



Acronis[®] Drive Monitor

User's Guide

Copyright © Acronis, Inc., 2000-2010. 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.

VMware and VMware Ready are trademarks and/or registered trademarks of VMware, Inc. in the United States and/or other jurisdictions.

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

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

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

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

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

Third party code may be provided with the Software and/or Service. The license terms for such third-parties are detailed in the license.txt file located in the root installation directory. You can always find the latest up-to-date list of the third party code and the associated license terms used with the Software and/or Service at <http://kb.acronis.com/content/7696>

Table of contents

- 1 Introduction4**
 - 1.1 What is Acronis® Drive Monitor?4
 - 1.2 About S.M.A.R.T. parameters4
 - 1.3 System requirements and supported media5
 - 1.3.1 Minimum system requirements 5
 - 1.3.2 Supported operating systems 5
 - 1.4 Technical support5

- 2 Acronis Drive Monitor installation and startup6**
 - 2.1 Installing Acronis Drive Monitor6
 - 2.2 Extracting Acronis Drive Monitor6
 - 2.3 Running Acronis Drive Monitor7
 - 2.4 Removing Acronis Drive Monitor7

- 3 Using Acronis Drive Monitor7**
 - 3.1 Summary page7
 - 3.2 Disks8
 - 3.2.1 Disk overview 9
 - 3.2.2 S.M.A.R.T. parameters 10
 - 3.2.3 Events 11
 - 3.2.4 Health calculating 11
 - 3.2.5 Using custom script 13
 - 3.3 Backup17
 - 3.4 Critical events19
 - 3.4.1 Critical Events monitoring configuration 20
 - 3.5 Options21
 - 3.5.1 Alerts 21
 - 3.5.2 Temperature monitoring 23
 - 3.5.3 Critical events monitoring 23
 - 3.5.4 Disks monitoring 24
 - 3.5.5 Backup monitoring 24

- 4 Index25**

1 Introduction

1.1 What is Acronis® Drive Monitor?

Acronis Drive Monitor is a free tool available for public download, created to increase customer awareness about the health of their disk drives and to encourage them to back up their data in order to survive a disk failure.

1.2 About S.M.A.R.T. parameters

Self-Monitoring, Analysis, and Reporting Technology, or S.M.A.R.T., is a standard technology, which allows automatic monitoring of a hard disk drive's health. It notifies users about any potential problems with disks, caused by internal or external factors.

Manufacturers, supporting S.M.A.R.T. interface in various products, include: **Samsung, Seagate, IBM (Hitachi), Fujitsu, Maxtor, Western Digital, ExcelStor Technology**, and other vendors.

Each S.M.A.R.T. parameter describes a specific aspect of the disk state: damaged disk's surface, read/write errors, failures of the mechanical subsystem, electronic components failure, etc. Some of S.M.A.R.T. parameters are critical and indicate serious problems, which may lead to a disk failure and, thereafter, a complete data loss.

Below are significant values for each S.M.A.R.T. parameter:

- **Attribute** – includes a S.M.A.R.T. parameter's name, ID and Hex (for example: attribute name – Read Error Rate, attribute ID – 01, Hex – 01);
- **Normalized value** (usually called '**value**') – it can range from 1 to 253 and higher values are better. A manufacturer sets this value of the parameters equal to 100 or 200;
- **Raw offset** - changing this value allows you to adjust the S.M.A.R.T. parameter value, that will be used for disk health calculation (see Health calculation (p. 11)). Raw offset may be either positive or negative depending on your requirements;
- **Threshold** – the lowest acceptable value for a S.M.A.R.T. parameter, set by a manufacturer. When a parameter's value goes lower, than a Threshold, it means a hard disk is in a critical condition and should be replaced, and a user should urgently concern data to be protected. Such a disk may be returned to a manufacturer under warranty ("Threshold Exceeded Condition" situation);
- **Status** – this value indicates an importance and possible danger of the changed parameter's value: it can be critical (decreasing value indicated serious problems), warning (decreasing value may indicate disk's electromechanical problems) and informational (decreasing value does not indicate imminent disk failure).

A S.M.A.R.T. system, integrated into your hard disk, notifies you each time the disk's parameters change. Monitoring S.M.A.R.T. parameters allows you to avoid disk failures, which could be predicted – **up to 70% of all possible crashes!**

But still monitoring S.M.A.R.T. parameters cannot predict all unexpected failures caused by electronic or mechanical problems, which may suddenly occur. This is why it is so important to have an up-to-date backup archive for each disk, that will protect you from data loss.

1.3 System requirements and supported media

1.3.1 Minimum system requirements

The hardware requirements of Acronis Drive Monitor correspond to the minimum requirements for the operating system installed on the computer to be used for running Acronis Drive Monitor. In addition Acronis Drive Monitor requires the following hardware:

- 1024 MB RAM
- Processor Pentium 1 GHz or faster
- Mouse or other pointing device (recommended).

1.3.2 Supported operating systems

Acronis Drive Monitor has been tested on the following operating systems:

- Windows XP (including x64 editions)
- Windows Server 2003 (including x64 editions), SBS 2003 (all releases)
- Windows Server 2008 (including x64 editions), SBS 2008 (all releases)
- Windows Vista (all editions)
- Windows 7 (all editions)

1.4 Technical support

Users of Acronis Drive Monitor are entitled to free technical support at Acronis Discussion Forums. If you experience problems installing or using Acronis Drive Monitor that you can't solve yourself by using this guide, you can also view related articles in Acronis Knowledge Base.

2 Acronis Drive Monitor installation and startup

2.1 Installing Acronis Drive Monitor

To install Acronis Drive Monitor:

- Run the Acronis Drive Monitor setup file.
- In the **Install Menu**, click on the **Install Acronis Drive Monitor** to launch the installation procedure. Follow the install wizard instructions on the screen.
- Read and accept the Acronis Drive Monitor license agreement.
- Specify where to install the tool: click **Browse...** button and select the location. Also select whether you want to install it for all users sharing this machine, or only for the current user.
- To make sure there is enough of free space for installing Acronis Drive Monitor, click **Disk usage...** button, which opens a window with a list of hard drives and their disk space usage information. Click **Close** to return to the install wizard.



2.2 Extracting Acronis Drive Monitor

When installing Acronis Drive Monitor, you also can select **Extract installation files** from the install menu to save the setup (.msi) file on a local or network drive and run the installation process later. This will help when modifying or recovering the existing component installation.

To extract Acronis Drive Monitor:

- Run the Acronis Drive Monitor setup file.
- Select **Extract installation files** from the install menu.
- Select a component - Acronis Drive Monitor.
- Specify where to extract the file: click **Browse...** button and select the location.

- To make sure there is enough of free space for extracting and installing Acronis Drive Monitor, click **Disk usage...** button, which opens a window with a list of hard drives and their disk space usage information. Click **Close** to return to the install wizard.
- Click **Extract**.

2.3 Running Acronis Drive Monitor

You can run Acronis Drive Monitor in **Windows** by selecting **Start** → **Programs** → **Acronis** → **Acronis Drive Monitor** → **Acronis Drive Monitor** or by clicking on the appropriate shortcut on the desktop.

2.4 Removing Acronis Drive Monitor

Select **Start** → **Settings** → **Control panel** → **Add or remove programs** → **Acronis Drive Monitor** → **Remove**. Then follow the instructions on the screen. You may have to reboot your computer afterwards to complete the task.

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

3 Using Acronis Drive Monitor

This chapter describes the main features of the Acronis Drive Monitor.

3.1 Summary page

The first page to be opened is a **Summary** page, where the current state of disks, available backup archives and other options are displayed.

When your disks do not experience any hardware problems and your data is protected with recent backups for all monitored disks, you will see green icons at each section on the right. Yellow icons warn you about non-critical problems with the disks, reported by S.M.A.R.T. or a custom script (p. 13).

The red icons alarm you about critical problems with your hard drives. This means a critical parameter's value decreased below the threshold and indicates an imminent drive failure.

In case disks and/or backups are not monitored, corresponding icons (as well as tray icons) will be grayed out.

To view detailed information and change settings you can click on the links in the end of each section:

Disks

The **Disks** section shows brief information on your hard disks state, if they are being monitored by Acronis Drive Monitor.

Drive monitoring checks hardware parameters, such as temperature, head stability, spin-up time, etc. (see S.M.A.R.T. parameters (p. 4) article for details).

When all your disks are being monitored and no hardware problems were detected, the status icon on the right will show OK status.

This section may also reflect a warning message in case there are disks, which are not monitored.

Click **Show disks** link to go to a Disks page, where you can view for more detailed information, enable/disable monitoring and change other settings if required.

Backup

The **Backup** section informs you whether your data is protected with recently created backup archives.

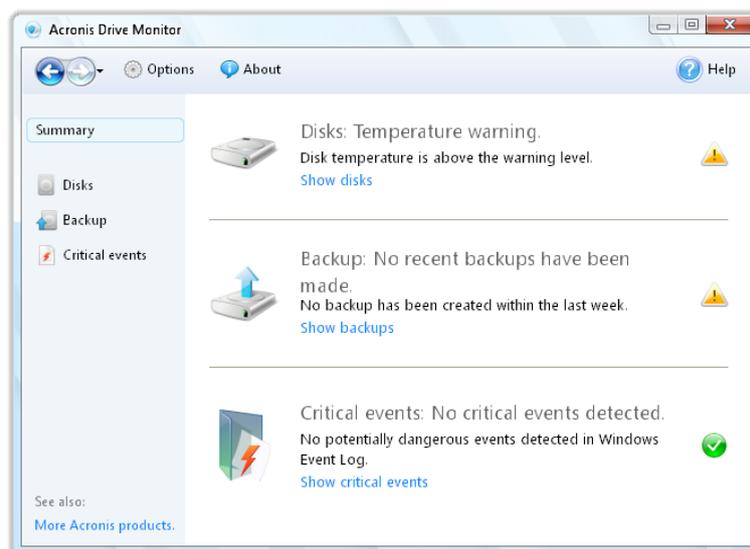
For the proper functioning you need a newer Acronis backup software to be installed on your computer. In case no backup software is detected, you will be invited to Acronis web site.

Click **Show backups** link to go to a Backup page, where you can view for more detailed information and change backup monitoring settings if required.

Critical events

The **Critical events** section displays a list of messages, reported by **Windows Event Log**, which are considered critical by Acronis Drive Monitor. To customize logs displaying to your needs, you will need to create a script - see Critical Events monitoring configuration (p. 20) article for more information.

To view the detailed problem description, click the **Show critical events** link, which will take you to the Critical events (p. 19) page.



3.2 Disks

Disk health is monitored through S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) interface. If a disk does not support S.M.A.R.T., a custom script may be used for monitoring. Click the link below to configure monitoring options - this will lead you to the **Options (p. 21)** page, where you can specify the required program behavior.

Available disks

The table displays all disks in your computer. It reflects brief details about manufacturer and model, capacity, volumes and common health status.

The colored health status reflection makes it easier to recognize at-a-glance which disk may be at risk.

When a health status decreases, look at the S.M.A.R.T. parameters' values to research where a problem may appear.

By default the first hard disk is selected and its details are displayed in the table. To view other disks' information, select it in the table.

Running Acronis Drive Monitor on a virtual machine.

While using Acronis Drive Monitor on a virtual machine, disks monitoring should be **disabled** due to the following reasons:

- virtual disks do not report useful information about your computer's physical disks' states, so disks monitoring and health calculating do not make sense anyway;
- the calculated virtual disk's health may spontaneously change from 100% to 0, and then back to 100%, because VMware virtual disk reports some S.M.A.R.T. parameters in a special way: it reports the parameter's value decreased below the threshold, which is considered by S.M.A.R.T. interface as a potential hardware problem that affects the overall disk health status.

3.2.1 Disk overview

The **Disk overview** tab reflects the state of the most important values and parameters of the selected disk. This is an informational tab, and to view and/or change settings go to the **Options (p. 21)** page.

Monitoring

Acronis Drive Monitor allows monitoring your disks conditions using S.M.A.R.T. or previously created custom scripts. To change the monitoring mode, go to the **Options** page and click the link near the required disk. See details in the **Options (p. 21)** chapter.

Power on time

This line shows how long the selected disk is being powered on. By default days are counted.

Disk health

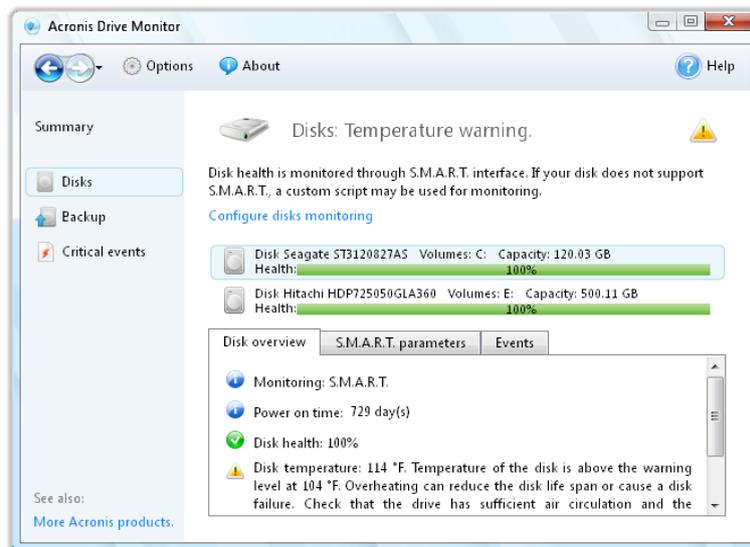
The hard disk health is expressed as a percentage.

Also the disk health status is displayed using an icon with a specific color:

-  - your hard disk is running normally;
-  - some problems with the disk, which actually will not lead to a data loss, were detected;
-  - serious problems are detected or a disk failure is predicted, it is strongly recommended to take actions to protect your data;
-  - the disk is not monitored: monitoring is disabled by the user or is not available.

Disk temperature

The hard disk temperature is displayed in *Centigrade* or *Fahrenheit* depending on your settings.



3.2.2 S.M.A.R.T. parameters

This tab contains a table with S.M.A.R.T. parameters, available for our hard drive (this list depends on the hardware manufacturer).

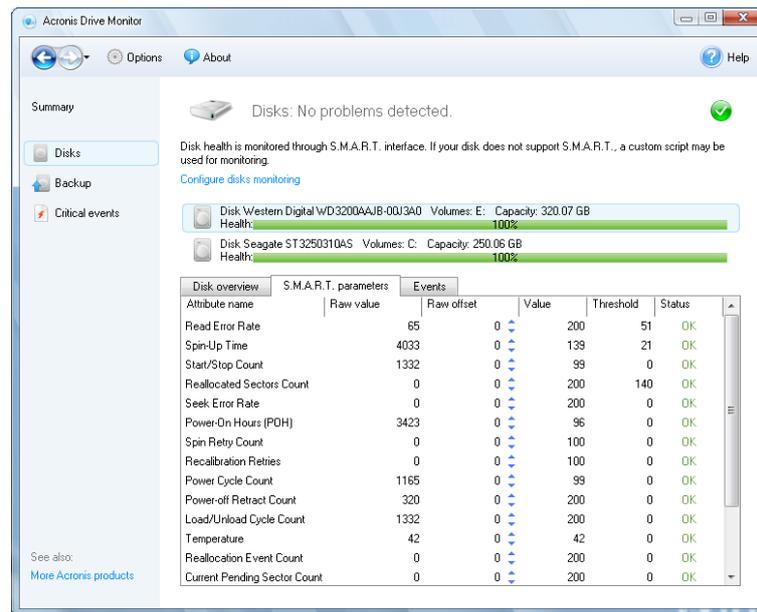
Each line shows the parameter name, its current value, threshold (the lowest limit set by the manufacturer) and the common status.

You may right-click any column name to view and change values to be displayed in the table.

Right-click a parameter and select one of the menu items:

- **Knowledge base...** - select this item to view the information on the selected S.M.A.R.T. parameter;
- **Copy entire page to clipboard** - select this item in case you need to copy and save displayed information;
- **Ignore parameter** - select this item to disable parameter-specific error messages, though the parameter still will be monitored and its values will be displayed in gray. It is not recommended to use this feature for critical parameters;

- **Reset to default** - select this item to cancel all changes you have made before (ignored parameters, changed Raw offset values).



3.2.3 Events

The **Events** tab contains a table with event logs. It shows which S.M.A.R.T. parameter has changed, its previous and new values.

Double click will open a window with the detailed information on the event.

3.2.4 Health calculating

Why calculating a disk's health status?

- The calculated hard drive's health shown as percentage provides you a better visual representation of S.M.A.R.T. related problems
- A health status warns you of a disk degradation, when S.M.A.R.T. reports a problem
- This will help you to protect your data before your disk's failure.

How to calculate a disk's health?

Critical parameters:

Initially a hard disk has 100% health condition.

All S.M.A.R.T. parameters considered by Acronis Drive Monitor as critical for a hard drive (if they are available for monitoring, it depends on the manufacturer), decrease the health of your disk. Such attributes have a predefined weight and a maximum limit value (see a Table 1 below).

A limit defines how much the attribute may decrease an overall health value. A weight of an attribute defines how important the parameter's value decreasing affects the disk's health.

The overall disk health is calculated by a formula below:

$$\text{Disk health (\%)} = \Pi (100\% - (\min(\text{limit}, \text{attribute_value} * \text{Weight})))$$

where:

100% - an initial health of a disk;

Π - the product of minimums from (limit, attribute_value*Weight) - calculated for each critical S.M.A.R.T. parameter;

Weight - a weight of each critical S.M.A.R.T. parameter (see a Table 1 below);

limit - a limit of each critical S.M.A.R.T. parameter (see a Table 1 below);

attribute_value - a current parameter's value.

Example:

1. Soft Read Error Rate = 30 (attribute value), weight = 1, limit = 20;
2. Spin Retry Count = 12(attribute value) , weight = 2, limit = 50.

So in this case the disk's health is calculated as the following:

$$\text{Disk health} = (100\% - (\min(30 * 1, 20))) * (100 - \min(12 * 2, 50)) = 80\% * 76\% = 60.8\% \approx 61\%$$

The following table contains the health related (critical) S.M.A.R.T. attributes affecting the health value with their weights and maximum limits.

Table 1.

Attribute ID	S.M.A.R.T. attribute	Weight	Limit %
05	Reallocated Sectors Count	2	70
10	Spin Retry Count	2	50
184	End-to-End Error	1	50
196	Reallocation Event Count	1	40
197	Current Pending Sectors Count	1	40
198	Off-Line Uncorrectable Sectors Count	2	70
201	Soft Read Error Rate	1	20

Not critical parameters:

Other S.M.A.R.T. parameters, which have a predefined by manufacturer Threshold value, also affect a disk's health: after decreasing below the threshold, this parameter subtracts 10% from the **current** disk health. This means, when the current health is 90%, **9%** will be subtracted.

A Table 2 shows non-critical S.M.A.R.T. parameters, that affect a disk health.

Table 2.

Attribute ID	S.M.A.R.T. attribute
01	Raw Read Error Rate
02	Throughput Performance
03	Spin Up Time
04	Start/Stop Count
07	Seek Error Rate
08	Seek Time Performance
09	Power-On Time Count
12	Drive Power Cycle Count
221	G-sense Error Rate
228	Power off Retract Cycle
225	Load/Unload Cycle Count
194	Disk Temperature
199	Ultra ATA CRC Error Count
193	Load/Unload Retry Count

What else may decrease a disk's health?

When a disk is monitored using a custom script:

- **exit code is 0** : Health = (disk health calculated by S.M.A.R.T.) * 100%
- **exit code is 1** (warning) : Health = (disk health calculated by S.M.A.R.T.) * 50%
- **exit code is 2+** : Health = 0%

Factors not affecting a disk health

- Decreasing value of a non-critical parameter does not affect the disk health till it is above a threshold, specified by the disk's manufacturer;
- Event log entries also do not change the overall disk health, but still can generate *Warnings* or *Errors*.

3.2.5 Using custom script

If any of your hard drives does not support S.M.A.R.T. for monitoring, you can create a custom script.

Each hard disk needs a separate custom script. On an **Options (p. 21)** page you may select a required script for a drive in a **Disk monitoring (p. 24)** section.

The executable's output will be returned through the exit code and recorded to the respective log entry.

Executed custom script provides a report about disk status:

0 - there are no errors and warnings, the disk is healthy;

1 - electromechanical problems occurred, the disk needs to be checked to avoid possible failure in the future;

2 - error: there is serious problem with the disk, it needs urgent data backup and, probably, hardware replacement.

Below is a sample of a custom script applicable for Intel(R) RAID controllers using Intel(R) CmdTool2 v5.00.11:

```
@echo off
```

```
setlocal
```

```
echo Sample ADM custom script for Intel(R) RAID controllers using Intel(R) CmdTool2 v5.00.11
```

```
echo Copyright (c)Acronis, 2000-2010 All rights reserved
```

```
echo.
```

```
echo.
```

```
echo Controller information
```

```
echo.
```

```
set critical_disks=0
```

```
set failed_disks=0
```

```
::CmdTool2 -AdpAllInfo -aAll
```

```
for /f "tokens=1-10" %%a in ('CmdTool2 -AdpAllInfo -aAll ^| findstr "Product Serial Critical Failed") do
```

```
(
```

```
if %%a==Product (
```

```
echo Model: %%d %%e %%f %%g %%h
```

```
)
```

```
if %%b==No (
```

```
echo Serial number: %%d
```

```
)
```

```
if %%a==Critical (
```

```
if %%b==Disks (
```

```
echo Critical disks: %%d
set /a critical_disks=%%d
)
)
```

```
if %%a==Failed (
if %%b==Disks (
echo Failed disks: %%d
set /a failed_disks=%%d
)
)
```

```
)
```

```
echo.
echo Physical devices information
echo.
```

```
set error_count=0
```

```
::CmdTool2 -PDList -aALL
```

```
for /f "tokens=1-4" %%a in ('CmdTool2 -PDList -aALL ^| findstr "Error Adapter Slot"') do (
```

```
if %%a==Adapter (
```

```
echo %%a %%b
```

```
echo ***
```

```
)
```

```
if %%a==Slot (
```

```
echo Device on slot %%c
```

```
)
```

```
if %%a==Media (  
set /a error_count+=%%d  
echo Media error count: %%d  
)
```

```
if %%a==Other (  
set /a error_count+=%%d  
echo Other error count: %%d  
echo.  
)  
)
```

```
echo ***  
echo.
```

```
set /a ret_code_ok=0  
set /a ret_code_warning=1  
set /a ret_code_critical=2
```

```
set ret_code=%ret_code_ok%
```

```
if %failed_disks% gtr 0 (  
echo Alert! Failed disks found!  
set /a ret_code=%ret_code_critical%  
)
```

```
if %critical_disks% gtr 0 (  
echo Alert! Disks with critical state found!  
set /a ret_code=%ret_code_critical%  
)
```

```
if %error_count% gtr 4 (  
    echo Alert! Errors found on some devices!  
    set /a ret_code=%ret_code_critical%  
    ) else (  
    if %error_count% neq 0 (  
        echo Warning! Errors found on some devices!  
        set /a ret_code=%ret_code_warning%  
        ) else (  
            echo All devices are running normally  
            set /a ret_code=%ret_code_ok%  
        )  
    )  
    echo exiting with return code %ret_code%  
  
exit %ret_code%
```

If you have any questions concerning custom scripts, please refer to Acronis Discussion Forums.

3.3 Backup

Although S.M.A.R.T. is a powerful technology, that is able to predict about 60-70% of hard disk failures, some kinds of crashes occur unexpectedly.

Your computer may experience electromechanical problems, or it even can be stolen. In this case only up-to-date backup archives protect you from drastic data loss and allow you to recover the data quickly and easily, eliminating hours or days of work trying to rebuild your disk drive's data and applications.

Acronis Drive Monitor supports integration with Acronis products, such as Acronis True Image Home Update 2 or higher and Acronis Backup & Recovery Update 2 or higher, and monitors the backup archives availability for all disks/partitions on your computer. You can launch backup tasks directly from Acronis Drive Monitor interface.

Acronis Drive Monitor will search for the installed backup software and previously created archives when backup monitoring is enabled. Depending on the search result you will see a table with a list of disks and backup details or a page with information on Acronis backup software.

This page displays the backup archives availability for all hard disks and partitions in your computer.

Backup software is available:

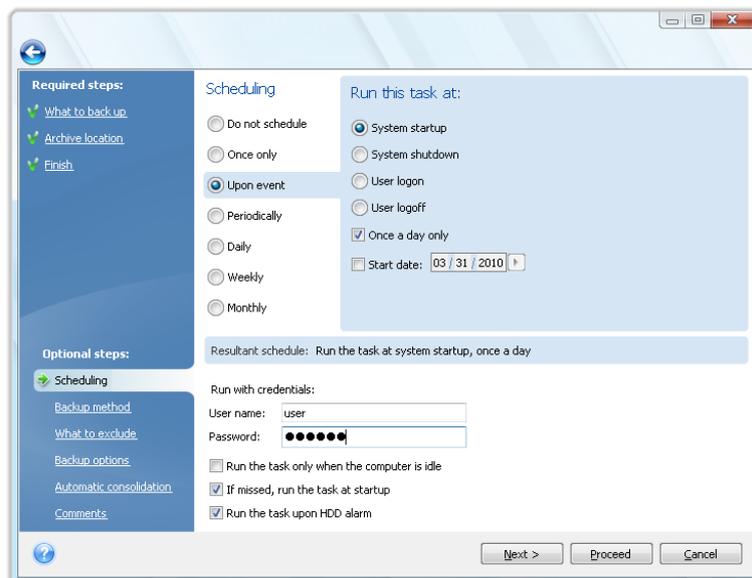
If a backup software is available on your computer, the table below shows a list of existing disks/partitions, creation time of the last backup of this disk/partition and its status (succeeded or failed).

Clicking **Configure backup monitoring** link will lead you to the Options (p. 21) page, where you can enable/disable backup monitoring behavior.

You may also select other software for monitoring or choose not to monitor backup status at all, but this is not recommended for your disks safety.

Click **Backup now...** button to run the backup software, installed on your computer. Also you may right-click on a volume from the table if you decide to back up particular disk/partition.

Also you may schedule running backup tasks from Acronis in case Acronis Drive Monitor reports about a potential problem with one of the hard disks. To do this, select **Run the task upon HDD alarm** check box when creating a backup task using the Acronis software, installed on your computer.



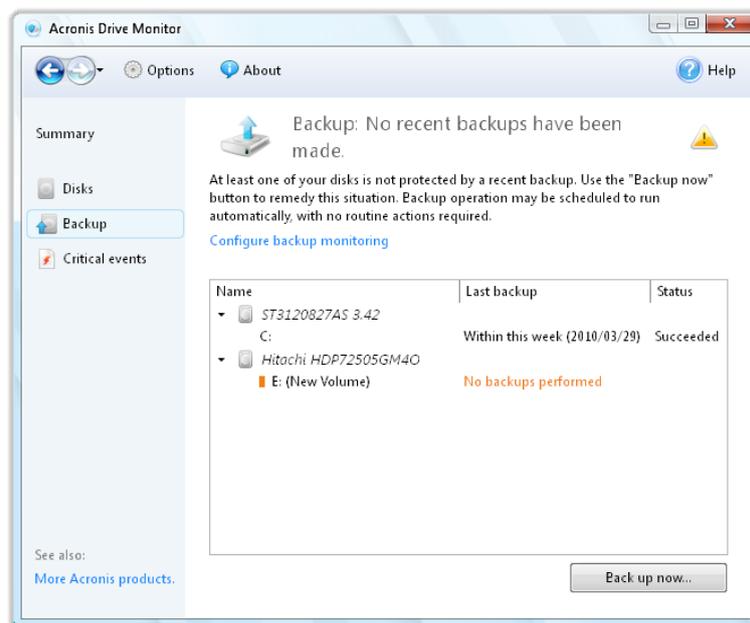
If older versions of Acronis products are installed on your computer, backup archives availability will be monitored, but you will need to run backup tasks manually from the console to obtain ut-to-date backups.

Backup software is not detected:

Acronis products, such as Acronis Backup & Recovery and Acronis True Image Home provide you with all the essential tools you need to recover your computer system should a disaster occur, such as losing data, accidentally deleting critical files or folders, or a complete hard disk crash. These products are easy to download and install. User friendly wizards and a **Windows Vista**-style interface will make your work easier.

Click **Download Acronis Software** to purchase Acronis products or download a trial version from our web site.

You may disable notifications about unavailable backups, thus they will not be displayed on the Summary page.



3.4 Critical events

Acronis Drive Monitor informs you in case of a dangerous event and allows viewing its working logs.

Critical events page displays only potentially dangerous events for data safety caused by changes of critical parameters. Some **Windows** events, such as errors related to the file system or storage drivers, can appear before more significant problems, such as file system corruption arise.

You may sort displayed events by date, risk, severity, source or by event ID.

Double-clicking on a required event opens a window with event's detailed information.

Right-click on any event to open a menu, where you can select the following items:

- **Details...** - select this item (or double-click the entry) to view detailed information on the selected event;
- **Knowledge base** - select this item to view the information on the selected event;
- **Export** - select this item to export the event message to another program;
- **Ignore once** - select this item to ignore an event only once in particular case (with a certain date and time), for example in case when a problem had been already fixed and does not affect the overall disk status any more);
- **Ignore always** - select this item to place this event to a **Windows Event Log** monitoring configuration file (see Critical Events monitoring configuration (p. 20) article for detailed information). But note, to start displaying this even again, you need to delete it from a script file manually;
- **Reset to default** - select this item if you want messages about **all** critical events to be listed in the table - the `<exclude_filter>` section in the XML file (see Critical Events monitoring configuration (p. 20) article) will be empty.

Event details window

Event details page shows all data and description concerning the selected event. Up and down arrow buttons on the right allow moving up and down in the list of events not quitting back to the main program area.

In the bottom of the page there is a link to an Acronis Knowledge Base web site. To provide you the better and early support, our team needs the complete system information.

To send the details you need to confirm the feedback.

3.4.1 Critical Events monitoring configuration

Acronis Drive Monitor allows you to specify which events from **Windows event logs** will be considered as critical for hard disks; and then the program will inform you **only** about such events in the **Critical events** page. You can change **Windows Event Log** monitoring configuration file for System and Application **Windows logs**.

To configure them you need to change a XML file (*winlog_filter.xml*) (*Exclude* and *Include* parts of the file have the same format, so you can specify them in the same file), which is located in **C:\ProgramData\Acronis\Drive Monitor** (for **Windows Vista/Windows 7**) or **C:\Documents and Settings\All Users\Application Data\Acronis\Drive Monitor** (for other **Windows** operating systems).

For example, if you want to add monitoring of event 51 from source *Disk1* and to mark it as *High risk*, add the following line to "High risk" section:

```
<parameter source_name="Disk1" event_code="51" />
```

Argument values:

SourceName | Category | Type | EventCode | Message

Operation values:

contain | equal | more | less

Below is an example of a file with configuration for logs:

```
<?xml version="1.0" encoding="UTF-8" ?>
<filter_root>
  <!-- String parameters: -->
  <!-- argument = source_name/message -->
  <!-- operation = contain/equal -->
  <!-- Integer parameters: -->
  <!-- argument = category/type/event_code -->
  <!-- operation = equal/more/less -->
```

```
<!-- value for type = {NONE = 0, ERROR = 1, WARNING = 2, INFORMATION
= 3,
          SECURITY_AUDIT_SUCCESS = 4, SECURITY_AUDIT_FAILURE = 5} --
>
```

```
<include_filter risk="High">
  <!-- Conditions in tag 'parameter' are Logical AND-->
  <parameter argument="source_name" operation="contain" />
  <parameter argument="message" operation="equal" value="Achtung" />
</include_filter>
```

```
<!-- Conditions in individual tag 'include_filter' are Logical OR-->
<include_filter risk="Low">
  <parameter argument="event_code" operation="equal" value="6011" />
</include_filter>
```

```
<exclude_filter>
  <!-- Conditions in individual tag 'parameter' are Logical OR-->
  <parameter source_name="W32Time" event_code="35" />
</exclude_filter>
</filter_root>
```

3.5 Options

The **Options** page allows you to adjust the desired settings for the following actions (click the Down arrow icon on the right to open the respective menu):

- Alerts (p. 21) - configure receiving e-mail notifications and regular reports;
- Temperature monitoring (p. 23) - specify a critical or warning temperature;
- Critical events monitoring - enable/disable monitoring of critical events;
- Disks monitoring (p. 24) - configure disks monitoring settings;
- Backup monitoring (p. 24) - configure backups monitoring.

3.5.1 Alerts

When configured, Acronis Drive Monitor will notify you when problems are detected. Alerts may be delivered via e-mail. To provide an e-mail addresses or change details, click **Change settings...** link (see E-mail parameters (p. 22) section for details).

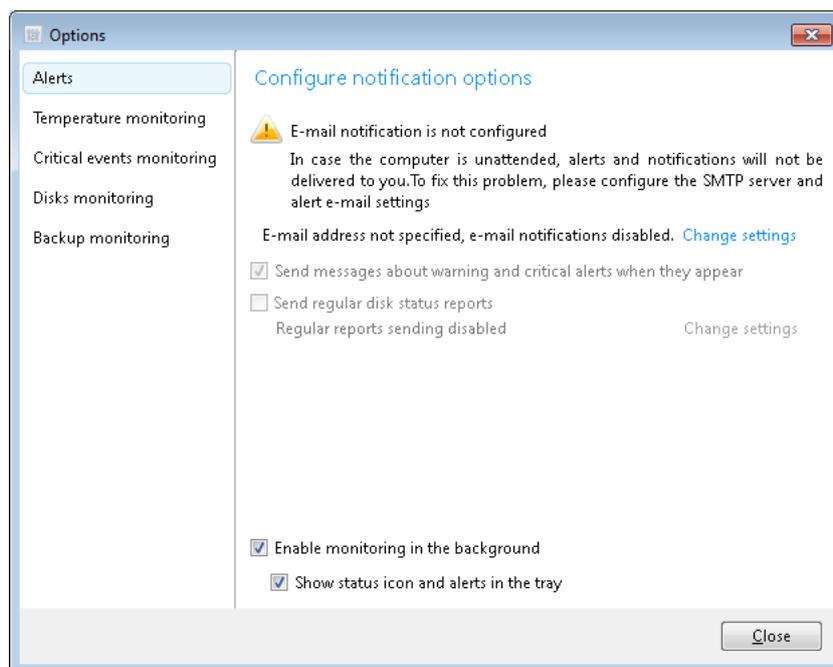
Acronis Drive Monitor allows you to select when and how often to receive reports:

- You may receive messages when a **critical event/warning** appears. Such messages will be sent when a problem occurs, and no new alerts will be sent until a system status is restored to OK, or a problem becomes more serious for the disk. This option is enabled by default.
- You may receive **regular disk status reports** with specified periodicity (see Regular reports schedule (p. 23) section for details).

Acronis Drive Monitor allows running monitoring process in the background. With the corresponding check box in the bottom of the page selected, scheduled tasks will continue running after you exit the program, e.g. when monitoring in the background is disabled, scheduled tasks will not run while the console is closed. This option is selected by default.

You can also specify whether you want a status icon to be shown in the tray while monitoring in the background (enabling this option is available only with **Enable monitoring in the background** selected).

Click **Close** when finished.



3.5.1.1 E-mail parameters

For receiving alert messages about any issue, happened with your disks, you need to specify the default e-mail account.

- Fill in **E-mail address** and **From** fields. You may also specify several addresses, separating them by commas.
- Provide the outgoing SMTP server name and port. A user name and a password might also be needed if the SMTP server requires user authentication. If the outgoing SMTP server requires logging on to an incoming mail server before it allows sending outgoing messages, enter the necessary information for the incoming mail server.
- Select **Use encryption** check box and select a cryptographic protocol for the safer communication over the network (SSL or TLS).

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

Click **OK** to save changes and return to the **Options** page.

3.5.1.2 Regular reports schedule

You can specify a schedule for regular disk status reports.

Such report contains all information on your disks, including a monitoring mode, health, temperature, S.M.A.R.T. parameters degradation, if any, and detected alerts. Acronis Drive Monitor also will inform you about the hard drive failure, that may occur soon.

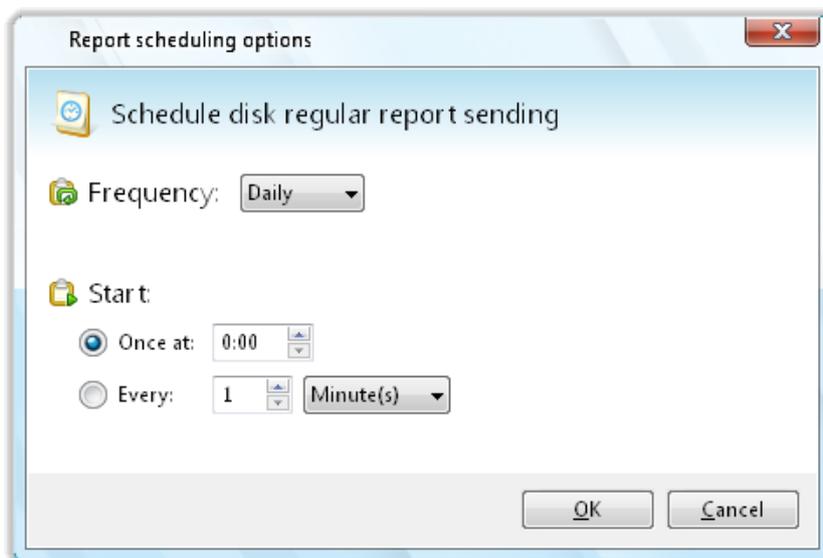
The second part of the report will contain results of **Windows event log** monitoring.

Select the **Frequency** (daily or weekly). By default reports will be sent once a day.

Also you can set up start parameters for sending reports:

- **Once at:** (hours and minutes) - set the time, when the report will be sent. Enter hours and minutes manually, or set the desired start time, by using the up and down buttons.
- **Every:** - specify the time (minutes or hours) between generation and sending reports. For example, if you entered 40 minutes, the report will be sent every 40 minutes after the previous report was sent.

Click **OK** to save changes and return to the **Options** page.



3.5.2 Temperature monitoring

Temperature is a parameter, monitored by S.M.A.R.T. only. This monitoring is enabled by default.

The temperature may be displayed in Centigrade or Fahrenheit. You can switch a temperature scale in **Regional and Language Options** in your operating system.

You may set a warning and/or critical disk temperature manually. By default these values are set by manufacturers to 42 C and 52 C respectively (107 F and 125 F).

3.5.3 Critical events monitoring

By default **Critical events monitoring** is enabled.

To specify the events, which you want to be informed about, you can change the monitoring configuration - see Critical Events monitoring configuration (p. 20) article.

Clicking **Reset to the original settings** link will reset exclude filters, that were specified in *winlog_filter.xml* (all user's changes will be lost; to return filtering back, you will have to change the file manually), so after confirming this, messages about **all** critical events will be listed in the table.

3.5.4 Disks monitoring

Here you can see a list of all disks and their properties. To change the monitoring method, click the link near the required disk.

In Defining disk monitoring method window select the way you want to monitor this disk - using S.M.A.R.T. parameters or a custom script (select it by clicking Browse button). A custom script may be used in case you need to monitor a disk with uncommon parameters. See Using custom script (p. 13) section for more information.

Click **Close** when finished.

3.5.5 Backup monitoring

Backup monitoring configuration page contains a list of all disk and volumes that are present in your system.

Here you can enable or disable backup monitoring separately for each disks/partitions.

- To disable backup monitoring for an individual volume, click on **Disable** link against the volume chosen. When disabled, the volume becomes grayed out, and the link changes to **Enable**.
- To enable backup monitoring for a volume, click on **Enable** link.

To disable backup monitoring globally for your system, simply disable it for every individual volume.

When no volumes with monitoring enabled left, overall backup monitoring status becomes disabled.

4 Index

A

- About S.M.A.R.T. parameters • 4, 7
- Acronis Drive Monitor installation and startup • 6
- Alerts • 21

B

- Backup • 17
- Backup monitoring • 21, 24

C

- Critical events • 8, 19
- Critical events monitoring • 23
- Critical Events monitoring configuration • 8, 19, 20, 24

D

- Disk overview • 9
- Disks • 8
- Disks monitoring • 13, 21, 24

E

- E-mail parameters • 21, 22
- Events • 11
- Extracting Acronis Drive Monitor • 6

H

- Health calculating • 4, 11

I

- Installing Acronis Drive Monitor • 6
- Introduction • 4

M

- Minimum system requirements • 5

O

- Options • 8, 9, 13, 18, 21

R

- Regular reports schedule • 22, 23
- Removing Acronis Drive Monitor • 7
- Running Acronis Drive Monitor • 7

S

- S.M.A.R.T. parameters • 10
- Summary page • 7
- Supported operating systems • 5
- System requirements and supported media • 5

T

- Technical support • 5
- Temperature monitoring • 21, 23

U

- Using Acronis Drive Monitor • 7
- Using custom script • 7, 13, 24

W

- What is Acronis® Drive Monitor? • 4