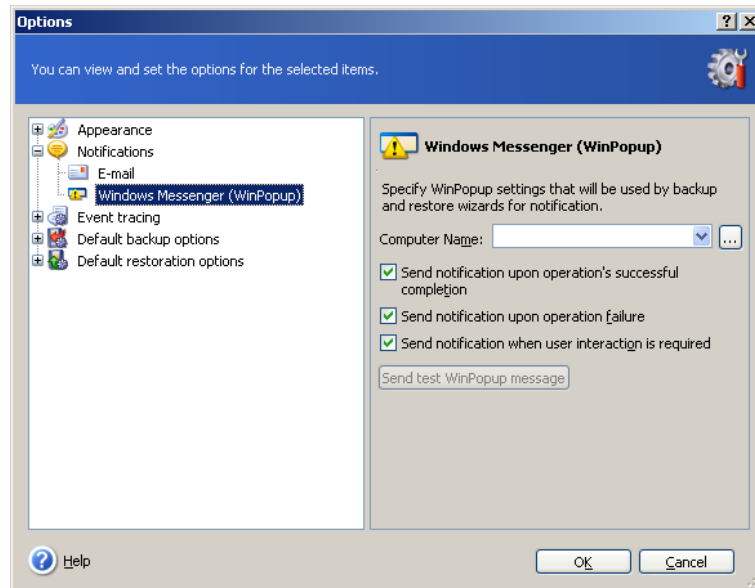
- when the operation is completed successfully (check **Add full log to the notification** to add the full operation log to the message)
- when the operation failed (check **Add full log to the notification** to add the full operation log to the message)
- during the operation when user interaction is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

12.2 WinPopup notification

To set up WinPopup notification:

1. Enable the Messenger service on both the computer executing the task and the computer that will receive messages.

2. Select **Tools -> Options -> Notifications -> Windows Messenger (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:

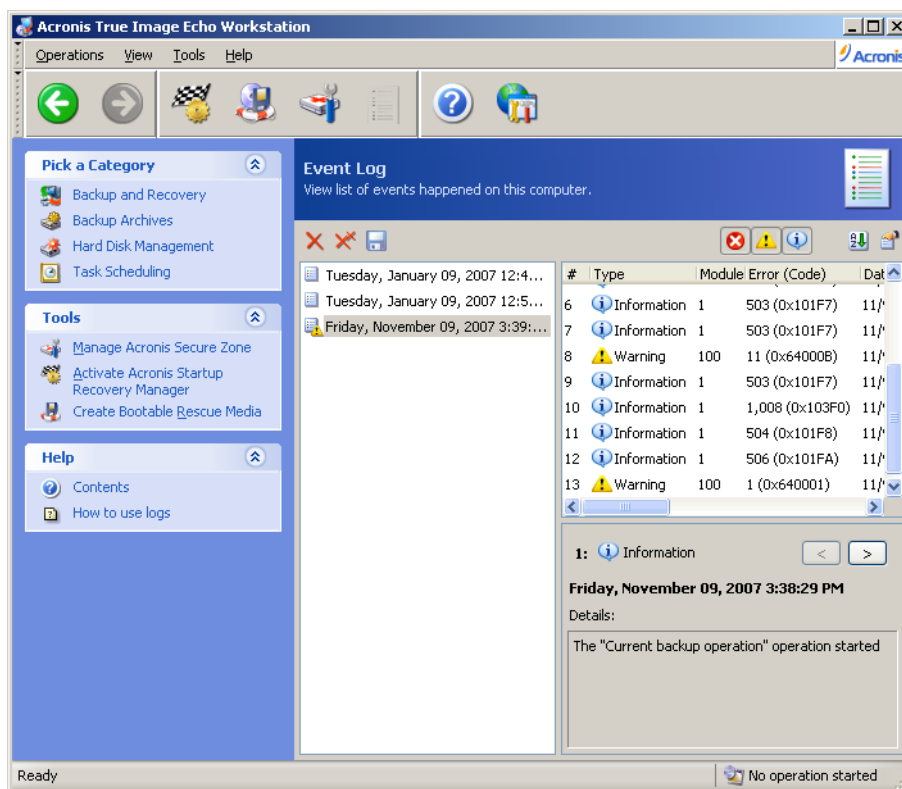
- when the operation is completed successfully
- when the operation failed
- during the operation when user interaction is required.

12.3 Viewing logs

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

To view 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 "X" 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 "X" 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.

12.4 Event tracing

12.4.1 Windows event log

You can choose whether to store event log messages issued by Acronis True Image Echo Workstation 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**.

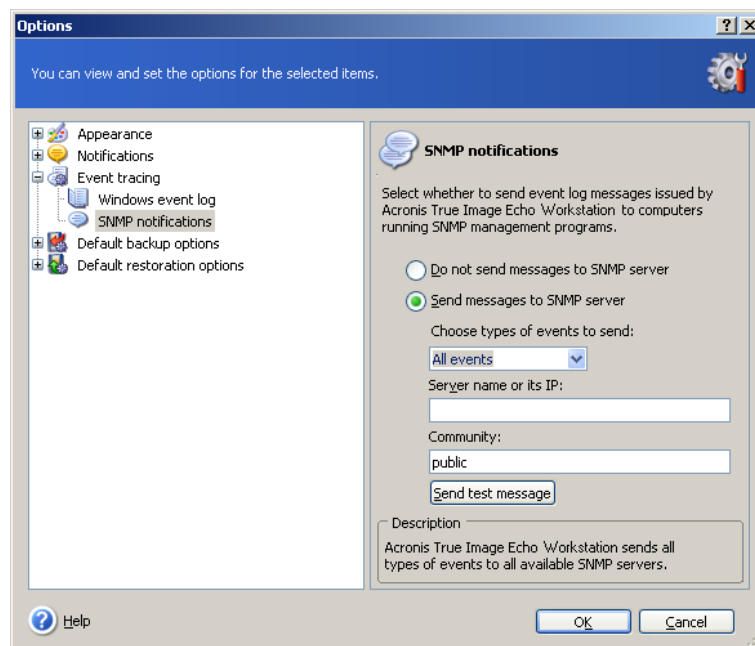
An additional choice is available - recording **All events, Warnings and Errors**, or **Errors only**.

12.4.2 SNMP notifications

Acronis True Image Echo Workstation can provide the following Simple Network Management Protocol (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 Echo Workstation in its log).



Sending SNMP messages is disabled by default. To set up sending messages, select **Send messages to SNMP server** and specify:

- types of events to be reported: All events, Warnings and Errors, or Errors only
- name or IP address of the host running the SNMP management application, to which notifications will be sent
- name of SNMP community to which both the host running SNMP management application and the computers executing the task belong.

12.5 Managing System Restore

Microsoft Windows System Restore tool, available in Windows XP and Windows Vista 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**.

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



This feature is available in Acronis True Image Echo Workstation local version only. Managing System Restore using Acronis True Image Management Console is not possible.

1. To start the **System Restore Management Wizard**, click the **Manage System Restore** icon in the main program window.
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 13. Working with a virtual environment

Virtual machine technologies provide a powerful tool to help accelerate the development, testing, deployment and support of PC applications.

As with physical machines, virtual machine (VM) data needs to be backed up periodically to prevent its loss due to hardware failure or human errors. Since more and more organizations choose running their business processes in a virtual environment, they need a solution to perform the data backup and restore on virtual machines. This chapter covers how Acronis True Image Echo Workstation can be used in virtual and heterogeneous environments.

13.1 Backing up data on virtual machines

A **virtual machine** is an emulated computer running within a host operating system. The software that emulates the computer is called the **virtualization software**. The most popular types of virtualization software are VMware Server and VMware Workstation, Microsoft Virtual Server and Microsoft Virtual PC, Citrix XenServer and Parallels Workstation.

Generally, a virtual machine can be treated:

1. As a physical computer (when it is online). Most Acronis True Image Echo Workstation features and settings are applicable to a VM. The backup procedure is almost the same (see details in *Chapter 6. Creating backup archives*).
2. As a set of files that change in line with the VM state. The files represent the VM configuration, storage, memory or other parameters. The files can be backed up with both imaging and file-level backup.

However, backing up the running VM files can prevent us from restoring the virtual system to a consistent point-in-time state. The issue is somewhat like backing up a database. (The classic example is the Active Directory database, which seldom can be recovered to a usable state.) Therefore, integration with dedicated tools available from VM vendors is advisable.

With the current version of Acronis True Image Echo Workstation, it is advisable that you treat online virtual computers that need to be backed up, as physical machines.

Stop or suspend the virtual machine if you plan to back up the virtual machine files. Since the virtual disk file changes from session to session and therefore will be always included in the backup, incremental or differential backups are not appropriate in this case. An incremental backup size will be almost equal to a full backup size.

13.2 Recovering data on virtual machines

A virtual disk can be restored from its image (.tib file), previously created with Acronis True Image Echo Workstation just as physical disk can be recovered.

If the virtual machine cannot start, boot it into Acronis rescue environment using physical bootable media or RIS server, or by adding the bootable media ISO to the virtual machine. Another option is to create a new virtual machine with same configuration and disk size as the imaged machine and recover data to this disk.

The procedure is the same as with physical machines. See details in *Chapter 7. Restoring the backup data*.

The alternative way of recovering a VM is by converting the image (.tib) file to a virtual disk file of appropriate format and adding this disk to the VM. This is the easiest way to recover data on a virtual machine.

13.3 Using the disk conversion feature

A virtual hard disk is a file that provides storage for a virtual machine. Different virtualization software use different virtual disk format and therefore the file extension.

Acronis True Image Echo Workstation has the ability to convert a disk image, created with the program (.tib), to a virtual disk file of the type you select (.vmdk, .pvs, and .vhd). You will then be able to add the disk to a virtual machine of compatible type: **VMware, Microsoft virtual machine (MS Virtual PC, MS Virtual Server, MS Hyper-V), Parallels virtual machine** and **Citrix XenServer**, respectively. The further usage of the disk is as follows.

13.3.1 Recover data on the VM

In case data is corrupted or inadvertently deleted while the VM is running, do one of the following:

- add the converted disk, either system or non-system, to the VM, copy the needed data to the original disk, then remove the converted disk, or
- add the converted disk, either system or non-system, to the VM and use the data contained on the disk.

13.3.2 Recover both data and the VM

In case the VM cannot start, do one of the following:

- add the converted system disk to the VM and remove the corrupted disk, or
- create a new VM with the converted system disk, or
- add the disk to the previously created machine clone (this allows replacing the machine on the network in seconds because you need not configure a new VM).

13.3.3 Physical to virtual migration

Physical disks images can be converted to virtual disks as well as virtual disks images.

A Windows system image will be supplemented with appropriate system drivers during conversion, so that Windows could boot up on the VM. (In fact, the Acronis Universal Restore technology is applied in background because the program is aware which drivers are needed for compatible virtual machines.)

The conversion operation enables five-step **physical to virtual** migration:

1. Create images of all (or some) physical machine disks, including the system disk.
2. Convert the images to virtual disks.
3. Create a new VM with the converted system disk.
4. Add the other converted disks to the VM.
5. Start the VM and complete the hardware drivers configuration, if Windows prompts.

This allows:

- the fastest replacement of the physical machine with the previously created virtual copy
- moving multiple workloads from legacy physical computers to virtual machines to reduce hardware maintenance and power consumption costs.

The alternative method of **physical to virtual** migration is by restoring a physical disk from an image to a virtual machine. The procedure is the same as with restoring physical machines.

To ensure booting up the system on the virtual machine, use Acronis Universal Restore. If the target virtual drive is a SCSI hard drive, provide appropriate drivers. For example, the VMware environment requires Buslogic or LSI logic drivers. Use drivers bundled with your virtualization software or download the latest drivers versions from the software manufacturer's website. For more information about the recovery procedure see *Chapter 7. Restoring the backup data*.

The inverse migration - **virtual to physical** - is done using common disk imaging and restoring:

1. Create images of all (or some) virtual machine disks, including the system disk.
2. Restore the images to physical disks. When restoring a system disk, use Acronis Universal Restore. Complete the hardware driver configuration if Windows prompts.

Combination of the two migration features gives you the flexibility to implement a lot of scenarios, for example:

- replace your physical computer on the network with its virtual copy, while the computer is recovered or upgraded
- test the new software or other changes you wish to make to the computer on its virtual copy and then apply the changes to the physical computer.

13.3.4 Converting workloads

You can convert workloads from one virtual technology to another through imaging virtual drives. For example, let's say your company uses Microsoft Virtual Servers, but you need to use VMware-based virtual appliances. This is easy to do with the conversion functionality. Again, a Windows system image will be supplemented with appropriate system drivers during conversion so that Windows could boot up on the another type of VM.

1. Create images of all (or some) virtual machine disks, including the system disk.
2. Convert the images to virtual disks of desired format.
3. Create a new VM of the desired type with the converted system disk.
4. Add the other converted disks to the VM.
5. Start the VM and complete the hardware driver configuration if Windows prompts.

13. 4 Converting disk images to virtual disks

To convert a disk image to a virtual disk file:

1. Do one of the following:

Connect the console to the computer where Acronis True Image Agent is installed. Select **Backup and Recovery tasks** and click **Convert to Virtual disk**.

On a computer where Acronis True Image Echo Workstation local version is installed, select **Tools -> Convert to Virtual Disk** in the main program menu.

2. Select the disk image to convert. If the image is located on an Acronis Backup Server or in the Acronis Secure Zone, select Personal backup location or Acronis Secure Zone, to select the image during the next step.
3. If there are several disks in the image, select one to convert.
4. Choose a type of the disk to be created.
5. Specify the path to the file to be created. The file can be directed to any storage supported by Acronis True Image Echo Workstation, except for an Acronis Backup Server or the Acronis Secure Zone.

Since the disk space is not preallocated, the physical disk on which the virtual disk will run is expected to have sufficient space for the virtual disk to grow.

6. Click **Proceed** in the summary window.

Chapter 14. Transferring the system to a new disk

14.1 General information

Sooner or later computer users find that their hard disk is just too small. If you don't have space for more data, you can add another disk specifically for data storage.

For example, 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 Echo Workstation local version only. Transferring systems using Acronis True Image Management Console is not supported.

To transfer the system, you must first install the disk in the computer. If a computer 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 some 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 additional 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 among 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 "X" inside in the upper left corner. Before you start cloning, you should check such disks for errors using the appropriate operating system tools.

14.2 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.

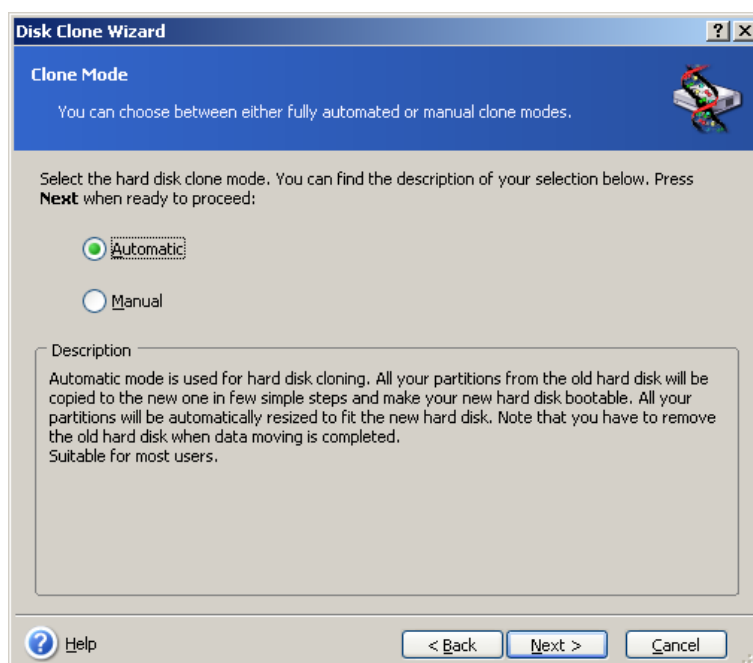
No data will be lost because the original disk is only being read (no partitions are changed or resized) until data transfer is completed.

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

14.3 Executing transfers

14.3.1 Selecting Clone mode

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

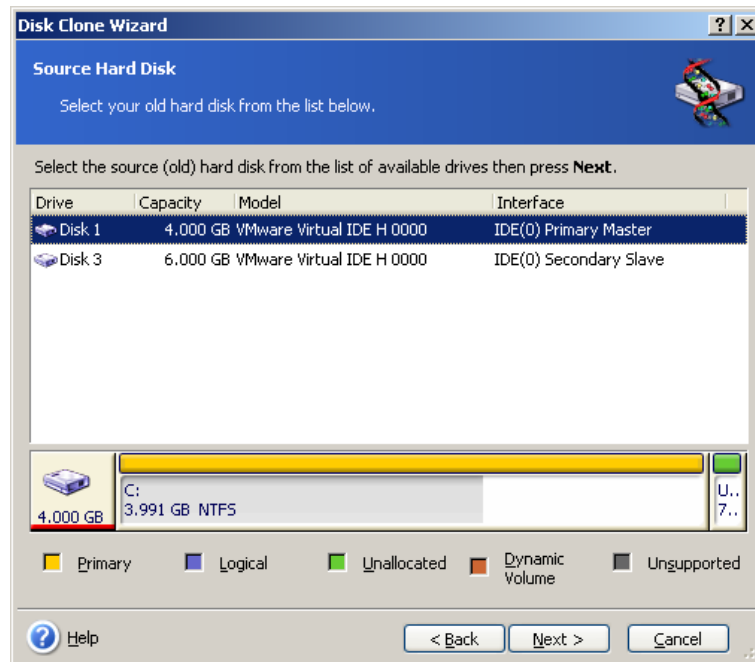


We recommend using automatic mode in most cases. The manual mode can be useful if you need to change the disk partition layout.

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.

14.3.2 Selecting source disk

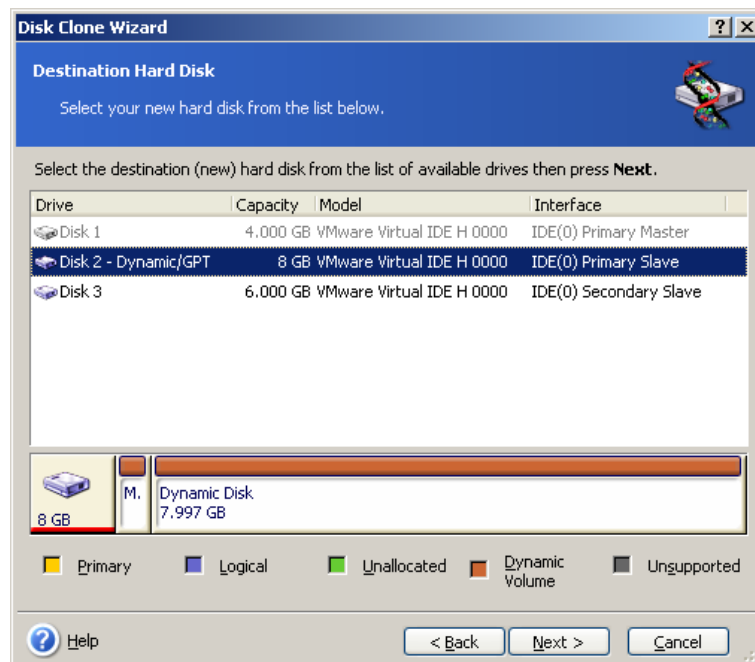
If the program finds several partitioned disks, it will ask you which is the source (i.e. the older data disk).



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

14.3.3 Selecting destination disk

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



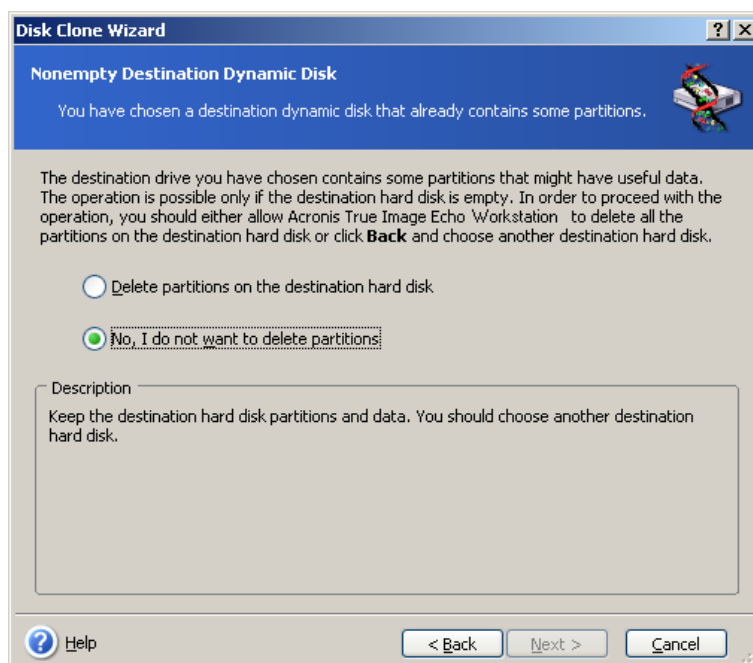
The previously selected source becomes grayed-out and disabled for selection.



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

14.3.4 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**.

14.3.5 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.

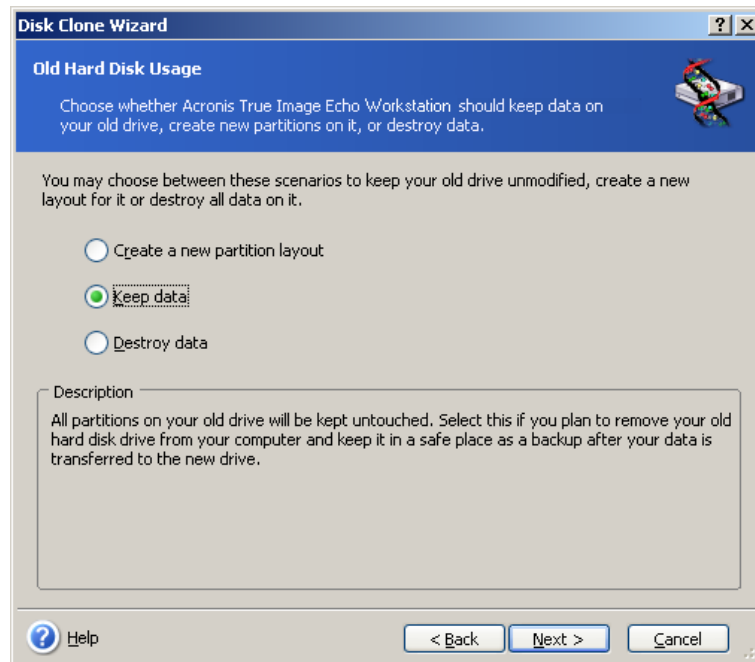
Next you will see the cloning summary.

14.3.6 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.

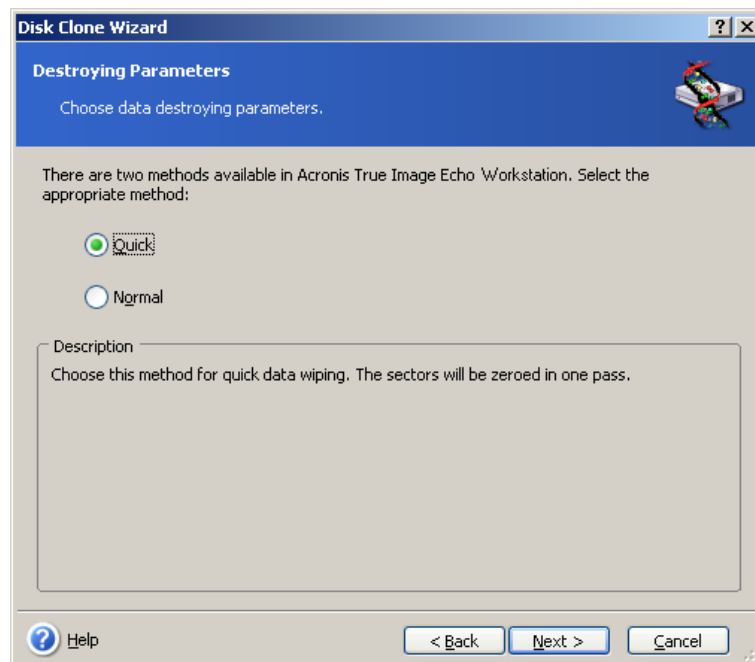
If you are going to keep it for data storage, you can create a new partition layout on it. In this case, the disk will be ready right after cloning is complete.

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.

14.3.7 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



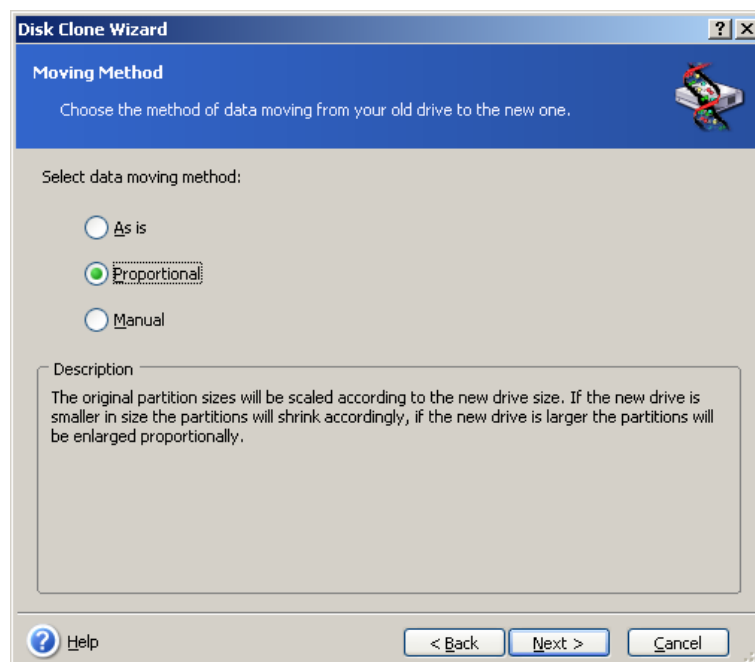
The second method takes more time, but makes it impossible to recover data afterwards, even with special equipment.

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

14.3.8 Selecting partition transfer method

Acronis True Image Echo Workstation 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 not recommended, as they leave much unallocated space on the new disk. Using the "as is" method, Acronis True Image Echo Workstation transfers unsupported and damaged file systems.

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

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

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

14.3.9 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.

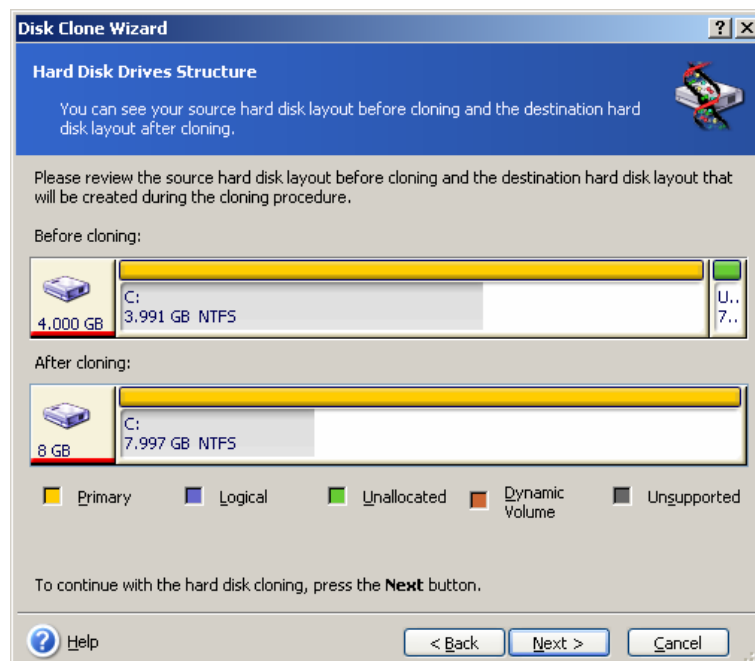
Having completed the required steps, you will add a new partition. To create another one, simply repeat those steps.

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**.

14.3.10 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.



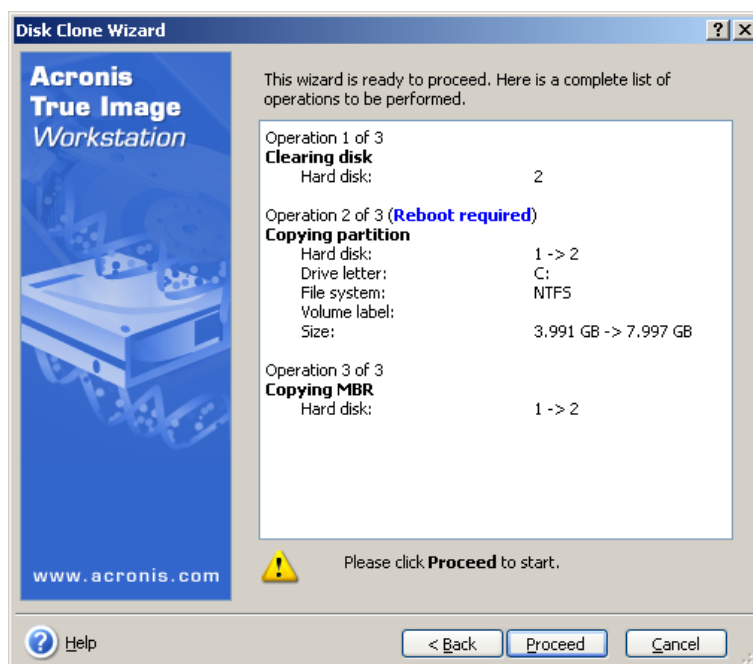
Along with the hard disk number, you will also see disk capacity, label, partition and file system information. Different partition types, including primary, logical and unallocated space are marked with different colors.



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

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

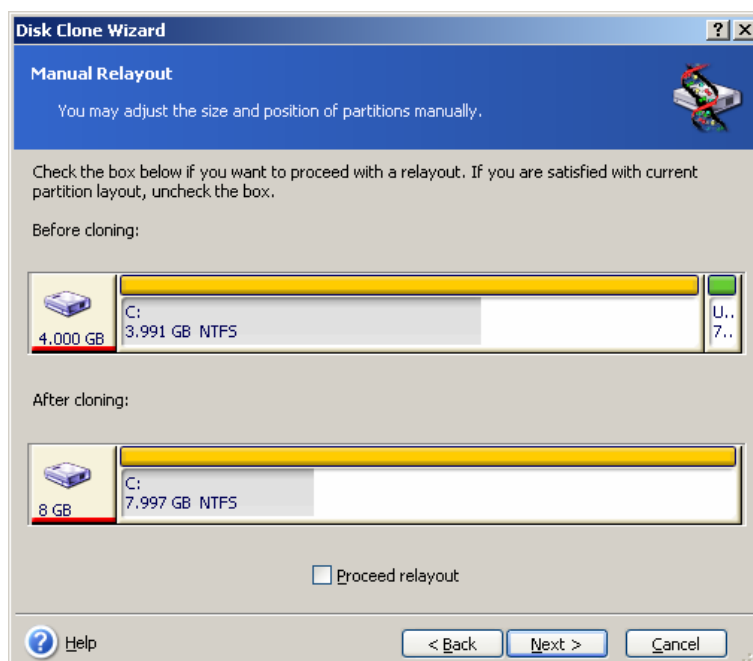
14.4 Cloning with manual partitioning

14.4.1 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 the **Unallocated space before**, **Partition size**, or **Unallocated space after** fields, by dragging the partition borders or by dragging 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 15. 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 to store data, leaving the system on the old disk. If the computer has space for another disk, it would be easier to add a data disk drive than to clone a system one.

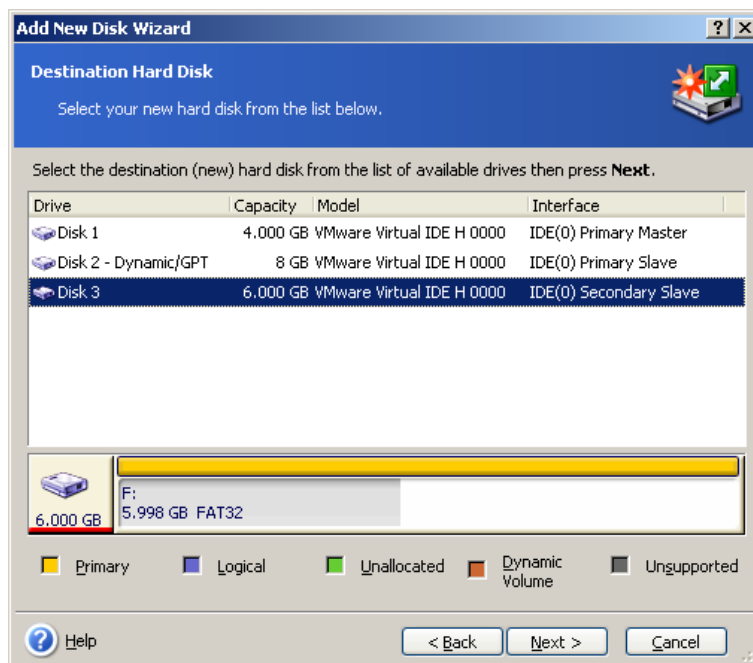


This feature is available in Acronis True Image Echo Workstation local version only. Adding disks using Acronis True Image Management Console is not supported.

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

15.1 Selecting a hard disk

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



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.

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

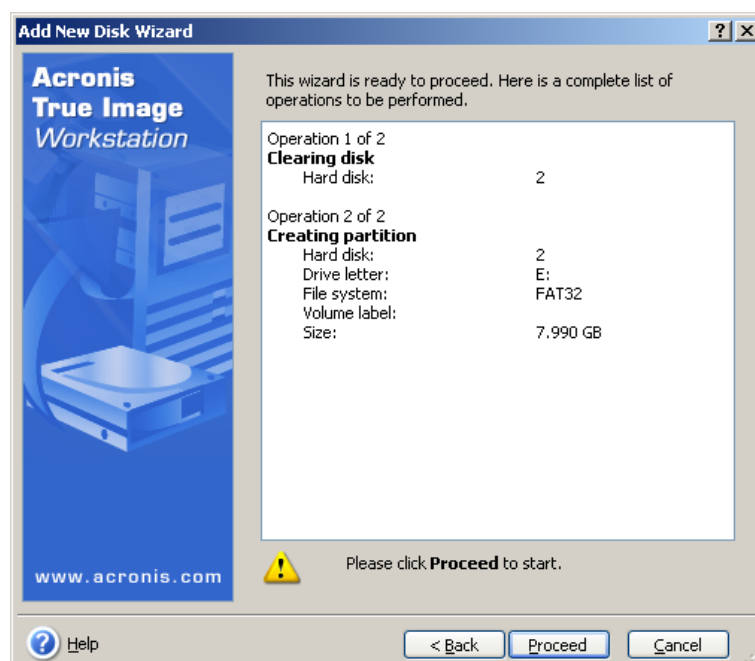
If the cursor turns to two vertical lines with left and right arrows, it is pointed at the partition border and you can drag it to enlarge or reduce the partition size. If the cursor turns to four arrows, it is pointed at the partition, so you can move it to the left or right (if there is unallocated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

15.3 Disk add summary

The disk add summary contains a list of operations to be performed on disks.



After you click **Proceed**, Acronis True Image Echo Workstation will start creating and formatting new partitions, indicating the progress in a special window. You can stop this procedure by clicking **Cancel**. In that case, you will have to repartition and format the new disk or repeat the disk add procedure.

Chapter 16. Command-line mode and scripting

Acronis True Image Echo Workstation (local version) supports the command-line mode and enables backup automation by executing XML scripts.

The command-line mode functionality is somewhat limited as compared to the GUI mode. You will not be able to perform operations that require the reboot of the system, such as restore a system partition or clone a system drive. These operations only can be done through the GUI.

Scripting is intended only for backup.

16.1 Working in the command-line mode

An administrator might need a console interface in some situations. Acronis True Image Echo Workstation supports this mode with **TrueImageCmd.exe** utility as well as the **ICompGS.exe** and **Ebasrvdb.exe** tools.

TrueImageCmd.exe is located in the folder where where Acronis True Image Echo Workstation has been installed, by default it is

C:\Program Files\Acronis\TrueImageEchoWorkstation.

ICompGS.exe is located in the folder where the Group Server is installed, by default it is

C:\Program Files\Acronis\GroupServer

Ebasrvdb.exe is located in the folder where the Backup Server is installed, by default it is

C:\Program Files\Acronis\BackupServer

16.1.1 TrueImageCmd supported commands

TrueImageCmd has the following format:

```
trueimagecmd /command /option1 /option2...
```

Commands may be accompanied with options. Some options are common for most trueimagecmd commands, while other are specific for individual commands. Below is a list of supported commands and compatible options.

Command	Common Options	Specific Options
create Creates an image of specified disks and partitions	/filename:[file name] /password:[password] /asz /net_user:[username] /net_password:[password] /ftp_user /ftp_password /incremental /differential /compression:[0...9] /split:[size in MB] /oss_numbers /reboot /log:[file name] /log_net_user:[remote user] /log_net_password:[password]	/harddisk:[disk number] /partition:[partition number] /file_partition:[partition letter] /raw /progress:[on off]
filebackup Backs up specified files and folders	/filename:[file name] /password:[password] /asz /net_user:[username] /net_password:[password] /ftp_user /ftp_password	/include:[names] /exclude_names:[names] /exclude_masks:[masks] /exclude_system /exclude_hidden

	/incremental /differential /compression:[0...9] /split:[size in MB] /reboot /log:[file name] /log_net_user:[remote user] /log_net_password:[password]	
deploy Restores disks and partitions, except for the MBR, from an image	/filename:[file name] /password:[password] /asz /index:N /net_user:[username] /net_password:[password] /ftp_user /ftp_password /oss_numbers /reboot /log:[file name] /log_net_user:[remote user] /log_net_password:[password]	/harddisk:[disk number] /partition:[partition number] /target_harddisk:[disk number] /target_partition:[partition number] /file_partition:[partition letter] /start:[start sector] /fat16_32 /size:[partition size in sectors] /type:[active primary logical] /preserve_mbr When using the Acronis Universal Restore option: /ur_path:[path] /ur_username:[user] /ur_password:[pwd] /ur_driver:[inf-filename]
deploy_mbr Restores the MBR from a disk or partition image	/filename:[file name] /password:[password] /asz /index:N /net_user:[username] /net_password:[password] /ftp_user /ftp_password /oss_numbers /reboot /log:[file name] /log_net_user:[remote user] /log_net_password:[password]	/harddisk:[disk number] /target_harddisk:[disk number]
filerestore Restores files and folders from a file archive	/filename:[file name] /password:[password] /asz /index:N /net_user:[username] /net_password:[password] /ftp_user /ftp_password /reboot /log:[file name] /log_net_user:[remote user] /log_net_password:[password]	/target_folder:[target folder] /overwrite:[older never always] /restore_security:[on off] /original_date:[on off]
verify Verifies the archive data integrity	/filename:[file name] /password:[password] /asz /net_user:[username] /net_password:[password] /ftp_user /ftp_password /reboot /log:[file name] /log_net_user:[remote user] /log_net_password:[password]	
pit_info Displays the numbered list of backups, contained in the specified archive	/filename:[file name] /password:[password] /asz /net_user:[username] /net_password:[password] /ftp_user /ftp_password	
consolidate Creates a consistent copy of the archive	/filename:[file name] /password:[password] /ftp_user /ftp_password /reboot /log:[file name]	/target_filename:[file name] /include_pits:[pits numbers] /net_src_user:[username] /net_src_password:[password]

which will contain only the specified backups	/log_net_user:[remote user] /log_net_password:[password]	/net_user:[username] /net_password:[password]
convert Converts an image to virtual disk format for using with a virtual machine	/filename:[file name] /password:[password] /asz /index:N /net_user:[username] /net_password:[password] /ftp_user /ftp_password /log:[file name] /log_net_user:[remote user] /log_net_password:[password]	/target_filename:[file name] /harddisk:[disk number] /vm_type:[vmware esx microsoft parallels] /ur /ur_path:[path]
list Lists available drives and partitions. With the filename option; lists the image contents	/password:[password] /index:N /asz /net_user:[username] /net_password:[password] /ftp_user /ftp_password	/filename:[file name]
explore Connects an image as a virtual drive	/filename:[file name]* /password:[password] /asz /index:N /net_user:[username] /net_password:[password] /log:[file name] /log_net_user:[remote user] /log_net_password:[password] *for a split image, the name of the last created file	/partition:[partition number] /letter:X
unplug Disconnects the image connected as a virtual drive		/letter:X /letter:all
asz_create Creates the Acronis Secure Zone on the selected drive	/oss_numbers /reboot /log:[file name] /log_net_user:[remote user] /log_net_password:[password]	/harddisk:X /partition:[partition number] /size:[ASZ size in sectors] unallocated /asz_activate
asz_activate Activates the Acronis Startup Recovery Manager	/password:[password]	
asz_content Displays the Acronis Secure Zone size, free space and contents	/password:[password]	
asz_files Displays the Acronis Secure Zone size, free space and contents using the	/password:[password]	

generated file names		
asz_delete_files Deletes the most recent backup in the archive located in the Acronis Secure Zone	/filename: [file name] /password: [password] /log: [file name] /log_net_user: [remote user] /log_net_password: [password]	
asz_delete Deletes the Acronis Secure Zone	/password: [password] /oss_numbers /reboot /log: [file name] /log_net_user: [remote user] /log_net_password: [password]	/partition: [partition number]
clone Clones a hard disk	/reboot	/harddisk: [disk number] /target_harddisk: [disk number]
help Shows usage		

16.1.2 Common options (options common for most trueimagecmd commands)

Option	Description	Archive location
Access to archives		
/filename: [file name]	Backup file name	Other than ASZ
	Archive name (when restoring or deleting files from ASZ). Can be obtained with asz_files)	ASZ
/password: [password]	Specify the password for the archive (if required)	Other than ASZ
	Specify the password for the ASZ (if required)	ASZ
/asz: [number of archive]	Addresses to the ASZ and selects the archive (a full backup with or without increments). To get the archive number, use /asz_content	ASZ
/index: N N = Number of the backup in an archive: 1 = basic full backup 2 = 1st increment... and so on 0 (default) = latest increment	Selects a backup in a sequence of incremental backups inside the archive. To get a backup index from the ASZ, use /asz_content	Any
/net_user: [username]	Specify a user name for network drive access	Network drive
/net_password: [password]	Specify a password for network drive access	Network drive
/ftp_user: [username]	Specify a user name for access to an FTP	FTP server

	server	
/ftp_password:[password]	Specify a password for access to an FTP server	FTP server
Backup options		
/incremental	Set the backup type to incremental. If not specified or there is no basic full backup, a full backup will be created	Any
/differential	Set the backup type to differential. If not specified or there is no basic full backup, a full backup will be created	Any
/compression:[0...9]	Specify the data compression level. It ranges from 0 to 9 and is set to 3 by default	Any
/split:[size in MB]	Split the backup into parts of the specified size	Other than ASZ
General options		
/oss_numbers	Declares that numbers of partitions in the /partition option are adjusted for the MBR partition table rather than just as ascending numbers. This means that primary partitions have numbers 1-1, 1-2, 1-3, 1-4; logical partitions numbers start with 1-5. For example, if the disk has one primary and two logical partitions, their numbers can appear as follows: /partition:1-1,1-2,1-3 or /oss_numbers /partition:1-1,1-5,1-6	Any
/reboot	Reboot the computer after the operation is completed	Any
/log:[file name]	Create a log file of the current operation with the specified file name	Any
/log_net_user:[remote user]	If the log file is created on a network share, include the user name for logon to the share	Any
/log_net_password:[password]	If the log file is created on a network share, include the password for logon to the share	Any

16.1.3 Specific options (options specific for individual trueimagecmd commands)

Option	Description
create	
/harddisk:[disk number]	<p>Specifies the hard disks to include into the image file. 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.:</p> <pre>/harddisk:1,3</pre> <p>By specifying</p> <pre>/harddisk:DYN</pre> <p>you will back up all dynamic volumes present in the system.</p>
/partition:[partition number]	<p>Specifies the partitions to include into the image file. The list of available partitions is provided by /list. Partition numbers are specified as <disk number>-<partition number>, e.g.:</p> <pre>/partition:1-1,1-2,3-1</pre> <p>Dynamic volumes are specified with prefix DYN, e.g.:</p> <pre>/partition:DYN1,DYN2</pre>
/file_partition:[partition letter]	<p>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:</p> <pre>/file_partition:D /filename:"\1.tib"</pre> <p>Dynamic volumes are specified with prefix DYN, e.g.:</p> <pre>/file_partition:DYN1 /filename:"\1.tib"</pre>
/raw	<p>Use this option to create an image of a disk (partition) with an 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 (for the supported file systems).</p>
/progress:[on off]	<p>Shows/hides the progress information (percent completed). It is shown by default.</p>
filebackup	
/include:[names]	<p>Files and folders to be included in the backup (comma separated). For example:</p> <pre>/include:E:\Workarea\MyProject</pre>
/exclude_names:[names]	<p>Files and folders to be excluded from the backup (comma separated). For example:</p> <pre>/exclude_names:E:\Workarea\MyProject\111.doc,E:\Workarea\MyProject\Old</pre>
/exclude_masks:[masks]	<p>Applies masks to select files to be excluded from the backup. Use the common Windows masking rules. For example, to exclude all files with extension .exe, add *.exe. My????.exe will exclude all .exe files with names consisting of five symbols and starting with</p>

	<p>"my".</p> <p>/exclude_masks:*.txt,111.*</p>
/exclude_system	Excludes all system files from the backup.
/exclude_hidden	Excludes all hidden files from the backup.
deploy	
/file_partition:[partition letter]	<p>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:</p> <p>/file_partition:D /filename:"\1.tib"</p> <p>Dynamic volumes are specified with prefix DYN, e.g.:</p> <p>/file_partition:DYN1 /filename:"\1.tib"</p>
/harddisk:[disk number]	Specifies the basic hard disks to restore.
/partition:[partition number]	<p>Specifies the partitions to restore.</p> <p>Dynamic volumes are specified with prefix DYN, e.g.:</p> <p>/partition:DYN1</p>
/target_harddisk:[disk number]	<p>Specifies the hard disk number where the image will be restored.</p> <p>By specifying</p> <p>/target_harddisk:DYN</p> <p>you will select unallocated space on all dynamic disks that present in the system.</p>
/target_partition:[partition number]	<p>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.</p> <p>Dynamic volumes are specified with prefix DYN, e.g.:</p> <p>/target_partition:DYN1</p>
/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).
/fat16_32	Enables the file system conversion from FAT16 to FAT32 if the partition size after recovery is likely to exceed 2GB. Without this option, the recovered partition will inherit the file system from the image.
/type:[active primary logical]	<p>Sets the restored partition active, primary or logical, if possible (for example, there cannot be more than four primary partitions on the disk.) Setting a partition active always sets it primary, while a partition set primary may stay inactive.</p> <p>If the type is not specified, the program tries to keep the target partition type. If the target partition is active, the restored partition is set active. If the target partition is primary, and there are other primary partitions on the disk, one of them will be set active, while the restored partition becomes primary. If no other primary partitions remain on the disk, the restored partition is set active.</p> <p>When restoring a partition on unallocated space, the program</p>

	<p>extracts the partition type from the image. For the primary partition, the type will be set as follows:</p> <ul style="list-style-type: none"> - if the target disk is the 1st according to BIOS and it has not other primary partitions, the restored partition will be set active - if the target disk is the 1st according to BIOS and there are other primary partitions on it, the restored partition will be set logical - if the target disk is not the 1st, the restored partition will be set logical.
<code>/preserve_mbr</code>	<p>When restoring a partition over an existing one, the target partition is deleted from the disk along with its entry in the target disk MBR. Then, with the <code>/preserve_mbr</code> option, the restored partition's entry will occupy the upper empty position in the target disk MBR. Thus, the target disk MBR is preserved. If not specified, the restored partition's entry will occupy the same position as in the source disk MBR saved in the image. If the position is not empty, the existing entry will be moved to another position.</p>
<p>The following options are available when using the Acronis Universal Restore add-on to Acronis True Image Echo Workstation. For more information see <i>3.7 Acronis Universal Restore</i>.</p>	
<code>/ur_path: [path]</code> <code>/ur_username: [user]</code> <code>/ur_password: [pwd]</code>	<p>Specifies using Acronis Universal Restore and the path to the drivers storage.</p>
<code>/ur_driver: [inf-filename]</code>	<p>Specifies using Acronis Universal Restore and the mass-storage driver to be installed.</p>
filerestore	
<code>/target_folder: [target folder]</code>	<p>Specifies a folder where folders/files will be restored (a target folder). If not specified, the original path is re-created from the archive.</p>
<code>/overwrite: [older never always]</code>	<p>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:</p> <p><code>older</code> – this will give the priority to the most recent file modification, whether it be in the archive or on the disk.</p> <p><code>never</code> – this will give the file on the hard disk unconditional priority over the archived file.</p> <p><code>always</code> – this will give the archived file unconditional priority over the file on the hard disk.</p> <p>If not specified, the files on the disk will <code>always</code> be replaced with the archived files.</p>
<code>/restore_security: [on off]</code>	<p>Specifies whether to restore files' security attributes (default) or the files will inherit the security settings of the folder where they will be restored.</p>
<code>/original_date: [on off]</code>	<p>Specifies whether to restore files' original date and time from the archive or assign the current date and time to the restored files. If not specified, the current date is assigned.</p>

consolidate	
/target_filename:[file name]	Specifies the path to and name of the archive copy to be created. If there are two or more backups (pits) in the copy, numbers will be added to their names.
/include_pits:[pits numbers]	Specifies the backups (pits) to be included in the archive copy. To get the numbers of pits, use /pit_info. Separate multiple values with semicolon, for example: /include_pits:2,4,5
/net_src_user:[username]	Specifies the username for logon to network share to access the source archive
/net_src_user:[password]	Specifies the password for logon to network share to access the source archive
/net_user:[username]	Specifies the username for logon to network share to save the resulting archive
/net_user:[password]	Specifies the password for logon to network share to save the resulting archive
convert	
/target_filename:[file name]	Specifies the path to and name of the virtual disk file to be created. The file extension corresponds to the type of the virtual machine to which the virtual disk will be added: VMware virtual machine - .vmdk MS virtual machine and Citrix XenServer - .vhd Parallels virtual machine - .hdd.
/harddisk:[disk number]	Specifies the hard disks to convert by numbers. For each disk, a separate virtual disk will be created. By specifying /harddisk:DYN you will convert all dynamic volumes that present in the system.
/vm_type:[vmware esx Micro soft parallels]	The type of the virtual machine to which the virtual disk will be added.
/ur	Use when converting image of a disk, containing Windows, and the resulting virtual disk is supposed to be bootable. With this key, the program will add drivers, necessary for the virtual machine type selected with /vm_type key, to the resulting virtual disk. If the image was taken from a virtual machine of the same type, normally the key is not needed. Drivers for the virtual machine reside in the storage, defined by the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\UniversalRestore\Drive rsPackPath. In case the storage has been moved, please change the key or use the command /ur_path:[path] .
/ur_path:[path]	The same as /ur with custom path to the virtual machine drivers storage.

list	
/filename: [file_name]	<p>With this option, the image contents is displayed.</p> <p>When listing image contents, partition numbers may not coincide with those in the drives/partitions list, if the image does not contain all the disk partitions. For example, if the image contains partitions 2-3 and 2-5, they will be listed as 2-1 and 2-2.</p> <p>If the <code>deploy /partition</code> command cannot find a partition in the image by its physical number, use <code>/partition:<number in the image> /target_partition:<physical number of the target partition></code> keys. For the above example, to restore partition 2-5 to its original place use:</p> <p><code>/partition:2-2 /target partition:2-5.</code></p>
explore	
/partition: [partition number]	<p>Specifies a list of partitions to be mounted as virtual drives. Without this option, all partitions stored in the image will be mounted.</p> <p>To obtain the partition number for this option, list the image contents with the <code>/list/filename</code> command and use the number from the <code>Idx</code> column.</p>
/letter	Assigns letters to the mounted drives. This option is used with <code>/partition</code> option only.
unplug	
/letter:X	Specifies the virtual drive to be disconnected by letter.
/letter:all	Disconnects all virtual drives.
asz_create	
/harddisk:X	Specifies the hard disk number where the Acronis Secure Zone will be created.
/partition: [partition number]	Specifies partitions from which free space will be taken for Acronis Secure Zone.
/size: [ASZ size in sectors unallocated]	<p>Sets the Acronis Secure Zone size (in sectors).</p> <p>If not specified, the size is set as an average between the maximal (unallocated space plus free space on all partitions selected with the <code>/partition</code> option) and minimal (about 35MB) values.</p> <p>Either way, the program will first use the unallocated space. If there is not enough unallocated space, the selected partitions will be decreased. Resizing of locked partitions requires a reboot.</p> <p>With "unallocated", the zone will use all unallocated space on the disk. Partitions will be moved, if necessary, but not resized. Moving of locked partitions requires a reboot. The <code>/partition</code> option is ignored.</p>
/asz_activate	Activates the Acronis Startup Recovery Manager. The option will not take effect if the system partition is resized during Acronis Secure Zone creation. In that case, use the separate <code>/asz_activate</code> command.
asz_activate	
/password: [password]	Sets a password for the Acronis Secure Zone.

asz_delete	
/partition:[partition number]	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.
clone	
/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.

16.1.4 Trueimagecmd.exe usage examples

1. Image disks and partitions

```
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. The image will be saved to the C:\Test\ folder.

```
trueimagecmd /create /asz /partition:2-1,1-3
```

- This will create an image of the partitions 2-1 and 1-3 in the Acronis Secure Zone.

```
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. The image will be saved in the folder \Test on 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 640MB, and contain all cluster data. Image compression level is 5. The computer will be rebooted after the operation is completed.

```
trueimagecmd /create /partition:2-1  
/filename:\\server1\folder\arc.tib /net_user:user1  
/net_password:pw1 /log:\\server2\dir\log1.log  
/log_net_user:user2 /log_net_password:pw2
```

- This will create an image of partition 2-1 named arc.tib in the shared folder \\server1\folder. The operation log file log1.log will be saved on another share \\server2\dir\ . Credentials for both shares are provided.

```
trueimagecmd /create /partition:2-1  
/filename:ftp://server/folder/archive.tib /ftp_user:usr1  
/ftp_password:pswd1
```

- This will create an image of partition 2-1 in the archive.tib file located on the FTP server.

2. Restore disks and partitions

```
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:63 /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 63 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.

```
trueimagecmd /deploy_mbr /harddisk:1 /asz:2 /index:3  
/password:pswd
```

- This will restore MBR from the image of hard disk 1 to the same hard disk 1. The image is contained in the backup 3rd created in the archive number 2, located in Acronis Secure Zone that is protected with the 'pswd' password.

```
trueimagecmd /deploy_mbr /harddisk:1 /target_harddisk:2  
/filename:ftp://server/folder/arc.tib /ftp_user:fuser  
/ftp_password:fpswd
```

- This will restore MBR from the image of hard disk 1 to the hard disk 2. The image is contained in the arc.tib file located on the FTP server.

3. Back up files

```
trueimagecmd /filebackup /filename:E:\Backups\Myproject.tib  
/include:D:\Workarea\MyProject /exclude_names:  
D:\Workarea\MyProject\Old /exclude_hidden
```

- This will back up files from the MyProject folder residing in D:\Workarea, except for files in the Old subfolder and hidden files, to the file Myproject.tib and save this file in E:\Backups folder.

4. Restore files

```
trueimagecmd /filerestore /filename:E:\Backups\Myproject.tib  
/original_date
```

- This will restore all files from E:\Backups\Myproject.tib to the original folder and assign the files the original date and time. Since the /overwrite option is not specified, the latest files modifications will be replaced with the original ones.

5. Consolidate backups

```
trueimagecmd /pit_info /filename:\\smbsrv\Archives\Kons.tib
```

- This will display the numbered list of backups, contained in the archive Kons.tib residing on the network share \\smbsrv\Archives\.

```
C:\Program Files\Acronis\TrueImageEchoWorkstation>trueimagecmd /pit_info /filename:\\srv\elenal\kons.tib
Pit number: 1
  type: image; kind: base; date: 6/27/2007 11:39:10 AM
Pit number: 2
  type: image; kind: incremental; date: 6/27/2007 11:43:13 AM
Pit number: 3
  type: image; kind: incremental; date: 6/27/2007 11:44:04 AM
Pit number: 4
  type: image; kind: incremental; date: 6/27/2007 11:48:22 AM
Pit number: 5
  type: image; kind: incremental; date: 6/27/2007 11:50:32 AM

Operation has succeeded.
```

```
trueimagecmd /consolidate
/filename:\\smbsrv\Archives\Kons.tib
/target_filename:D:\Kons_new.tib /include pits:2,4,5
```

- This will create on the disk D: an archive consisting of three files Kons_new.tib, (pit 2 of the archive \\smbsrv\Archives\Kons.tib, former \\smbsrv\Archives\Kons2.tib) Kons_new2.tib (pit 4, former \\smbsrv\Archives\Kons4.tib) and Kons_new3.tib (pit 5, former \\smbsrv\Archives\Kons5.tib).

6. Convert an image to virtual disk

```
trueimagecmd /convert /filename:C:\MyBackup.tib
/target_filename:C:\MyHDD.vmdk /vm_type:vmware /harddisk:1,3
```

- This will convert images of disks 1 and 3, contained in the file C:\MyBackup.tib, to the virtual disks C:\MyHDD.vmdk and C:\MyHDD2.vmdk for using with VMware type virtual machines.

7. List

```
trueimagecmd /list
```

- This will list available partitions.

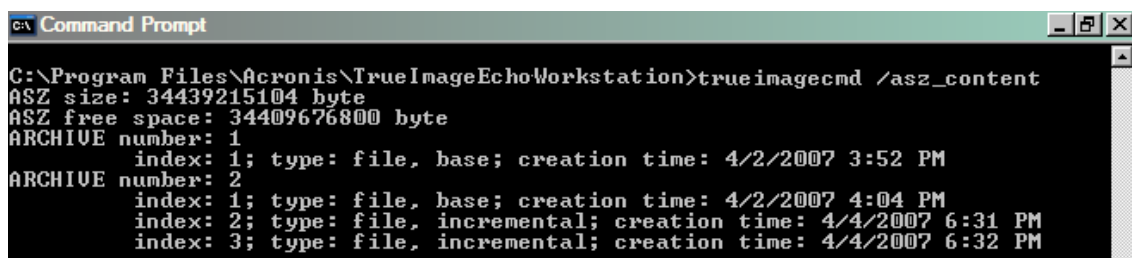
```
trueimagecmd /list /asz
```

- This will list contents of the latest image located in Acronis Secure Zone.

8. Acronis Secure Zone: managing backups by archive numbers

```
trueimagecmd /asz_content
```

- This will list the Acronis Secure Zone size, free space and contents.



```
C:\Program Files\Acronis\TrueImageEchoWorkstation>trueimagecmd /asz_content
ASZ size: 34439215104 byte
ASZ free space: 34409676800 byte
ARCHIVE number: 1
  index: 1; type: file, base; creation time: 4/2/2007 3:52 PM
ARCHIVE number: 2
  index: 1; type: file, base; creation time: 4/2/2007 4:04 PM
  index: 2; type: file, incremental; creation time: 4/4/2007 6:31 PM
  index: 3; type: file, incremental; creation time: 4/4/2007 6:32 PM
```


In our example, the Acronis Secure Zone contains two archives. The older archive #1 consists of one full (base) file-level backup created on 4/2/2007 at 3:52. The second archive contains a base file-level backup with two increments. You can restore data from any backup as follows:

```
trueimagecmd /filerestore /asz:2 /index:2 /target_folder:e:
```

- This will restore files and folders from the backup created on 4/4/2007 at 6:31 PM with their original paths to the root of partition E.

```
trueimage /list /filename:asz://2 /index:3 /password:aszpw
```

which is equal to:

```
trueimagecmd /list /asz:2 /index:3 /password:aszpw
```

- This will list content of the backup 3rd created in the archive number 2, located in Acronis Secure Zone that is protected with the 'aszpw' password.

9. Acronis Secure Zone: managing backups by file names

```
trueimagecmd /asz_files /password:aszpw
```

- This will list the Acronis Secure Zone size, free space and contents using generated filenames.

```
Command Prompt
C:\Program Files\Acronis\TrueImageEchoWorkstation>trueimagecmd /asz_files /password:aaa
ASZ size: 5387526144 byte
ASZ free space: 4363010048 byte
FILE name: AAA2.TIB; size: 56414317 byte
type: image, base; creation time: 2/16/2007 3:43:34 PM
type: image, incremental; creation time: 4/25/2007 11:44:47 AM
FILE name: FAAA.TIB; size: 3125550 byte
type: file, base; creation time: 8/22/2006 12:28:40 PM
FILE name: FAAB2.TIB; size: 5147 byte
type: file, base; creation time: 8/14/2007 2:17:45 PM
type: file, incremental; creation time: 8/14/2007 2:19:43 PM
```

In our example, the Acronis Secure Zone contains three archives.

The archive AAA2 (2 stands for number of backups in the archive) consists of:

- full (base) image backup created on 2/16/2007 at 3:43
- incremental backup created on 4/25/2007 at 11:44.

The archive FAAA (F means that this is a file-level archive) contains one base file-level backup.

The archive FAAB2 (B means that this is the second file-level archive in the zone) consists of:

- full (base) file-level backup created on 8/14/2007 at 2:17
- incremental backup created on 8/14/2007 at 2:19.

```
trueimagecmd /filerestore /filename:asz//FAAA
/target_folder:e: /password:aszpw
```

- This will restore files and folders with their original paths from the sole base backup FAAA to the root of partition E.

```
C:\Program Files\Acronis\TrueImageEchoWorkstation>trueimagecmd /filerestore /filename:asz//FAAA /target_folder:e: /password:aaa
[#####] 100%
Operation has succeeded.
```

10. Acronis Secure Zone: deleting backups

```
trueimagecmd /asz_delete_files /password:aszpw  
/filename:FAAB.tib
```

- This will delete the most recent backup in the FAAB archive.

In our example (7), the incremental backup created on 8/14/2007 at 2:19 will be deleted.

The next execution of the same command will delete the base FAAB backup. By continuing with the FAAA and AAA names, you can clear the Acronis Secure Zone except for the last remaining base backup that cannot be deleted.

11. Clone

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

- Clone hard disk 2 to hard disk 3.

12. 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.

16.1.5 ICompGS.exe tool: adding machines to the group server out of a *.txt file

Syntax:

```
ICompGS.exe /filename <path to the file>
```

The names of the machines in the file can be separated by commas, semicolons or carriage returns as follows:

Name_of_machine1, Name_of_machine2, ... , Name_of_machineN

or: Name_of_machine1; Name_of_machine2; ... ; Name_of_machineN

or: Name_of_machine1

 Name_of_machine2

...

 Name_of_machineN

The ICompGS.exe command has to be executed at the same machine where the group server is located, but the named *.txt file can be placed anywhere as long as the ICompGS.exe has access to it.

16.1.6 Ebasrvdb.exe tool: generate an XML file with the backup mapping details

Syntax:

```
EBaSrVDB.exe /filename:<path to the XML file>
```

The purpose of this tool is to provide a way to understand the mapping between a specific backup done on a specific computer at a specific time and the name of the file stored on the backup server. While this information can be useful in case of disaster

recovery, it should not be used to manipulate directly the file stored on the backup server. Doing so may lead to inconsistencies in the backup server management and result in turning the archives unusable through backup server or even directly.

The EBaSrvDB.exe tool has to be executed on the same machine where the Backup Server resides. The generated XML file can be located anywhere as long as the EBaSrvDB.exe tool has the write access to it.

If a file with the same name already exists at the target location, it will be overwritten without any warnings.

16.1.7 Command-line mode usage under DOS

For use in the MS-DOS-compatible environments Acronis True Image Echo Workstation includes the **TrueImageCmdDos.exe** utility which is located in the folder where Acronis True Image Echo Workstation has been installed, by default it is

C:\Program Files\Acronis\TrueImageEchoWorkstation.

16.2 Scripting

16.2.1 Script execution parameters

Scripts are executed by the **TrueImageTerminal.exe** utility located in the Acronis True Image Echo Workstation installation folder (i.e. C:\Program Files\Acronis\TrueImageEchoWorkstation). 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 Echo Workstation 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**.

16.2.2 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 a 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 whether 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.

16.2.3 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>
```