Acronis Privacy Expert Suite 7.0

User's Guide

Acronis

Compute with confidence

www.acronis.com

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.

END-USER LICENSE AGREEMENT

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

The Acronis Privacy Expert Suite (the Software) is Copyright © SWsoft, 2000-2003. All rights are reserved. The ORIGINAL PURCHASER is granted a LICENSE to use the software only, subject to the following restrictions and limitations.

1. The license is to the original purchaser only, and is not transferable without prior written Permission from SWsoft.
2. The Original Purchaser may use the Software on a single computer owned or leased by the Original Purchaser. You may not use the Software on more than a single machine even if you own or lease all of them without the written consent of SWsoft.
3. The Original Purchaser may not engage in, nor permit third parties to engage in, any of the following:

A. Providing or permitting use of or disclosing the Software to third parties.

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

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

D. Attempting to un-assemble, de-compile or reverse engineer the Software in any way.

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

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

G. Making telecommunication data transmission of the software.

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

ENTIRE RISK

THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE SOFTWARE IS WITH YOU THE PURCHASER. SWSOFT DOES NOT WARRANT THAT THE SOFTWARE OR ITS FUNCTIONS WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR FREE OR THAT ANY DEFECTS WILL BE CORRECTED. NO LIABILITY FOR CONSEQUENTIAL DAMAGES - IN NO EVENT SHALL SWSOFT OR ITS VENDORS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR THE LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE, EVEN IF SWSOFT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Table of Contents

Introduction

What is Acronis Privacy Expert Suite?

It is an integrated software suite that **provides confidentiality and protects** standalone PCs or machines connected to the Internet.

The following capabilities of Acronis Privacy Expert Suite ensure PC confidentiality:

- PC hard disk and any Windows partitions **clean-up of any traces of user actions**
- **Unwanted pop-up ad blocking** for convenient Web browsing
- **Clean-up of spyware** that secretly operates on a user's PC
- **Guaranteed confidential data destruction** on selected hard disks or disk partitions

Unlike other software, Acronis Privacy Expert Suite fully removes evidence of PC usage through the use of guaranteed data destruction methods.

It also increases PC performance by cleaning out temporary files.

Why is it necessary to keep PC work confidential?

Working with a PC creates a number of serious security problems for users:

- You have created and deleted multiple files on your computer. You do not want anyone to view its contents. But is a deleted file really gone? No! The problem is that deleted files can be easily recovered under the Windows operating system to gain access to information a user would like to conceal.
- Windows and the most widely used browsers, Internet Explorer and Netscape Navigator, **provide very weak protection on** keeping trace Internet data private.
- While working with a PC, you leave thousands of bytes of **evidence showing your actions** (records in various system files) you don't even know about.
- While installing software on your PC, you might unknowingly install programs that secretly change system settings, collect and transfer personal information to external addresses, and perform other unwanted and uncontrollable actions.
- When replacing your old hard drive with a new, higher-capacity one you, unwittingly leave lots or important and confidential information on the old drive that can be recovered even if you have reformatted it.

Acronis Privacy Expert Suite provides a solution to all of these problems. It assures complete confidentiality of your PC and Internet actions and prevents situations that threaten your computer and general security.

Standards of guaranteed destruction of confidential information

The software offers the guaranteed destruction of confidential information on hard disk drives with the help of special methods.

Acronis methods guarantee compliance with most national standards:

- American: U.S. Standard, DoD 5220.22-M
- American: NAVSO P-5239-26 (RLL)
- American: NAVSO P-5239-26 (MFM)
- German: VSITR
- Russian: GOST P50739-95

Besides methods corresponding to national standards, Acronis supports predefined methods proposed by widely known and authoritative specialists in the field of information security:

- Peter Gutmann's method – data on hard disk is destroyed with 35 passes
- Bruce Schneier's method – data is destroyed with 7 passes

The suite also supports simple but fast methods for information destruction that zero all sectors on a single hard disk pass.

Another major feature of this version is the opportunity for you to create your own methods for **data destruction.**

Detailed information on data destruction standards is given in Appendix A «Hard Disk Wiping methods» to the current guide.

What's new in Acronis Privacy Expert Suite 7.0?

Acronis Privacy Expert Suite has lots of new features that make it an **integrated software suite.** They include:

- Spyware clean-up
- Guaranteed data destruction on selected hard drives and partitions
- Pop-up blocking for convenient Web surfing
- Selected e-mail deletion in Microsoft Outlook and Outlook Express along with contact list and address book clean-up
- Browsed URLs clean-up
- Forms autocomplete and password lists clean-up
- Convenient paging file clean-up wizard
- Quick user files and folders clean-up through Windows Explorer interface or context menu
- Software actions logging

Additionally, improvements have been made to provide even more convenience in Acronis Privacy Expert Suite.

What Acronis Privacy Expert Suite enables you to clean up

The suite enables you to remove the evidence of your work **in any Windows section.** It allows you:

- to remove Windows **registry** backups that retain evidence of a user's work with PCs and the Internet
- to delete **temporary files** from standard Windows folders
- to delete custom folders/files from any disks connected to a PC
- to clean the Windows **Recycle Bin**
- to clean hard disk **free space**
- to clean the opened/saved files history
- to remove **evidence** from the Find Files list and Find Computers list
- to clean the **Internet cache**
- to delete **cookies**
- to delete downloaded **components**
- to clean up the **Last Visited Pages** and **Typed URLs lists**
- to delete **forms autocomplete and password lists** for Web sites that require authorization
- to delete **e-mail messages** in Microsoft Outlook and Microsoft Outlook Express and clean up the **contacts and address book lists**
- to block unwanted **pop-up ads**
- to **destroy securely** all data on hard disks or partitions, if needed
- to remove secretly operating **spyware** threats
- to clean up the Windows **paging/swap file**

Acronis Privacy Expert Suite **permanently** removes evidence of user PC activity. To clean up a PC, Acronis Privacy Expert Suite **strict methods for guaranteed confidential data destruction** that meet and/or exceed most national/state standards (see Appendix A «Hard Disk Wiping methods» for details).

On the contents of the guide, or how to find the necessary information

This user's guide contains the following main chapters:

- Chapter 1«Installing Acronis Privacy Expert Suite» — contains detailed information about the installation of this software suite.
- Chapter 2 «Working with Acronis Privacy Expert Suite»— describes common principles and settings of the software.
- Chapter 3 «Complex PC clean-up»:

  If you need to perform a **comprehensive clean-up of all PC partitions**, see the section 3.1 «Entire PC clean-up»

If you need to perform a **comprehensive system clean-up**, see the section 3.2 «System clean-up»

If you need to remove **Web activity traces only**, see the section 3.3 «Internet clean-up».

If you need to perform a comprehensive spyware clean-up, see the section 3.4 «Complete spyware clean-up».

- If you need to quickly clean up particular Windows components (partitions), see Chapter 4 «Separate PC components clean-up».
- Chapter 5 «Acronis Privacy Expert Pop-up Blocker» is dedicated to the pop-up ad tool included in Acronis Privacy Expert Suite.
- Chapter 6 «Acronis Drive Cleanser» provides tools for guaranteed data destruction on selected drives or partitions.
- Appendix A «Hard Disk Wiping methods» — contains more detailed information about **used methods of guaranteed confidential data destruction** on PC hard disk.

System requirements

- To take full advantage ofAcronis Privacy Expert Suite, you should have:
- a PC-compatible computer with a Pentium CPU or equivalent
- 32 MB RAM
- a floppy or a CD-RW drive
- VGA monitor
- a mouse (recommended)
- Microsoft Windows 95/98/Me/NT/2000/XP
- Microsoft Internet Explorer 4.0 or higher for correct Pop-up Blocker operation

Software use conditions

The conditions for use of Acronis Privacy Expert Suite are listed in the supplied «License Agreement». To be able to prove that you legally purchased and use the suite, you received a registration card along with the package. Each registration card has a unique number.

Based on current legislation, the «License Agreement» is considered as a contract between user and software vendor. Violation of the contract may lead to prosecution.

Illegal use or distribution of software a violation of the law and will be prosecuted.

Technical support

Users that have legally purchased and registered their copy of Acronis Privacy Expert Suite will receive free **e-mail** technical support from Acronis. If you have problems installing or using the system that you cannot resolve with the help of this guide and readme file, please e-mail technical support. You will also need to provide the registration number of your Acronis Privacy Expert Suite supplied with this package.

Support URL: http://www.acronis.com/support/

E-mail: support@acronis.com

Chapter 1. Installing Acronis Privacy Expert Suite

1.1 What's included

- installation CD-ROM
- this guide
- License Agreement
- registration card
- advertising information

1.2 Installing the system

To install the software, insert the installation CD-ROM into your drive and run the program. Please carefully follow all instructions shown in the installation wizard.

During the installation, you will be prompted to create a bootable diskette or CD with Acronis Privacy Expert Suite. Using this disk you will be able to easily and securely destroy information on your PC that doesn't have Acronis Privacy Expert Suite installed. If you don't want to create this diskette immediately, you will be able to do it later using the **Bootable Media Builder** feature included with the suite.

Having answered all the questions in the installation wizard and copied Acronis Privacy Expert Suite files to the hard disk, you must reboot your PC.

1.3 Recovering Acronis Privacy Expert Suite

If Acronis Privacy Expert Suite is damaged during installation or execution, run its installation program again. The software will determine that the suite has already been installed to your PC and ask if you want to recover (update) or remove it from the disk.

In the installation wizard window, select **Recover/update Acronis Privacy Expert Suite** and click Next. All files will be copied to your hard disk again to restore the software.

1.4 Removing the software

To remove the software, select **Acronis → Privacy Expert Suite → Remove Acronis Privacy Expert Suite** from the Programs menu. You will see the dialog box to confirm removal of the software from your PC hard disk.

To confirm removal, click Yes. Acronis Privacy Expert Suite will be removed completely from your PC.

Chapter 2. Working with Acronis Privacy Expert Suite

2.1 Getting started

The Acronis Privacy Expert Suite user interface features standard Windows XP icon graphical user interface (GUI) elements. We will not describe details here, but instead pay general attention to setting and executing clean-up variants.

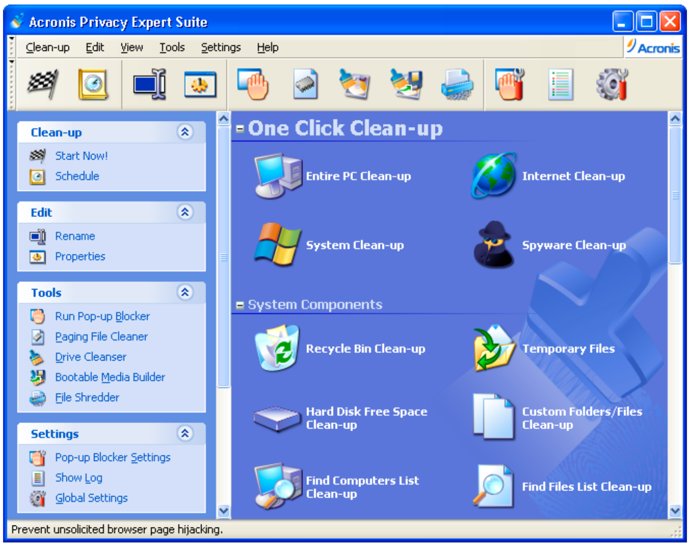
2.2 The main window

Acronis Privacy Expert Suite is controlled from the **main window.** It is shown on the screen after selecting **Acronis** → **Privacy Expert Suite** → **Privacy Expert Suite** from the Programs menu. The main window is a Windows dialog box split into two parts.

The right part contains grouped lists of main PC clean-up **variants** that the user can execute with Acronis Privacy Expert Suite.

The left part of the window called the **sidebar** – an element first introduced in Windows XP – contains the following sections:

- **Clean-up** – to perform upon objects in the right part of the window
- **Edit** – for changing properties and names of objects in the right part of the window
- **Tools** – included in the Acronis Privacy Expert Suite and providing a number of additional security and clean-up capabilities against spyware threats and pop-up windows. Also the **Tools** section includes a number of **wizards** for additional user convenience
- **Settings** – enabling fine suite tuning and **log** access
- **Details** – brief context help regarding either software component



Prevent unsolicited browser page hijacking.

The Acronis Privacy Expert Suite main window

Clean-up variants are executed, set, scheduled and renamed with the help of corresponding items of the main menu, toolbar, sidebar and context menus.

2.3 Logical software organization: sections

Logically, Acronis Privacy Expert Suite consists of **several parts**, each enabling users to perform various tasks:

(1) specific **variants of complex PC clean-up** from PC activity evidence

(2) **clean up separate components (System components, Internet components, Spyware components)**

(3) **Tools**

2.3.1 Complex PC clean-up

In the **One Click clean-up** section, shown by default in the right part of the main window, users have access to **icons of four predefined complex PC clean-ups.**

If you need to perform:

1. **entire PC clean-up**, including Windows system areas and sections related to working on the Internet, execute **Entire PC clean-up**;
2. **clean-up of sections related to working on the Internet**, execute **Internet clean-up;**
3. Windows **system section and user files/folders clean-up**, execute **System clean-up.**
4. Clean your PC up from spyware, select **Spyware clean-up.**

Attention! Described clean-up variants are **fully set up** by default and **ready for immediate work** after Acronis Privacy Expert Suite is installed. They were created so the majority of users could take advantage of them without understanding all the advanced settings, and contain everything necessary for most users. Any of these variants can be executed by a click of the mouse!

2.3.2 Cleaning separate system components

Internet components and System components sections allow you to perform a **quick clean-up** of separate system components after you take specific actions at your PC.

For example, you need to clean up the browser cache to get rid of garbage after visiting a dubious-content site and remove its URL from the list of visited sites, etc. This takes much less time than a complex clean-up.

If you need to perform:

1. a quick clean-up of **only separate** components of Windows system sections and **separate** user files/folders, execute one of the clean-up variants from the **Components** section.
2. a quick clean-up of **only separate** Windows components related to working on the Internet, execute a variant from the **Internet components** section.
3. a quick clean up of **only particular** Windows components that might be threatened by spyware and parasites, select one of the **Spyware clean-up** variants.

Separate components clean-up takes less time than a complex clean-up of the entire Windows area.

All PC clean-up variants, as well as separate components clean-up, are executed manually or by schedule and are set universally (see the section 2.4 Acronis Privacy Expert Suite global settings)

2.3.3 Additional cleanup tools

You will find additional cleanup and security tools in the **Tools** section that eliminate unwanted components.

1. To **block** unwanted **pop-ups** on websites, select **Acronis Privacy Expert Pop-up Blocker**
2. To **clean the paging file**, select **Paging File Cleaner**
3. To **destroy data** on a selected partition or disk **securely and permanently**, select **Acronis Drive Cleanser**
4. To **permanently delete selected files or folders**, select the **File Shredder.**

2.4 Acronis Privacy Expert Suite global settings

If you regularly use Acronis Privacy Expert Suite, you can provide custom preferences for typical situations.

The global settings window can be invoked in different ways:

- From the **Tools sidebar** of the Acronis Privacy Expert Suite main window
- From the **Tools submenu of the main menu**
- By clicking the **Edit global settings** icon on the **Toolbar**

2.4.1 General preferences

The **general preferences** section contains the following items:

- **Ask Before Clean-up –** When this is flagged, the software will ask for your confirmation before each component, group of components or system as a whole is cleaned up.
- **Treat shortcuts as separate files --** When this is flagged, the **shortcut target** will be left untouched. Otherwise target files will be deleted along with the shortcuts.

2.4.2 Scheduled tasks

The **scheduled clean-up** (see the section 2.13 Executing scheduled PC clean-up) might lead to errors if data to be deleted is used by other programs.

You can set up Acronis Privacy Expert Suite for such situations by selecting from the following variants:

- Ignore
- Retry
- Cancel
- Ask user

2.5 Executing PC clean-up manually

There are **three ways to manually execute** complex PC and component clean-up.

PC or separate component clean-up, previously selected from the right part of the main window, can be executed by:

- mouse-clicking **Start Now!** in the main window sidebar
- selecting **Clean-up → Start Now!** from the main menu
- selecting **Start Now!** from the task context menu

If you can't see clean-up variants or components to clean in the workspace, scroll down to make them visible.

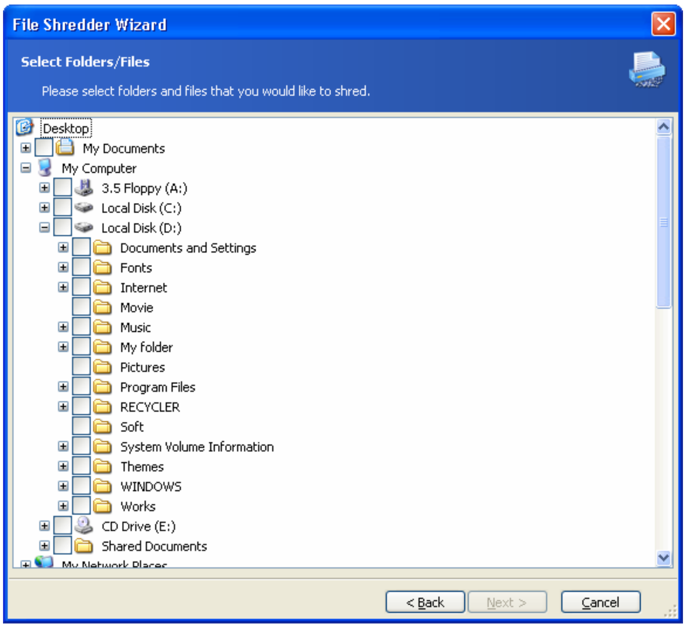
2.6 Using File Shredder

The File Shredder enables users to select files and folders quickly in order to destroy them permanently.

This wizard features the familiar Windows Explorer interface, ensuring that it is easy to use.

To run the folders/files cleaner, do one of the following:

- Select **File Shredder** in the **Tools** section of Acronis Privacy Expert Suite sidebar
- Select **Tools → File Shredder** in the main menu



Please select folders and files that you would like to shred.

Using File Shredder

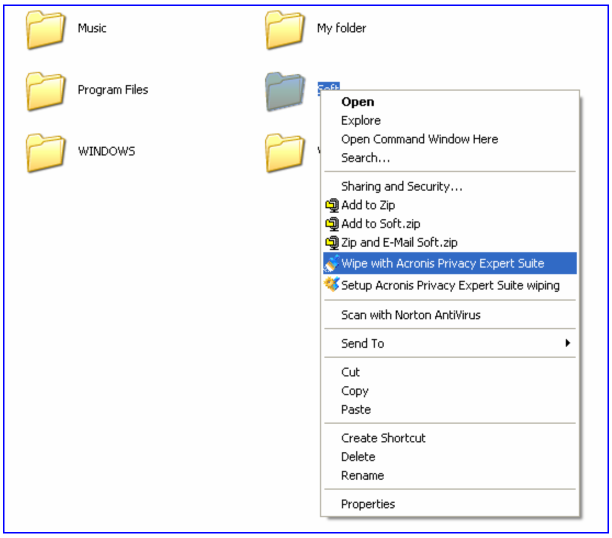
2.7 Folders/files clean-up through the context menu

Acronis Privacy Expert Suite provides an easy way to quickly delete files and clean up folders through the **Windows Explorer context menu.** This requires you to:

- select the necessary files or folder with the mouse or the Tab button
- click the right mouse button or the context menu button on the keyboard
- in the invoked window, select **Wipe with Acronis Privacy Expert Suite.**

After this, the suite will securely delete the selected file or clean up the selected folder (leaving the folder itself untouched).

With the help of the context menu, you can also **set up the clean-up preferences** and select a data destruction method (for more details see the section 2.10.1 «Data destruction method» setting).



Folders/files clean-up through the context menu

The context menu also allows you to securely clean up the **Windows Recycle Bin.** At that, **clean-up preferences** can not only include the data destruction method, but also the destruction wildcard.

2.8 Clean-up settings

By changing clean-up settings, you can set Acronis Privacy Expert Suite for your personal needs. For example, you can select an method of guaranteed data destruction that suits your needs by speed and reliability; enter the type of temporary files to clean; directly select browser used; disable separate component clean-up; etc. This will enable the software to clean your PC at **maximum speed and performance.**

Settings are described below.

2.8.1 Clean-up settings editor

Having selected a clean-up variant by mouse-clicking from the right part of the main window, and then Properties from the sidebar Edit list, you invoke the **settings editor**. You can also do this by selecting a clean-up variant and **Clean-up → Properties** from the main menu. Finally, the settings editor can be invoked from the context menu of a clean-up variant by selecting Properties.

2.8.2 Setting PC component clean-up with the editor

Below you can see the opened settings editor, featuring two groups of components to clean that belong to the **Entire PC clean-up**. These include:

- **Internet clean-up** – this group includes clean-up of sections related to working on the Internet
- **System clean-up** – this group includes Windows system section and user files/folders clean-up
- **Spyware clean-up** – includes spyware threat clean-up tools

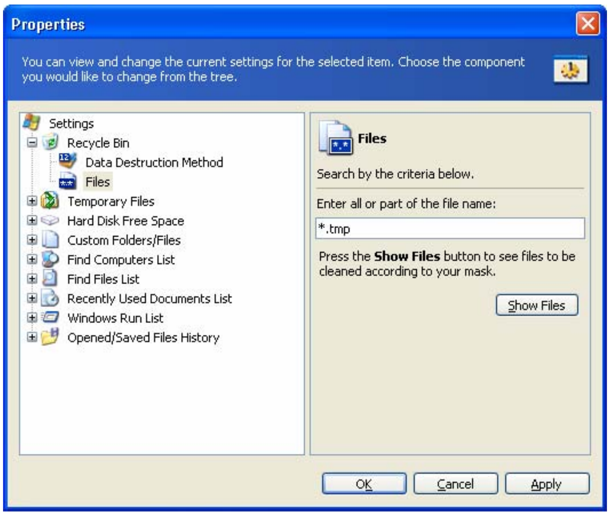
Grouped PC components to clean are described later (see Chapter 4 «Separate PC components clean-up»).

If you need to set up component clean-up:

1. Select the component from the left part of the editor and check the Enable <component name> box.

The description of a component to clean

2. Set component clean-up; for this consecutively select each component clean-up setting and set it up as necessary (selecting/entering clean-up method, file type, Internet browser, etc.).



Properties

You can view and change the current settings for the selected item. Choose the component you would like to change from the tree.

Files

Search by the criteria below.

Enter all or part of the file name: *.tmp

Press the **Show Files** button to see files to be cleaned according to your mask.

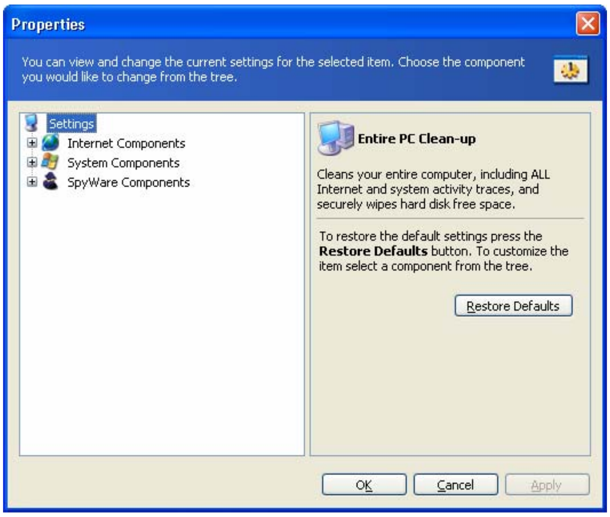
«Files» setting

3. To save your settings, click Apply. To discard changes, click Cancel.

If you need to restore Acronis Privacy Expert Suite default clean-up settings:

1. Select the component tree root — **Settings.**

2. In the right part of the editor, click Restore Defaults.



Properties

You can view and change the current settings for the selected item. Choose the component you would like to change from the tree.

Entire PC Clean-up

Cleans your entire computer, including ALL Internet and system activity traces, and securely wipes hard disk free space.

To restore the default settings press the **Restore Defaults** button. To customize the item select a component from the tree.

Restoring Acronis Privacy Expert Suite default settings

2.9 Separate components clean-up settings

Having selected a specific component to clean from the editor, you open the list of its clean-up **settings**.

Each component to clean has in Acronis Privacy Expert Suite several settings (from 1 to 3 depending on a component).

Below are settings **common** for a number of components. **Specific** settings of separate components are described in Chapter 4 «Separate PC components clean-up».

2.10 System component clean-up settings

«Data Destruction Method» and «Files» settings are common for system component clean-up.

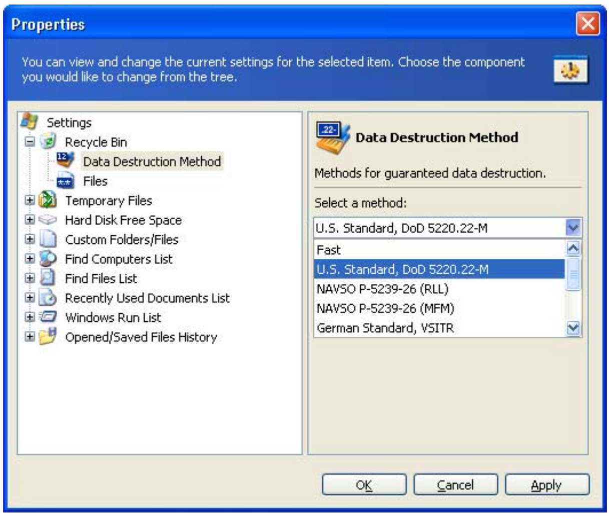
2.10.1 «Data destruction method» setting

Having selected the «Data Destruction Method» setting, you can change the **security level** provided for PC clean-up and **clean-up speed.**

For detailed information about data destruction methods, please see Appendix A «Hard Disk Wiping methods»

The most secure methods are always very slow, and conversely, the quickest methods provide lower levels of reliability and security.

Having mouse-clicked a setting name, you will see its available element in the right part of the editor – the selection of data destruction methods.



Properties

You can view and change the current settings for the selected item. Choose the component you would like to change from the tree.

- Settings
  - Recycle Bin
    - Data Destruction Method
    - Files
  - Temporary Files
  - Hard Disk Free Space
  - Custom Folders/Files
  - Find Computers List
  - Find Files List
  - Recently Used Documents List
  - Windows Run List
  - Opened/Saved Files History

Data Destruction Method

Methods for guaranteed data destruction.

Select a method: U.S. Standard, DoD 5220.22-M

- Fast
- U.S. Standard, DoD 5220.22-M
- NAVSO P-5239-26 (RLL)
- NAVSO P-5239-26 (MFM)
- German Standard, VSITR

Selecting a data destruction method

You will see all data destruction methods available in Acronis Privacy Expert Suite by clicking your mouse on the drop-down list in the right part of the editor.

If you need to ensure:

1. **maximum security** of PC activity evidence, select Peter Gutmann's method (35 data destruction cycles), but please keep in mind that this method is quite slow.

2. **mid-level security at an average speed** of clean-up, select VSITR or Bruce Schneier's method (7 data destruction cycles).

3. **fast PC clean-up** with limited security in mind, select any of the 1-3-pass methods (see A.2 «Information wiping methods used by Acronis»).

2.10.2 «Files» setting

The «Files» setting **provides** temporary **filenames to clean with** Acronis Privacy Expert Suite (from the Windows Recycle Bin and from system and user folders) and can be used with a search string.

Under the Windows operating system, a search string can represent a full or partial filename. A search string can contain any alphanumeric symbols, including comma, * and ? symbols, and can have values similar to the following:

- *.* – to delete all files from the Recycle Bin – with any file names and extensions
- *.doc – to delete files with specific extension – a Microsoft document file in this case
- read*.* – to delete all files with any extensions, and names beginning with «read»
- read?.* – to delete all files having five-letter names and any extensions, names beginning with «read»; the fifth letter is random
- The last search string, for example, will result in removal of read1.txt, ready.doc files, but readyness.txt will remain with its longer name (excluding the extension)

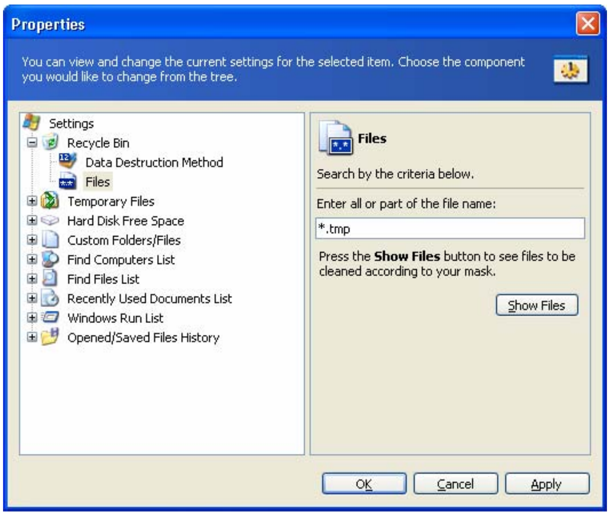
You can enter several different search strings separated by a semicolon; for example:

*.bak; *.tmp; *.~~~;

. . . and so on. All files with names corresponding to at least one of the search strings will be deleted.

Attention! The length of a search string with full or partial filenames is almost infinite! You can enter any number of filenames or their parts like *.tmp, read?.* separated by a semicolon.

The «Files» setting has five system components to clean: Recycle Bin, Temporary Files, Custom Folders/Files, Find Files List and Recently Used Documents List.



You can view and change the current settings for the selected item. Choose the component you would like to change from the tree.

Search by the criteria below.

Enter all or part of the file name: *.tmp

Press the **Show Files** button to see files to be cleaned according to your mask.

«Files» setting

If you need to:

1. delete only specific file **types** from the Recycle Bin (system or user folder), enter filenames separated by a semicolon as follows:
   *.jpg; *.gif;

2. delete only **specific filenames** from the Recycle Bin (system or user folder), enter names as follows:
   read*.txt.

3. This will result in removal of read!.txt, readme.txt, read1.txt, etc. files, while read.doc, readme.doc, etc. will remain.

4. delete only **specific-length filenames** from the Recycle Bin (system or user folder), enter filename as follows:
   read?.txt.

As a result, files read!.txt, read1.txt, read2.txt, etc. will be deleted, while read.doc, readme.doc, etc. will remain.

Having entered filenames, you can see files selected by Acronis Privacy Expert Suite. To do this, click the Show files button.

You can unmark a file for deletion by unchecking the corresponding box.

2.10.3 «Computers» setting

The «Computers» setting cleans up the registry search strings for finding computers in the local network. These strings keep information on what interested you in the network. These elements should also be deleted to maintain confidentiality.

The «Computers» setting is the same as «Files». The «Computers» setting is a string that can contain any number of full or partial computer names separated by a semicolon. The deletion of computer search strings is based on a comparison with the «Computers» setting according to Windows rules (see the section 2.10.2 «Files» setting).

If you simply **need** to delete all local network computer search strings (suitable in most cases):

1. Select **Find Computer List**.
2. Check the **Enable the Find Computer List cleaning** box.
3. Select the «Computers» setting; leave its default value unchanged – *.

As a result, **all** computer search strings will be deleted from the registry.

Upon entering the «Computers» setting value, you can browse the search strings in the registry selected by Acronis Privacy Expert Suite. To do this, click Show Computers. You will see the window with full and partial computer names searched for in the network. These strings will be deleted during the registry clean-up.

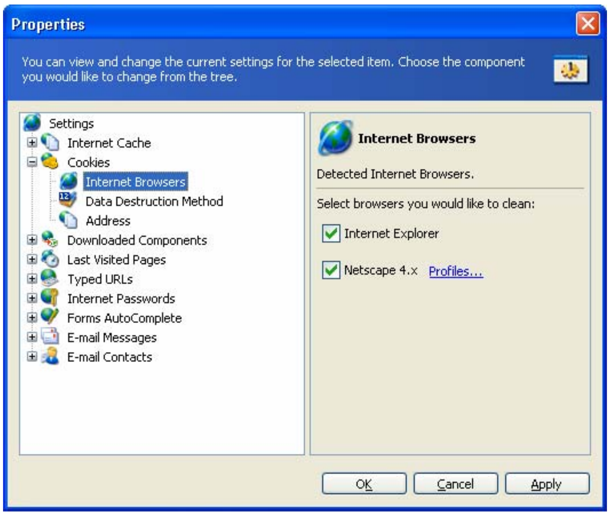
2.11 Clean-up settings of components related to working on the Internet

The «Internet Browsers» and «Address» settings are common for components related to working on the Internet.

2.11.1 «Internet Browsers» setting

Acronis Privacy Expert Suite automatically locates all installed and supported browsers and removes any of their Web activity traces by default.

If you have Internet Explorer installed, the structures to clean belong only to the currently logged on user.



Properties

You can view and change the current settings for the selected item. Choose the component you would like to change from the tree.

Internet Browsers

Detected Internet Browsers.

Select browsers you would like to clean:

☑ Internet Explorer

☑ Netscape 4.x Profiles...

«Internet Browsers» setting

Netscape Navigator and Mozilla support personal profiles. Without additional settings, Acronis Privacy Expert Suite cleans either the «default profile» (if it is the only one), or the profile of the currently logged on user.

If you need to clean up only one browser:

1. Set the checkbox near its name only (for example, Internet Explorer), unchecking all other boxes.

2. If you use a version of Netscape Navigator (or Mozilla), you should additionally select a personal profile (by clicking **Profiles...** link).

2.11.2 «Address» setting

The «Address» setting is meant for cleaning up the Internet cache and the last visited pages list. («Address» setting has six system components to clean: **Internet Cache, Cookies, Download Components, Last Visited Pages, Typed URLs**, **Passwords**).

You can also enter any full or partial Internet addresses separated by a semicolon as a value of the «Address» setting; for example:

*worldsoccer.com; *formula1.com;

. . . and so on. All files downloaded from sites fully or partially corresponding to at least one of the addresses entered will be removed.

Attention! The length of a search string with full or partial Internet addresses is almost infinite! You can enter any number of addresses like *worldsoccer.com or *formula1.com separated by a semicolon.

If you need to:

1. clean up the Internet cache (last visited pages list) from **all** files (lists, elements), downloaded from a **specific** Internet **address** (site), enter addresses or their parts separated by a semicolon; for example, like:

CompanyA;*XYZ123*

As a result, all files downloaded from www.CompanyA.com, www.xyz123.com will be deleted.

2. clean up the Internet cache from **only specific file types** downloaded from a **specific** Internet **address** (site), enter addresses separated by a semicolon; for example, like:

companya.jpg;*companya*.gif;*xyz123*.jpg;*xyz123*.gif

As a result, only *.jpg, *.gif files will be deleted, while *.html files, for example, remain in the cache.

Entering the Internet addresses list, you can browse files (visited pages) selected according to the list. To do this, click Show URLs. You will see the window with selected addresses. They will be deleted during the selected component clean-up.

If you want to **cancel** the deletion of any address in this list, uncheck the corresponding box.

2.12 Spyware clean-up preferences

The **Spyware clean-up** group contains three elements: **Spyware; Browser hijacking pages; Trusted sites.** Each has its own clean-up preferences thoroughly described in the section 4.3 «Spyware clean-up» .

The **Browser hijacking pages** element contains the common **Internet browsers** preference (see the section 2.11.1 «Internet Browsers» setting).

The **Trusted sites** component contains the common **Address** preference (see the section 2.11.2 «Address» setting).

2.13 Executing scheduled PC clean-up

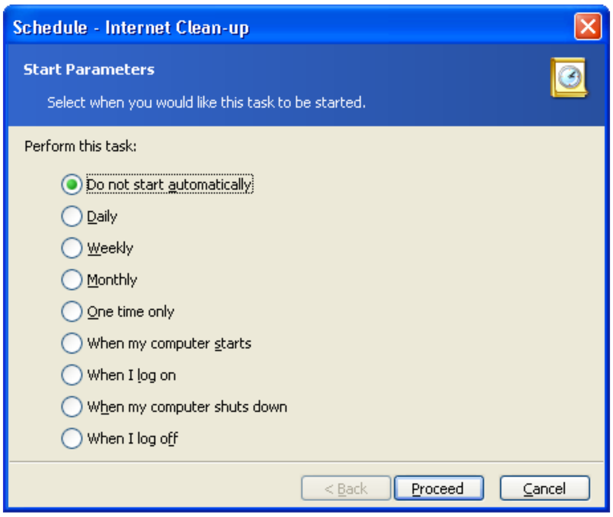
Each PC clean-up variant of Acronis Privacy Expert Suite can be executed either manually or **automatically as scheduled.**

Having set PC clean-up as a daily procedure, to be performed, for example, at the end of a workday before powering the PC off, you can be sure that all evidence of your PC and Internet activity will be reliably removed each day.

Acronis Privacy Expert Suite features a built-in **scheduler**.

2.13.1 Invoking the scheduler

Having mouse-clicked a clean-up variant in the right part of the main window, and selected **Schedule** in the sidebar **Clean-up** list, you invoke the scheduler. You can also do this by selecting a clean-up variant and **Clean-up → Schedule** from the main menu. Finally, you can invoke the scheduler from the clean-up variant context menu selecting Schedule.



Schedule - Internet Clean-up

Start Parameters

Select when you would like this task to be started.

Perform this task:

● Do not start automatically
○ Daily
○ Weekly
○ Monthly
○ One time only
○ When my computer starts
○ When I log on
○ When my computer shuts down
○ When I log off

Scheduler

2.13.2 Scheduled tasks preferences

The scheduled tasks wizard offers flexible **automatic execution** capabilities for any selected variant of PC clean-up.

You can perform automatic clean-up:

- **Do not start automatically**
- **Daily**, according to the schedule with the ability to select only workdays or once every few days
- **Weekly**, according to the schedule with the ability to select particular days, such as Tuesday and Friday, or once every two or three weeks, etc
- **Monthly,** according to the schedule on the time and day set; The suite supports clean-up on the <first, second, third, fourth, last> <day of the week> (Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday), for example
- **One time only,** at a specific time (hours:minutes) on a particular day (month/day/year)
- **When my computer starts**
- **When I log on**
- **When my computer shuts down**
- **When I log off**

Having selected any variant, click Next to set additional parameters on the second wizard page.

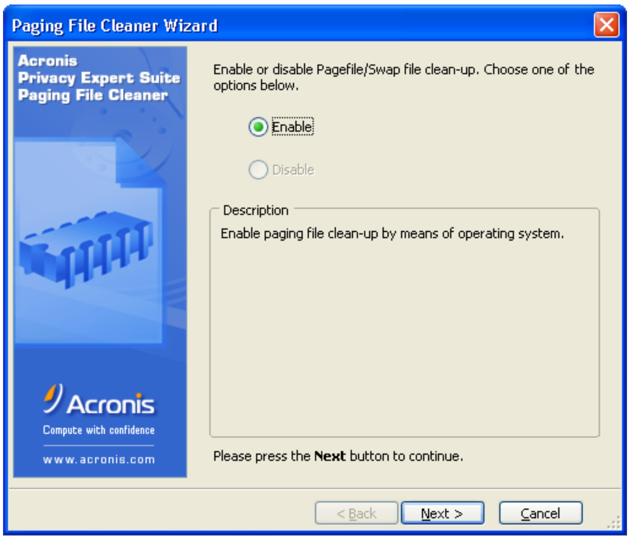
2.14 Paging file

The **Paging file clean-up** allows you to free it from any traces of PC or Internet activity permanently.

A **paging file** is a file on a hard disk (e.g. C:\win386.swp in Windows 95/98/Me or C:\pagefile.sys in Windows NT/2000/XP) used by Windows as additional memory when that is required in order to run applications.

The paging file clean-up is not a part of any system clean-up variants. At the same time, this file might contain personal information that a user is unaware is there. For example, if a user opened too many Internet Explorer windows and entered personal information in one of them, then tried to switch to another Internet Explorer window, the operating system might lack enough physical memory for all the windows and store the contents of the previous one in its paging file. If a user closes browser windows after this, there is a strong possibility that confidential information will have been left in the paging file.

To perform **Paging file clean-up,** click on the corresponding item in the **Tools** section sidebar and follow the instructions of the **clean-up wizard.**



Enable or disable Pagefile/Swap file clean-up. Choose one of the options below.

● Enable

○ Disable

Description

Enable paging file clean-up by means of operating system.

Please press the **Next** button to continue.

Paging file cleaner Wizard

After swap file clean-up under Windows 95/98/Me, Acronis Privacy Expert Suite offers to reboot your PC. The swap file clean-up is performed when the system shuts down. This file will be wiped after any reboot under Windows NT/2000/XP.

2.15 Renaming clean-up variants

Enabling/disabling separate component clean-up and selecting clean-up settings, you set up and customize your PC clean-up variant(s) as needed. That said, you will want to rename the variant(s) to better represent PC clean-up contents.

If you want to rename a PC (or separate component) clean-up variant, you can do so by following one of these methods:

- clicking on **Rename** on the sidebar

- selecting **Clean-up → Rename** from the main menu
- selecting **Rename** from the context menu of a PC (component) clean-up variant

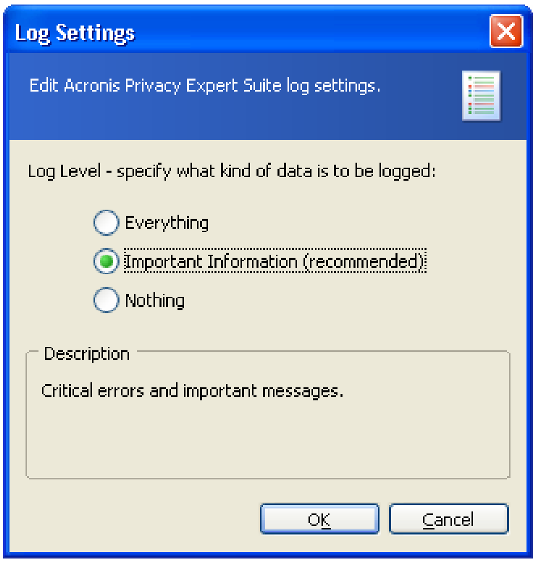
As a result of any of these actions, you will see the **Rename Item** window enabling you to enter a new name for a PC or component clean-up variant.

2.16 Using the Log

The **Log** keeps track of all actions performed by Acronis Privacy Expert Suite. It can provide you with complete actions history and reasons for any problems that have taken place.

Log settings enables you to keep track with different degree of detail. You can select one of the following variants:

- **Everything**
- **Important information** – error and spyware messages
- **Nothing**



Log Settings

Edit Acronis Privacy Expert Suite log settings.

Log Level - specify what kind of data is to be logged:

○ Everything
● Important Information (recommended)
○ Nothing

Description

Critical errors and important messages.

Log settings

Chapter 3. Complex PC clean-up

Using variants of **complex PC clean-up** described below, you can **clean a large number of various** Windows **components** that regain evidence of your PC activity, and also remove various spyware that perform unauthorized actions on your PC.

Vice versa, if you need to clean up **only a specific** Windows **component**, for example, last visited Internet pages, you should use one of the Acronis Privacy Expert Suite sections described below (see Chapter 4 «Separate PC components clean-up»). Separate component clean-up is faster than any variant of complex PC clean-up.

3.1 Entire PC clean-up

If you need to clean a PC of **any evidence** of your activity, select the **Entire PC clean-up**. Executing it, you'll be able to clean **all** Windows **components accessible by** Acronis Privacy Expert Suite:

- clean the Windows **registry** of user activity evidence
- delete **temporary files** from standard Windows folders
- delete **any file types from user folders** on any disks connected to the PC
- clean the Windows **Recycle Bin**
- clean hard disk **free space**
- clean the last visited pages and **last used documents** list
- delete **evidence of searching** for files on connected disks, for networkedcomputers, for information on the Internet
- clean the **Internet cache**
- delete **cookies**
- delete downloaded **components**
- clean up the **Browsed URLs and History,** stored in the browser address line
- remove **e-mail** (from MS Outlook and MS Outlook Express) and clean up **Contacts and address book**
- delete Web **forms autocomplete** and **passwords** for Web sites that require authorization
- remove **spyware** threats that perform secretly

Entire PC clean-up is executed by a mouse-click on its name in the right part of the main window (for other execution methods see the sections 2.5, 2.13).

For detailed descriptions of what Acronis Privacy Expert Suite performs in specific cases (how and what files, folders, system or registry sections it cleans from what data see the sections 2.5, 2.13).

3.2 System clean-up

If you need to wipe the evidence of your PC activity **from its system sections**, use the **System clean-up**. Executing it allows you to:

- clean the **Windows registry** from user activity traces;
- delete **temporary files** from standard Windows folders;
- delete **any file types from user folders** on any disks connected to a PC;
- clean the Windows **Recycle Bin**;
- clean hard disk **free space**;
- clean the **last used documents list;**
- delete the **evidence of searching** for files on connected disks, for networked computers, for information on the Internet.

System clean-up can be executed by mouse-clicking the clean-up variant in the right part of the main window (for other execution methods see the sections 2.5, 2.13).

For detailed descriptions of what Acronis Privacy Expert Suite performs in specific cases, see Chapter 4 «Separate PC components clean-up».

3.3 Internet clean-up

If you need to wipe evidence of your Internet activity, use **Internet clean-up**. This variant allows you:

- Clean up the **Internet cache**
- delete **cookies**
- delete **downloaded components**
- clean the **Internet history and last visited pages list**
- remove **e-mail** (from MS Outlook and MS Outlook Express) and clean up **contacts and address book**
- delete Web **forms autocomplete** and **passwords** for Web sites that require authorization

Internet clean-up can be executed by mouse-clicking its name in the right part of the main window (for other execution methods, see the sections 2.5, 2.13).

For detailed descriptions of what Acronis Privacy Expert Suite performs in specific cases, see Chapter 4 «Separate PC components clean-up.

3.4 Complete spyware clean-up

If you need to clean your PC of various spyware that performs unauthorized actions, select **Spyware clean-up**. It will allow you to:

- remove spyware and threats that operate secretly
- restore Web presets that have been changed without your notice.
- clean up the Trusted sites list of any unwanted addresses.

Chapter 4. Separate PC components clean-up

In the **One Click clean-up** section, you were able to execute **variants of complex** PC clean-up (manually or scheduled), to clean a **number of system components.** These variants will suit most user needs.

However, if you need to quickly clean up **separate system components**, use **System clean-up, Internet components clean-up, and Spyware clean-up** sections.

Separate component clean-up is described step by step further, in Chapter 3 «Complex PC clean-up» of this guide.

In particular, it explains where and how personal user information is kept, and why it is necessary to perform separate component clean-ups (of, for example, a swap file).

The following chapters are generally meant for **experienced PC/Windows users** who are interested in actions that Acronis Privacy Expert Suite can perform in specific cases.

Various **execution and setup** capabilities of PC and separate components clean-up variants of are described in detail **above** (see the sections 2.5, 2.13 and 2.9). Clean-up of each component is set similarly, so this will not be described further in the guide. Only **specific** settings will be explained. If you have questions, please follow the links provided.

4.1 System components

In the **System clean-up** section, you can clean up components (folders, files, registry sections, etc.), related to general system tasks. These Windows components keep evidence of user PC activity, so they too should be thoroughly wiped to maintain confidentiality.

4.1.1 Recycle Bin

The Windows Recycle Bin clean-up destroys trace files according to the provided «Files» value.

The Windows Recycle Bin is meant to retain accidentally deleted files so you can recover them anytime. Thus, files in the Recycle Bin containing your data become a potential security threat.

You can also use context menu for Windows recycled bin clean-up by selecting it on Windows desktop and clicking the right mouse button or the context menu keyboard button (see the section 2.7)

The Windows Recycle Bin, represented by an icon on the desktop and as a folder in Explorer, is actually a number of system folders located on your logical PC disk. Acronis Privacy Expert Suite completely cleans every system folder.

4.1.2 Temporary Files

Temporary files clean-up enables you to thoroughly destroy temporary files from the special **system folders**, which type (or name) corresponds to the provided «Files» setting value.

Windows usually keeps temporary files in a special folder. For example, C:\Windows\Temp or D:\Documents and Settings\<user name>\Local Settings**Temp** folder.

In this case, temporary files folder means a folder specified in the temp environment variable. It is set by the Windows set command. You can check temp value by typing set temp in the command line. As a result, under Windows XP you will get a string like D:\Documents and Settings\<user name>\Local Settings**Temp**.

Temporary files can usually be determined by their extensions. For example, they can be as follows:

- *.bak, *.old – backup copies
- *.gid – a temporary file, created when opening Windows help
- *.chk – files, created while disk is checked for lost clusters
- *.tmp, *.$*, *.~*, *.---, ~*.* – other temporary files, created by a variety of programs

Please note that the above list is far from complete.

Besides **temporary files** clean-up**,** Acronis Privacy Expert Suite offers to clean your **user folders and files** (described further), deleting all temporary files from folders **on any connected disks** according to the provided «Files» value.

Setting the **temporary files** clean-up, you can provide *.* «Files» value to destroy **all files** from the temporary files folder.

4.1.3 Hard Disk Free Space

Disk free space clean-up allows you to destroy all data possibly stored in the hard disk drive's free space sectors.

Disk free space almost always contains information and data under the control of Windows.

Windows does not actually remove anything when **deleting a file**: its name is simply replaced with unusable characters in the File Allocation Table, (FAT). The file becomes invisible only for a user, and the **cluster** chain with file data is considered free, but the information does not disappear from the hard disk sectors. It is actually very simple to recover deleted Windows files. There are numerous programs for doing this under either DOS and Windows.

Formatting or deleting a partition also does not destroy information from the hard disk sectors. It can be read directly from them if needed.

The clean-up of disk free space, comprising **every sector**, is an important part of maintaining confidentiality of PC activity. Please note that a 20-40 GB hard disk drive will take considerable time to wipe clean, however your privacy and data security are what matter most.

4.1.4 Custom Folders/Files

Custom folders/files clean-up enables you to wipe files from selected folders.

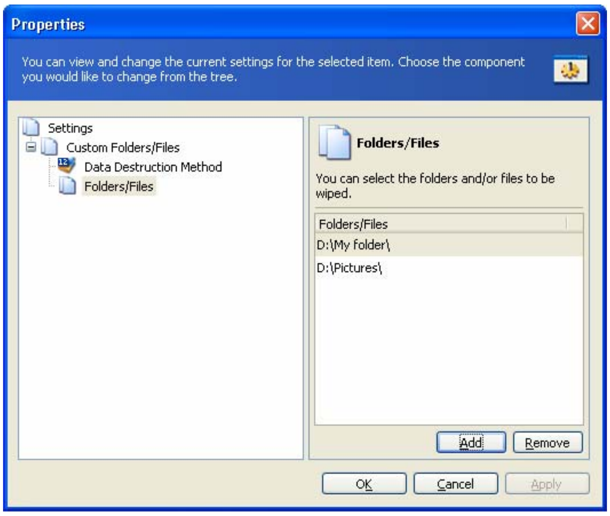
Windows does not securely delete files. Any file deleted by Windows can be recovered.

Unlike Windows, Acronis Privacy Expert Suite securely and unrecoverably destroys user files from specified folders, using special methods. (See Appendix A «Hard Disk Wiping methods»).

To delete user files, the suite enables you to select a data destruction method, specify «Files» setting value and the **user folder list** to clean.

To select a list of folders and files to clean with Acronis Privacy Expert Suite:

1. Select **Custom Folders/Files List.**
2. Select «Folders/Files» setting and add the folders and files to destroy, clicking Add in the right part of the editor window.



Properties

You can view and change the current settings for the selected item. Choose the component you would like to change from the tree.

- Settings
  - Custom Folders/Files
    - Data Destruction Method
    - Folders/Files

Folders/Files

You can select the folders and/or files to be wiped.

Folders/Files
D:\My folder\
D:\Pictures\

Custom folders/files clean-up

You can also use the context menu for user files and folders clean-up by selecting them and clicking the right mouse button or the context menu keyboard button (see the section 2.7 Folders/files clean-up through the context menu)

Attention! **Please be careful –** the selected folders will be completely wiped out! All their files will be permanently destroyed!

4.1.5 Registry Backups

Windows 95/98/Me operating systems create registry backup copies that may contain evidence of PC use or Internet activity.

Registry backup copies clean-up destroys backup copies of registry files, i.e. not just deleted files, but also corresponding hard disk clusters (sectors) using a specified wiping method.

Under Windows 95/98/Me, registry files are system.dat, user.dat, located in the C:\WINDOWS folder; under Windows Millennium registry files also feature classes.dat. Registry file backup copies are kept in the C:\WINDOWS\SYSBCKUP system folder in archives rb<file number>.cab («rb» means «registry backup»).

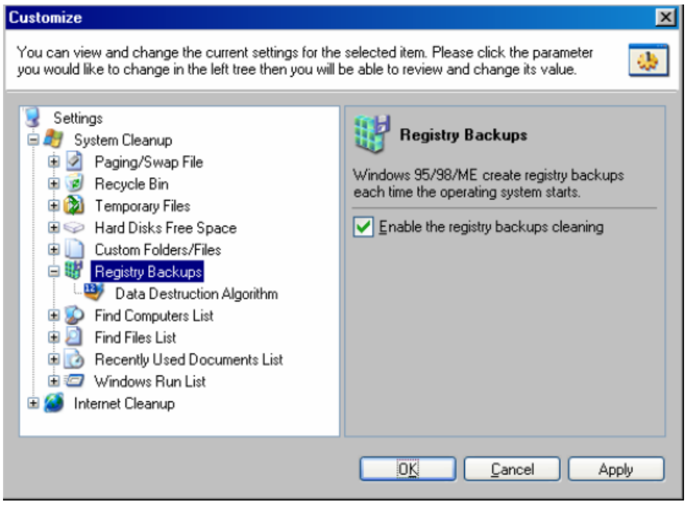
When Windows boots, it creates a backup copy of the system registry files. So user data – last visited pages lists, files or computers search lists, etc. – are stored not only in the registry, but also in its backup copy.

If you clean up the user data stored in the registry with Acronis Privacy Expert Suite **and re-boot** the PC, Windows will automatically create a backup copy without traces of your PC activity.

If you only clean the registry **and power** the PC **off**, the old backup copy will still contain the traces. So to fully maintain confidentiality of your PC activity, you must also clean the registry backup copy.

Unlike cleaning other components with Acronis Privacy Expert Suite, the **Registry backup copy** clean-up deletes not just the registry keys, but the entire backup copy of registry files, using a guaranteed data destruction methods (see Appendix A «Hard Disk Wiping methods). If you also clean the registry using other components clean-up, the new backup copies of registry files will be clean of any user activity traces.

All backup copies of registry files are cleaned under Windows 95/98/Me!



Customize

You can view and change the current settings for the selected item. Please click the parameter you would like to change in the left tree then you will be able to review and change its value.

Registry Backups

Windows 95/98/ME create registry backups each time the operating system starts.

☑ Enable the registry backups cleaning

Registry backup copies clean-up under Windows 95/98/Me

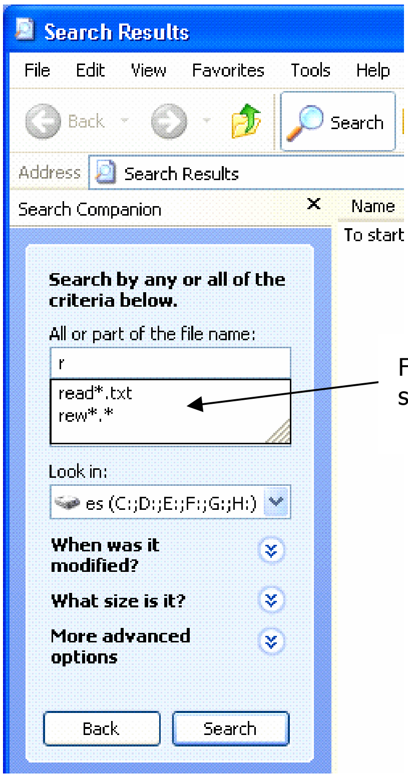
4.1.6 Find Computers List

Find computers list clean-up deletes it from the Windows registry. A search string may contain a full computer name, including its domain name, but can also be a **partial computer name.**

Windows Explorer performs various file system navigation functions. It also supports searching for networked computers as well as files and folders on local and connected disks, Explorer activity leaves multiple evidence of local and Internet work on the hard disk that may become a threat to your confidentiality.

4.1.7 Find Files List

Find files list clean-up deletes the list that indicates your file search activity on computer disks from the Windows registry. A file string may contain a full filename, including its path, or just a partial name.



Search by any or all of the criteria below.

All or part of the file name: r

read*.txt
rew*.*

Look in: es (C:;D:;E:;F:;G:;H:)

Find files strings stored in the registry

Find files strings stored in the registry

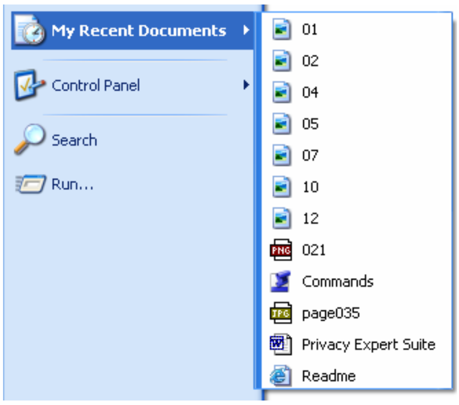
In most cases, you can simply specify «Computers» value as *.* to wipe the entire find computers list.

4.1.8 Recently Used Documents List

Recently used documents list clean-up deletes the list of documents recently opened by a user during PC activity.

Selecting **Documents** from the Start menu, you will find that Windows shows recently executed or opened files. These can be images viewed, Excel tables, MP3 or WAV sound files, etc.

To protect your privacy, you should regularly wipe the Recently used documents list.

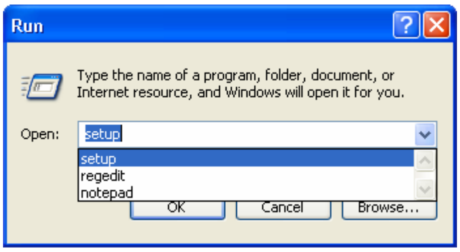


Recently used documents list in the Start menu

4.1.9 Windows Run List

Windows Run List clean-up deletes the list of files opened or executed from the **Run** box in the Start menu.

The **Open** list of the Windows **Run** window may contain a list of executed programs, opened files and **folders** (as well as visited Internet pages).



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: setup

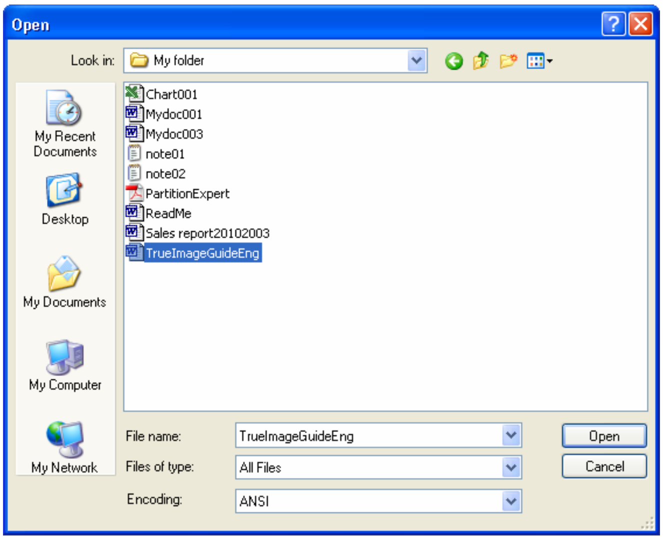
Windows Run List

Selecting **Run** from the Start menu opens a window with the same name. The **Open** list lets you type in a name of a file, folder, network folder or Internet address. Clicking OK, you run the program (application), open file or connect to the selected site. Windows keeps a history of your actions. You can see this by opening the **Open** list. Acronis Privacy Expert Suite completely wipes it, deleting names of files and folders accessed by the user.

The list of Internet addresses typed into the **Run** list by user, will not be deleted at clean-up! This is be done by **Last Visited Pages** clean-up (see the section 4.2.4 Last Visited Pages)

4.1.10 Opened/Saved Files History

The Windows operating system has a standard dialog box for opening/saving files. You can see this by selecting **Open**, **Save** or **Save As...** in a standard Windows application (Notepad, Paint, etc). Every office application has a similar dialog box.



Look in: My folder

Chart001
Mydoc001
Mydoc003
note01
note02
PartitionExpert
ReadMe
Sales report20102003
TrueImageGuideEng

File name: TrueImageGuideEng

Files of type: All Files

Encoding: ANSI

Windows Open (Save, Save As...) window

All information about access to application files (Word, Excel, etc.) and folders are stored as links in the D:\Documents and Settings\<user name>\Recent folder. Even if a file was deleted, it is referenced from the Recent folder. The link contains the file and folder name, plus the creation and modification date. To maintain confidentiality of your PC activity, the opened/saved files history must be cleaned whether a file or folder was deleted or not.

Performing the PC clean-up, Acronis Privacy Expert Suite will destroy the opened/saved file history according to the provided «Files» value.

4.2 Internet components

Today, most PC security threats come from the Internet. These were briefly listed in the introduction as well as in the system sections or components that keep traces of local user PC and Internet activity. Browser, cache, cookies, Internet history and last visited pages list are kept in different places/files on your hard disk drive.

Acronis Privacy Expert Suite supports and automatically determines files used and/or generated by the following browsers:

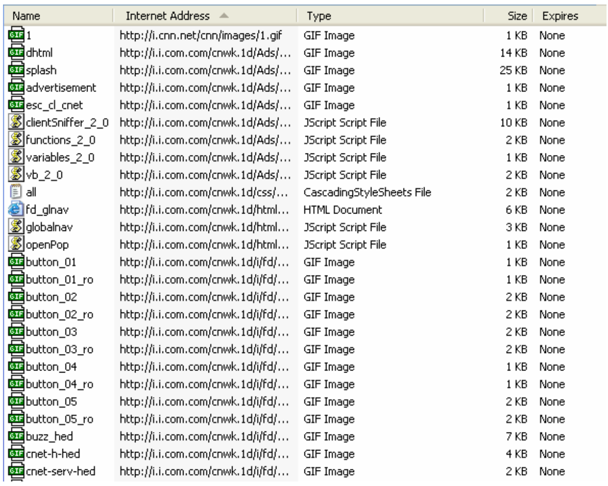
- Internet Explorer
- Netscape v.4x, 6x, 7x
- Mozilla

4.2.1 Internet Cache

Internet cache clean-up deletes files downloaded during browsing of Internet pages.

As you surf the Internet, your browser keeps («caches») the content of pages you visited in a special folder on a hard disk. This Internet cache folder contains Web pages (HTML files), including text and graphics (in JPEG and GIF graphic files). Page caching speeds up Internet access and viewing. If you want to return to a previously visited page, your browser will take the majority of its contents from the cache to show on-screen instead of downloading it again.

The Internet Explorer cache is kept in the C:\Windows\Temporary Internet Files folder under Windows 95/98/Me, and in the C:\Documents and Settings\<user name>\Local Settings**Temporary Internet Files** folder under Windows XP.



Name	Internet Address	Type	Size	Expires
1	http://i.cnn.net/cnn/images/1.gif	GIF Image	1 KB	None
dhtml	http://i.i.com.com/cnwk.1d/Ads/...	GIF Image	14 KB	None
splash	http://i.i.com.com/cnwk.1d/Ads/...	GIF Image	25 KB	None
advertisement	http://i.i.com.com/cnwk.1d/Ads/...	GIF Image	1 KB	None
esc_cl_cnet	http://i.i.com.com/cnwk.1d/Ads/...	GIF Image	1 KB	None
clientSniffer_2_0	http://i.i.com.com/cnwk.1d/Ads/...	JScript Script File	10 KB	None
functions_2_0	http://i.i.com.com/cnwk.1d/Ads/...	JScript Script File	2 KB	None
variables_2_0	http://i.i.com.com/cnwk.1d/Ads/...	JScript Script File	1 KB	None
vb_2_0	http://i.i.com.com/cnwk.1d/Ads/...	JScript Script File	2 KB	None
all	http://i.i.com.com/cnwk.1d/css/...	CascadingStyleSheets File	2 KB	None
fd_glnav	http://i.i.com.com/cnwk.1d/html...	HTML Document	6 KB	None
globalnav	http://i.i.com.com/cnwk.1d/html...	JScript Script File	3 KB	None
openPop	http://i.i.com.com/cnwk.1d/html...	JScript Script File	1 KB	None
button_01	http://i.i.com.com/cnwk.1d/i/fd/...	GIF Image	1 KB	None
button_01_ro	http://i.i.com.com/cnwk.1d/i/fd/...	GIF Image	1 KB	None
button_02	http://i.i.com.com/cnwk.1d/i/fd/...	GIF Image	2 KB	None
button_02_ro	http://i.i.com.com/cnwk.1d/i/fd/...	GIF Image	2 KB	None
button_03	http://i.i.com.com/cnwk.1d/i/fd/...	GIF Image	2 KB	None
button_03_ro	http://i.i.com.com/cnwk.1d/i/fd/...	GIF Image	2 KB	None
button_04	http://i.i.com.com/cnwk.1d/i/fd/...	GIF Image	1 KB	None
button_04_ro	http://i.i.com.com/cnwk.1d/i/fd/...	GIF Image	1 KB	None
button_05	http://i.i.com.com/cnwk.1d/i/fd/...	GIF Image	2 KB	None
button_05_ro	http://i.i.com.com/cnwk.1d/i/fd/...	GIF Image	2 KB	None
buzz_hed	http://i.i.com.com/cnwk.1d/i/fd/...	GIF Image	7 KB	None
cnet-h-hed	http://i.i.com.com/cnwk.1d/i/fd/...	GIF Image	4 KB	None
cnet-serv-hed	http://i.i.com.com/cnwk.1d/i/fd/...	GIF Image	2 KB	None

Internet Explorer cache contents

Attention! Each cached file has the «Internet address» property to track its origin. It is therefore better to set the «Address» setting instead of «Files» when erasing the Internet cache. This enables you to delete files downloaded from specific addresses (see the section 2.11.2 «Address» setting»). By providing «Address» setting values, you can also specify the type of files to clean!

The Netscape Navigator cache is kept in a folder that can be specified by the user. Under Windows XP, the cache is created in the user profile folder by default: C:\Documents and Settings\<user name>\Application Data\Mozilla\Profiles\<profile name> as a folder named **Cache**.

Keeping Internet cache files can threaten the confidentiality of your PC activity, as everything that interested you on the Web remains in the cache. When you're absent anybody – your children, spouse or co-workers -- can easily get access to your home or work PC and look through your Internet cache, thus finding what has attracted your attention for the past week or month.

Besides, the Internet cache can also occupy a considerable amount of space on a hard disk unless limited by the operating system. You'll be surprised by the amount and size of files in the Windows cache folder. You should also remember that the cache keeps a huge amount of garbage images, in particular banner ads. Moreover, keeping a large Internet cache can degrade your browser's overall performance.

Acronis Privacy Expert Suite cleans the Internet cache while maintaining the confidentiality of your PC activities and speeding up pages of visited sites (reducing time to find necessary files in cache).

4.2.2 Cookies

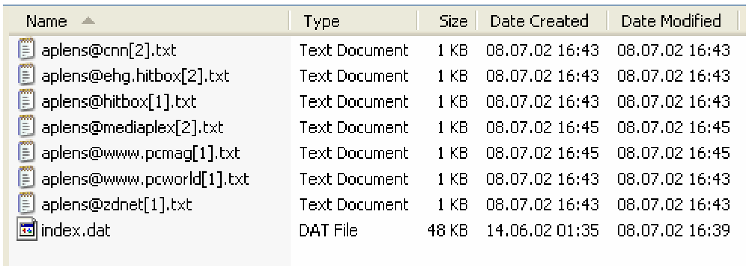
Cookies are small files created on a user's PC during visits to some Web sites. Cookies may contain user name and other data entered while registering on a site. When a user revisits the site, he/she may be greeted by name and, perhaps some setting selected last time will be applied, such as the language, page design elements and/or the content.

Acronis Privacy Expert Suite enables you to delete **unnecessary** cookies. You **can keep the cookies you need**, as the Acronis Privacy Expert Suite can choose what cookies to delete and which to save.

Which cookies are unnecessary and what is their threat? **In the aggregate,** cookies can provide full traces of where and how you surfed the Internet.

There are many scandals discussed in the media where network companies have been gathering user information and buying preferences. It is widely known that companies like A.S.A.P. Investigations, Dig Dirt and Infoseekers offer other companies personal user information, including biographical data, bank account information, phone numbers, property, health, and/or Social Security card numbers for as little as $100 (source: http://www.pcmag.com/article/0,2997,a=2443,00.asp – *PC Magazine*, January, 16, 2001, "Leave Me Alone" by Matthew Graven).

If Internet Explorer is your default browser, cookies are kept in the C:\Windows\Cookies folder under Windows 95/98/Me, and in the C:\Documents and Settings\<user name>**Cookies** folder under Windows NT/2000/XP.



Name	Type	Size	Date Created	Date Modified
aplens@cnn[2].txt	Text Document	1 KB	08.07.02 16:43	08.07.02 16:43
aplens@ehg.hitbox[2].txt	Text Document	1 KB	08.07.02 16:43	08.07.02 16:43
aplens@hitbox[1].txt	Text Document	1 KB	08.07.02 16:43	08.07.02 16:43
aplens@mediaplex[2].txt	Text Document	1 KB	08.07.02 16:45	08.07.02 16:45
aplens@www.pcmag[1].txt	Text Document	1 KB	08.07.02 16:45	08.07.02 16:45
aplens@www.pcworld[1].txt	Text Document	1 KB	08.07.02 16:43	08.07.02 16:43
aplens@zdnet[1].txt	Text Document	1 KB	08.07.02 16:43	08.07.02 16:43
index.dat	DAT File	48 KB	14.06.02 01:35	08.07.02 16:39

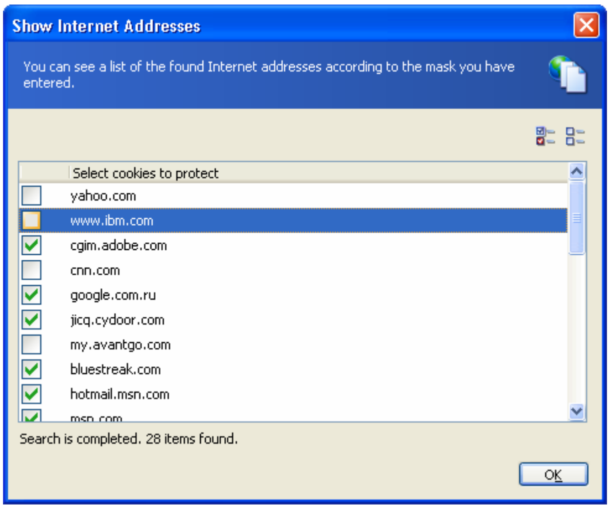
Windows XP Cookies folder content

If Netscape Navigator is your default browser, cookies are kept in the single **cookies.txt** file in the user profile folder – by default in C:\Documents and Settings\<user name>\Application Data\Mozilla\Profiles\<profile name>.

You can protect selected cookies and delete all others:

1. select **Cookies** from the **Internet Components** group;
2. select «**Addresses**» and click the Show URLs button;
3. uncheck boxes next to the cookies you want to **keep** after running the PC or components clean-up utility.

Fully cleaning your PC, Acronis Privacy Expert Suite will destroy all cookies **except those protected.**



You can see a list of the found Internet addresses according to the mask you have entered.

	Select cookies to protect
□	yahoo.com
□	www.ibm.com
☑	cgim.adobe.com
□	cnn.com
☑	google.com.ru
☑	jicq.cydoor.com
□	my.avantgo.com
☑	bluestreak.com
☑	hotmail.msn.com
☑	msn.com

Search is completed. 28 items found.

«Protected Cookies» setting

4.2.3 Downloaded components

In this guide, downloaded components refers to **ActiveX elements**. These can be installed on a PC without the user's knowledge as various sites are visited.

ActiveX elements enable dynamic content on Web pages instead of just static viewing. ActiveX elements can provide Internet access to video and cartoons, enable complex controls and menus, and/or organize user interaction with the site in many complex ways.

The threat of ActiveX elements is that they can be used malevolently. Using an ActiveX element, its creator can get access to your PC resources. ActiveX elements can be used to search your hard disk for passwords, your ISP site, to damage or delete disk files or folders, or to format a disk or make computers inoperable in a wide variety of ways.

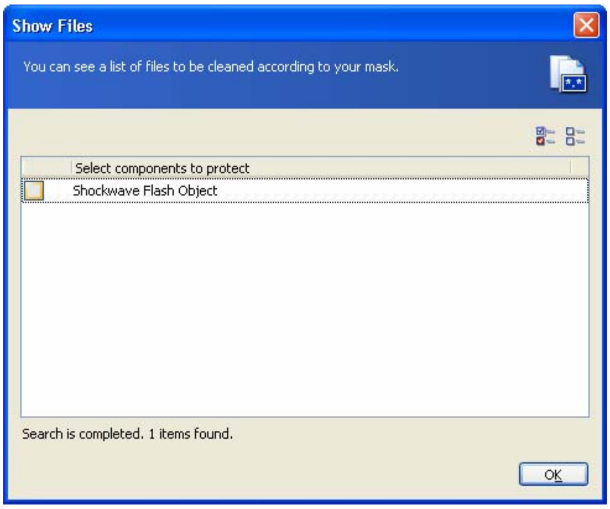
Downloaded ActiveX components clean-up enables you to delete installed elements that may have doubtful use. If you have accidentally downloaded an ActiveX element from a dubious site, Acronis Privacy Expert Suite will help you to delete it from your hard disk drive.

You can control downloads of ActiveX elements to your hard disk to a certain extent by setting an appropriate security level for Internet access. Still, it is nearly impossible to fully control all ActiveX elements.

If you wish to control installed downloaded components:

1. select **Downloaded components** clean-up in the settings editor.
2. select «**Files**» and click the Show Files button;
3. uncheck boxes near the names of components you want to **keep** on your PC.

When cleaning your PC, Acronis Privacy Expert Suite destroy all downloaded components **except protected** ones.



You can see a list of files to be cleaned according to your mask.

Select components to protect

□ Shockwave Flash Object

Search is completed. 1 items found.

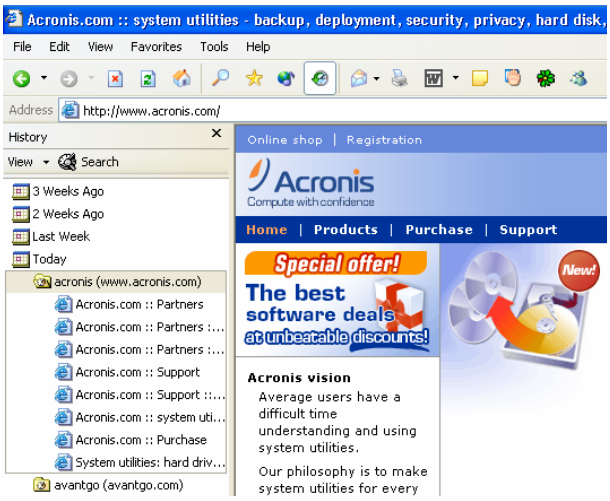
«Protected components» setting

4.2.4 Last Visited Pages

Last visited pages clean-up removes Web address lists for selected browsers, according to the Address parameter.

If this parameter hasn't been set, the suite removes all Last visited pages information.

In the setup mode, you can browse addresses to delete in the "Show URLs" window to deselect any you want to keep by unchecking corresponding boxes.


Acronis.com :: system utilities - backup, deployment, security, privacy, hard disk,
File
Edit
View
Favorites
Tools
Help
Address
History
View
Search
Online shop | Registration
Acronis
Compute with confidence
Home | Products | Purchase | Support
Special offer!
The best software deals at unbeatable discounts!
New!

http://www.acronis.com/

3 Weeks Ago
2 Weeks Ago
Last Week
Today
acronis (www.acronis.com)
Acronis.com :: Partners
Acronis.com :: Partners :...
Acronis.com :: Partners :...
Acronis.com :: Support
Acronis.com :: Support ::...
Acronis.com :: system uti...
Acronis.com :: Purchase
System utilities: hard driv...
avantgo (avantgo.com)

Acronis vision

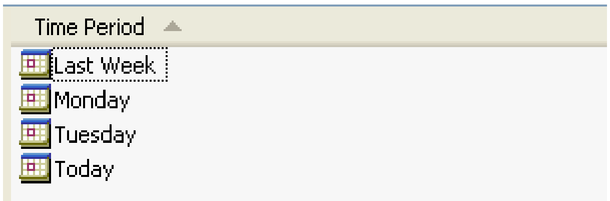
Average users have a difficult time understanding and using system utilities.

Our philosophy is to make system utilities for every

Internet Explorer History list

In Microsoft Internet Explorer, the list of visited pages is kept in the History log located in C:\Documents and Settings\<user name>\Local

Settings\History\History.IE5 (Windows XP). Here you can find system files and folders, whose contents are represented by Windows Explorer as **Last week, Monday, Tuesday**, etc., **Today** folders.

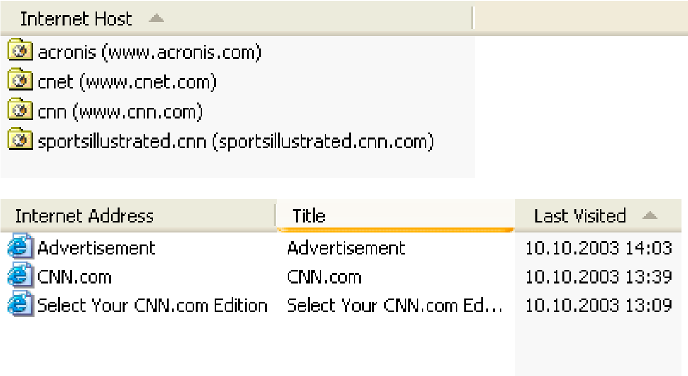


Time Period ▲

- Last Week
- Monday
- Tuesday
- Today

Internet Explorer History folders

These folders also have **index.dat** files that contain folders named according to Web sites visited, e.g. **AFAB Media Services (www.afab.com)** with URLs of particular visited pages.



Internet Host ▲

- acronis (www.acronis.com)
- cnet (www.cnet.com)
- cnn (www.cnn.com)
- sportsillustrated.cnn (sportsillustrated.cnn.com)

Internet Address	Title	Last Visited ▲
Advertisement	Advertisement	10.10.2003 14:03
CNN.com	CNN.com	10.10.2003 13:39
Select Your CNN.com Edition	Select Your CNN.com Ed...	10.10.2003 13:09

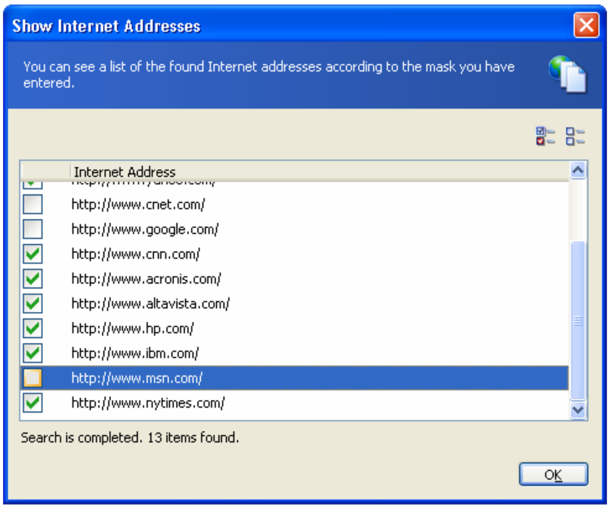
Web site folders and visited pages addresses in Internet Explorer History

Netscape Navigator (Mozilla) also keeps track of similar lists, but keeps them in its own folders.

Acronis Privacy Expert Suite cleans up all visited Web sites lists either entered manually, or by selecting links with mouse.

4.2.5 Typed URLs

Internet browsers usually keep track of Web sites, whose URLs were typed in. This relieves you from typing them in repeatedly. However, at the same time, it allows unauthorized people to see what pages you have visited.



Show Internet Addresses

You can see a list of the found Internet addresses according to the mask you have entered.

	Internet Address
□	http://www.cnet.com/
□	http://www.google.com/
☑	http://www.cnn.com/
☑	http://www.acronis.com/
☑	http://www.altavista.com/
☑	http://www.hp.com/
☑	http://www.ibm.com/
□	http://www.msn.com/
☑	http://www.nytimes.com/

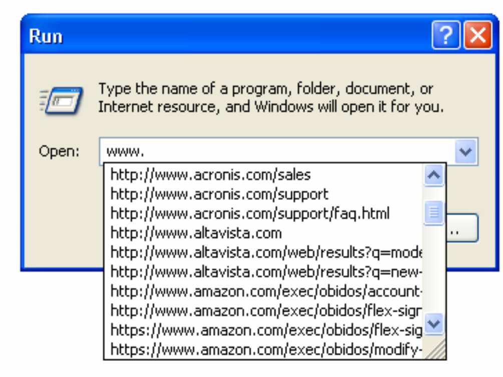
Search is completed. 13 items found.

Typed URLs list

You can securely clean up the typed URLs list using the **Typed URLs** component found in the **Internet components clean-up** group**.**

In the setup mode, you can browse addresses to delete in the "Show URLs" window and deselect any you want to keep by unchecking corresponding boxes.

Note that you can enter the address in the **Open** field of the **Run** item invoked from the Start menu. Clicking OK in this window opens the corresponding Web site in the default browser. The Visited pages list clean-up cleans the **Run** window list as well.



Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: www.

http://www.acronis.com/sales
http://www.acronis.com/support
http://www.acronis.com/support/faq.html
http://www.altavista.com
http://www.altavista.com/web/results?q=mode
http://www.altavista.com/web/results?q=new-
http://www.amazon.com/exec/obidos/account-
http://www.amazon.com/exec/obidos/flex-sigr
https://www.amazon.com/exec/obidos/flex-sig
https://www.amazon.com/exec/obidos/modify-

Visited pages list in the «Run» window

No Web addresses are removed during the **Run** clean-up (see the section 4.1.9 Windows Run List, but only the names of executed applications and opened files.

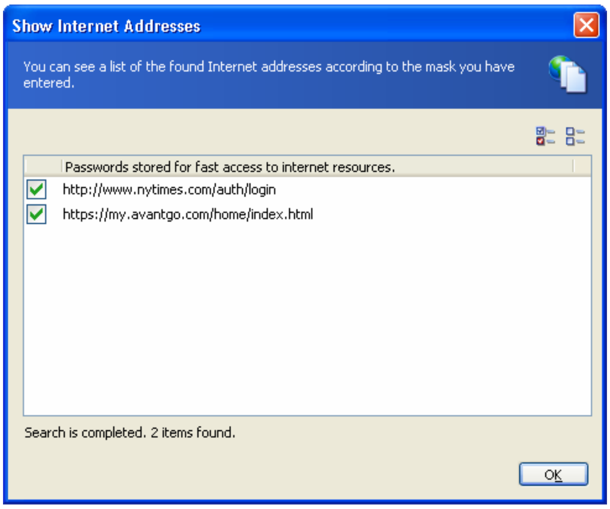
4.2.6 Passwords

Internet browsers can save your passwords for Web sites that require authorization, so you won't have to enter them again. However, if other people use the same PC, they can easily gain access to your password-protected information and that is often confidential.

You can prevent this using the **Passwords clean-up** component of Acronis Privacy Expert Suite.

In the Address settings (**Show URLs** window) you can see the list of Web sites that require user authorization.

If you don’t want to clean Password autocomplete for any Web site, uncheck the corresponding box in this list.



Show Internet Addresses

You can see a list of the found Internet addresses according to the mask you have entered.

Passwords stored for fast access to internet resources.

☑ http://www.nytimes.com/auth/login

☑ https://my.avantgo.com/home/index.html

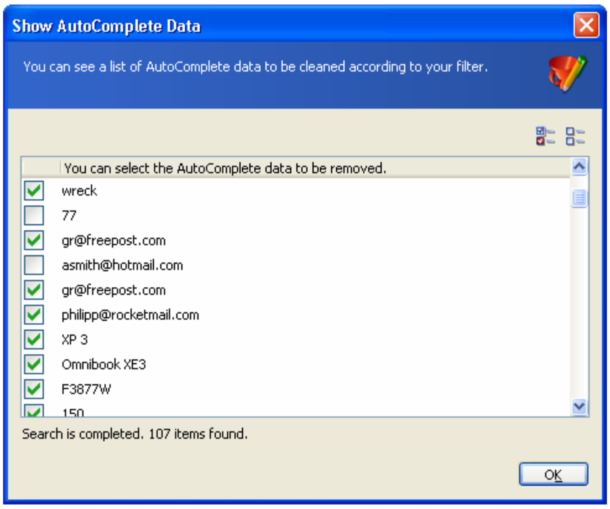
Search is completed. 2 items found.

Passwords clean-up settings

Note that the **Password clean-up** removes only particular autocomplete lists. To clean up user lists stored for **Login** fields use **Forms autocomplete clean-up.**

4.2.7 Forms autocomplete clean-up

The **Forms autocomplete clean-up** enables you to easily and securely destroy all lists kept by your browser to autocomplete forms on some Web sites, including polls, questionnaires, etc. Such information usually includes user names, e-mail addresses, mailboxes, phone numbers and other confidential data.



Show AutoComplete Data

You can see a list of AutoComplete data to be cleaned according to your filter.

You can select the AutoComplete data to be removed.

☑ wreck

□ 77

☑ gr@freepost.com

□ asmith@hotmail.com

☑ gr@freepost.com

☑ philipp@rocketmail.com

☑ XP 3

☑ Omnibook XE3

☑ F3877W

☑ 150

Search is completed. 107 items found.

Forms autocomplete clean-up settings

Using **Forms autocomplete clean-up** you can securely prevent other people from gaining access to this information.

By default, **Forms autocomplete** cleans up all autocomplete fields stored by your Internet browser for future use.

In the **settings** of this component, you can see the list of fields to be cleaned up.

If you want to keep some of the fields, uncheck the corresponding boxes.

4.2.8 E-mail messages

This clean-up component allows you to permanently delete all or selected e-mail in the selected folders of MS Outlook or Outlook Express.

By default, all messages are permanently deleted from folders provided in **Properties → Messages folders.**

Using the **Properties → Messages filter** parameter, you can select messages by Path, E-mail address, Sender name, Recipient name, Subject or Date.

You should use wildcards for filtering. For example, to filter out all messages with «Weekend» in the subject, you should enter the following in the search line:

weekend

The suite searches both whole and partial words.

This will allow you to delete only those messages that meet the chosen criteria.

Note that this component removes only **local e-mail messages**. Messages stored on the mail server accessed over IMAP or by Microsoft Exchange can't be deleted by it.

4.2.9 E-mail contacts

The **E-mail contacts clean-up** allows you to permanently delete **Address book** contacts stored by MS Outlook Express and **Contacts** stored by Microsoft Outlook.

You can select the e-mail client for contacts clean-up in **Properties → E-mail clients.**

By default, the suite permanently deletes all contacts in the selected e-mail clients.

You can select contacts to delete using **Properties → Contacts filter.**

You should use wildcards for filtering. For example, to filter out all contacts that contain **John**, you should enter the following in the search line:

john

The suite searches both whole and partial words.

This will allow you to delete only those contacts that meet the chosen criteria.

4.3 Spyware clean-up

Today there are lots of applications that can operate secretly once on your PC. Their actions might include gathering your personal information, changing user

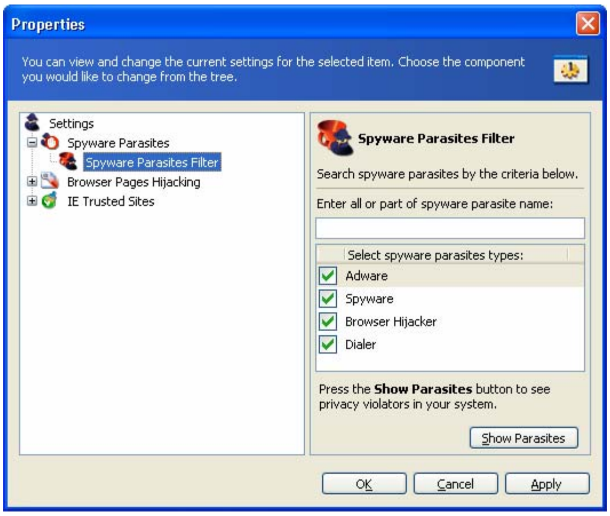
PC and Internet settings without permission, etc. These applications are called spyware.

4.3.1 Spyware threats

This category includes the following applications that operate secretly:

- **Adware** – a kind of Internet marketing where ad banners are implemented into freeware and shareware. While using such applications, the user has to see banners sent over the Internet. This increases traffic and slows down the Internet connection
- **Spyware** – These are applications that secretly gather and transfer personal information to a third party without your knowledge or consent. Spyware might be included in various products, including commercial
- **Browser hijacking** – that change Home, search, and other pages for your Internet browsers
- **Dialers** – these can secretly establish an Internet connection to load usually adult content

In the **Settings** of this component, you can select the spyware kind to clean up. By default, it is set to remove any kind of spyware.



You can view and change the current settings for the selected item. Choose the component you would like to change from the tree.

Spyware Parasites Filter

Search spyware parasites by the criteria below.

Enter all or part of spyware parasite name:

Select spyware parasites types:

☑ Adware
☑ Spyware
☑ Browser Hijacker
☑ Dialer

Press the **Show Parasites** button to see privacy violators in your system.

Spyware threats settings

4.3.2 Browser pages hijacking

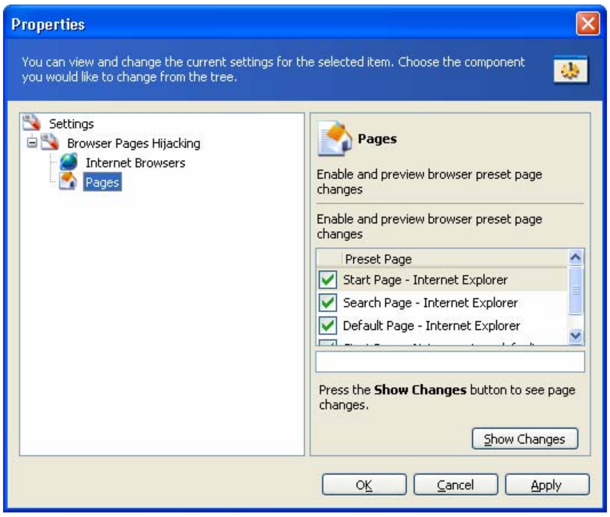
Internet browsers have **preset Web pages** that load automatically under particular conditions. These include the **home page** that is loaded along with the browser, **search page**, and **default page.**

Some applications can secretly change these pages, and in most cases, users can't restore the previous settings themselves, as all changes are made to Windows registry.

Browser pages hijacking clean-up easily solves this problem by remembering preset Web pages to restore in case they are changed.

In the Browser pages hijacking settings you can:

- provide browser(s) to restore preset pages. It supports and automatically locates the following browsers: MS Internet Explorer, Netscape Navigator and Mozilla
- provide the type of preset pages to restore in case they are secretly changed.



You can view and change the current settings for the selected item. Choose the component you would like to change from the tree.

Enable and preview browser preset page changes

Enable and preview browser preset page changes

☑ Start Page - Internet Explorer
☑ Search Page - Internet Explorer
☑ Default Page - Internet Explorer

Press the **Show Changes** button to see page changes.

Preset pages settings

4.3.3 IE Trusted Sites

In the MS Internet Explorer settings, you can set **Trusted sites** – Web sites to browse with less security.

Usually this list is formed by users, however there are applications that can secretly add addresses to the Trusted sites list.

You can use the **Trusted sites** component to clean this list up.

By default, the suite removes all trusted Web site addresses. However using **Properties → Show URLs**, you can see the list of trusted addresses and deselect those you want to save.

Chapter 5. Acronis Privacy Expert Pop-up Blocker

5.1 What are pop-ups?

While browsing some Web sites you might have unwanted pop-up windows open along with the Web site you are browsing. As a rule, pop-ups contain bothersome advertising. They slow down your Internet connection speed and increase the traffic you pay for.

5.2 Acronis Privacy Expert Pop-up Blocker

Acronis Privacy Expert Pop-up Blocker automatically prevents windows from popping up except the one the user wants to view.

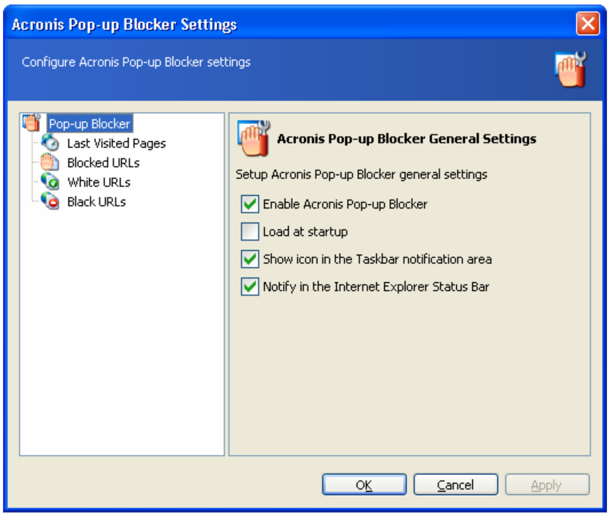
If you haven't activated Pop-up Blocker during installation, you can do it anytime by clicking **Run Pop-up Blocker. Then** the Pop-up Blocker icon will appear in the System tray.

In the future, you will be able to invoke Pop-up Blocker settings by double-clicking the icon.

5.3 Pop-up Blocker settings

You can invoke the Pop-up Blocker settings window in the following ways:

- By selecting Pop-up Blocker in **Settings** on the sidebar of the Acronis Privacy Expert Suite main window
- By selecting a similar item in the **main menu**
- By double-clicking the Pop-up Blocker **icon** in the system tray with the left mouse button (this works only if Pop-up Blocker is already running).



Acronis Pop-up Blocker General Settings

Setup Acronis Pop-up Blocker general settings

☑ Enable Acronis Pop-up Blocker

☐ Load at startup

☑ Show icon in the Taskbar notification area

☑ Notify in the Internet Explorer Status Bar

Pop-up Blocker Settings

5.3.1 Acronis Privacy Expert Pop-up Blocker general settings

In the general settings section, you can enable or disable the following:

- Enable Acronis Privacy Expert Pop-up Blocker
- Load it at startup
- Show the Pop-up Blocker icon in the system tray
- Check on its status in the IE status bar

5.3.2 Browsed history

The **Browsed history** section is an exact representation of **Microsoft Internet Explorer History.**

In this list, you can select Web sites to move to either White, or Black list.

5.3.3 Blocked URLs

In this section you can see what Web sites contained pop-ups that were blocked.

You can move any of these to either the White or Black list.

5.3.4 White URLs

If you want to cancel Acronis Privacy Expert Pop-up Blocker for a particular Web site, you can move it to the White (approved) list:

- By clicking "New" and entering it manually
- By selecting the address and clicking "Add" in the **History, Blocked URLs**, and **Black list**

5.3.5 Black URLs

If necessary, you can use Acronis Pop-up Blocker to block a Web site by adding its address to the Black (rejected) list. In this case, you will see "Acronis Privacy Expert Pop-up Blocker: Black URL link – navigation stopped" message in the browser when trying to access this Web site.

Chapter 6. Acronis Drive Cleanser

6.1 Acronis Drive Cleanser capabilities

Many operating systems do not provide users with enough data destruction tools, so deleted files can be restored easily by simple applications. Even complete disk reformatting can't guarantee permanent confidential data destruction.

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

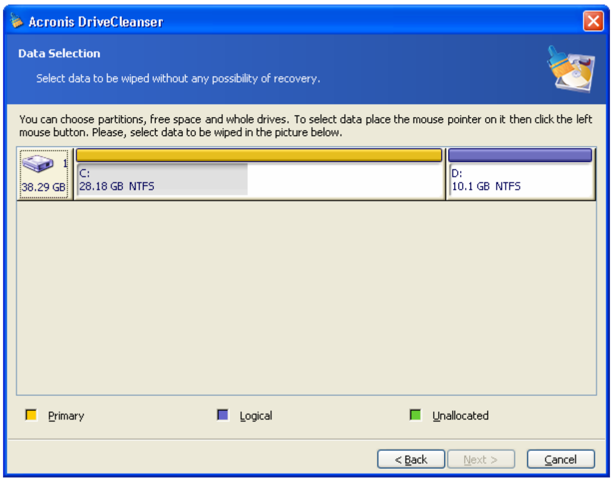
6.2 Working with Acronis Drive Cleanser

Acronis Drive Cleanser allows to perform the following:

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

Acronis Drive Cleanser is based on a **wizard** that **scripts** all hard disk operations, so no data destruction is performed until you execute the complete script. At any stage, you can return to the previous stages to select other disks or partitions or data destruction methods.

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



Acronis DriveCleanser

Data Selection

Select data to be wiped without any possibility of recovery.

You can choose partitions, free space and whole drives. To select data place the mouse pointer on it then click the left mouse button. Please, select data to be wiped in the picture below.

The list of PC hard disks with partitions

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

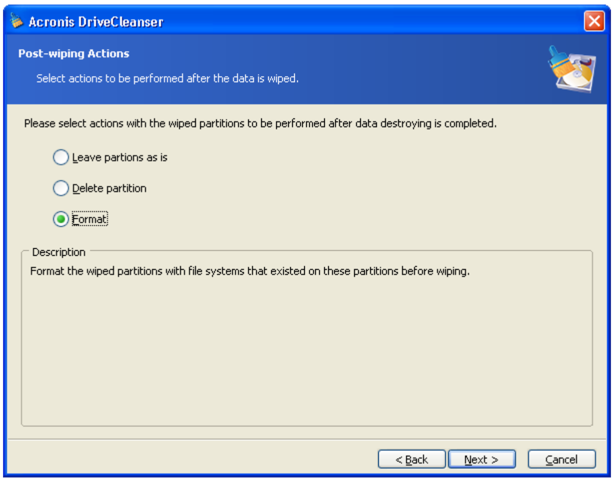
You can select an entire hard disk or several disks for data destruction. To do this, click the rectangle corresponding to the hard disk (with a device icon, disk number and capacity.)

You can select several partitions simultaneously located on different hard disks or on several disks.

Click Next to continue.

In the **Final actions** window, you can select actions to be performed on the partitions selected for data destruction. Acronis Drive Cleanser offers you three variants:

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



Post-wiping Actions

Select actions to be performed after the data is wiped.

Please select actions with the wiped partitions to be performed after data destroying is completed.

○ Leave partions as is

○ Delete partition

● Format

Description

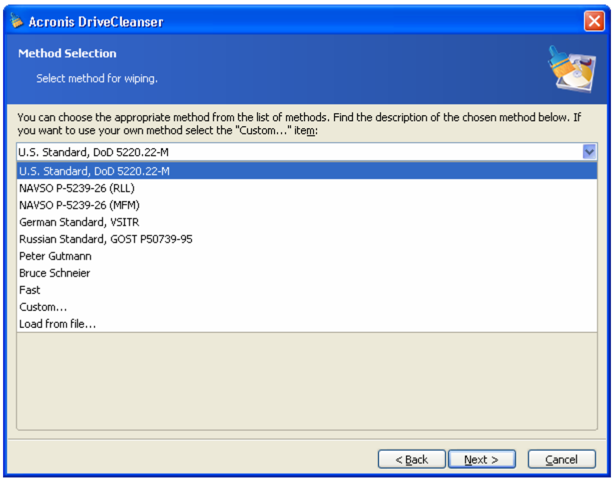
Format the wiped partitions with file systems that existed on these partitions before wiping.

Final actions window

In this example, the switch is set to **Leave partition as is.** This will allow you to see the results of partition data destruction only.

6.3 Using preset data destruction methods

Acronis Drive Cleanser utilizes a number of the most popular data destruction methods that are described in detail in Appendix «Information wiping methods used by » of this manual.



Method Selection

Select method for wiping.

You can choose the appropriate method from the list of methods. Find the description of the chosen method below. If you want to use your own method select the "Custom..." item:

U.S. Standard, DoD 5220.22-M

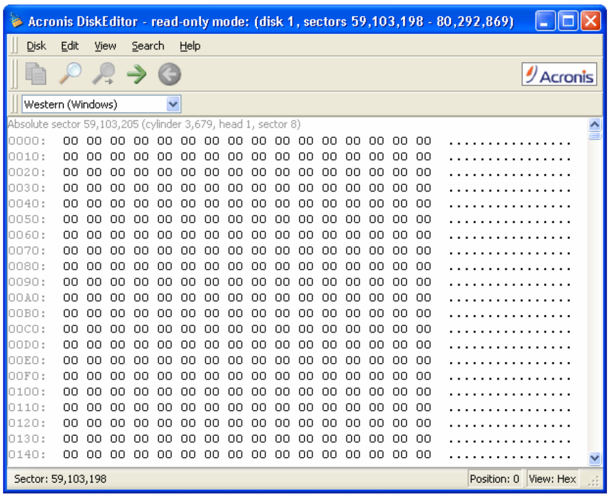
U.S. Standard, DoD 5220.22-M
NAVSO P-5239-26 (RLL)
NAVSO P-5239-26 (MFM)
German Standard, VSITR
Russian Standard, GOST P50739-95
Peter Gutmann
Bruce Schneier
Fast
Custom...
Load from file...

The list of preset methods

After you select an method, Acronis Drive Cleanser will perform all actions necessary to destroy contents of the selected partition or disk. After this is done, you will see a message indicating the successful data destruction.

Acronis Drive Cleanser offers you another useful capability — to estimate the results of executing a data destruction method on a hard disk or partition. It features an integrated **DiskViewer hard disk browsing tool.**

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



```
Acronis DiskEditor - read-only mode: (disk 1, sectors 59,103,198 - 80,292,869)
Western (Windows)
Absolute sector 59,103,205 (cylinder 3,679, head 1, sector 8)
0000:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0010:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0020:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0030:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0040:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0050:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0060:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0070:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0080:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0090:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00A0:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00B0:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00C0:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00D0:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00E0:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00F0:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0100:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0110:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0120:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0130:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0140:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
Sector: 59,103,198                                    Position: 0   View: Hex
```

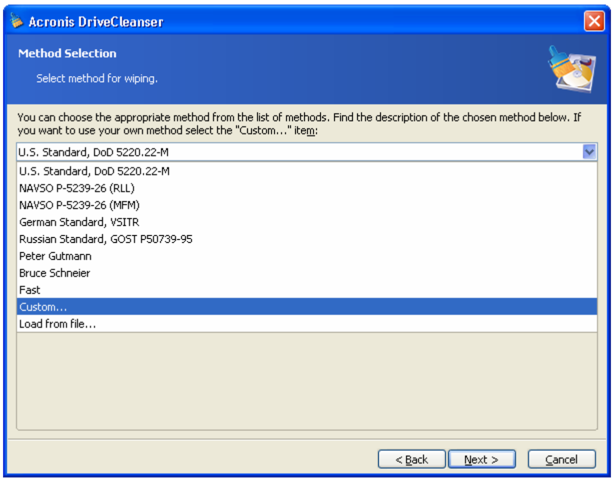
DiskViewer window

6.4 Creating custom methods of data destruction

Acronis Drive Cleanser gives you an opportunity to create your own methods for wiping hard disks. Although the software includes methods of all classes, you may choose your own methods.

6.4.1 Creating custom methods

To create a custom method of hard disk wiping, select and mouse-click the «Custom…» line from the drop-down list in the **Method selection** window. Please pay close attention to the load method option in the same drop-down list.



Method Selection

Select method for wiping.

You can choose the appropriate method from the list of methods. Find the description of the chosen method below. If you want to use your own method select the "Custom..." item:

U.S. Standard, DoD 5220.22-M

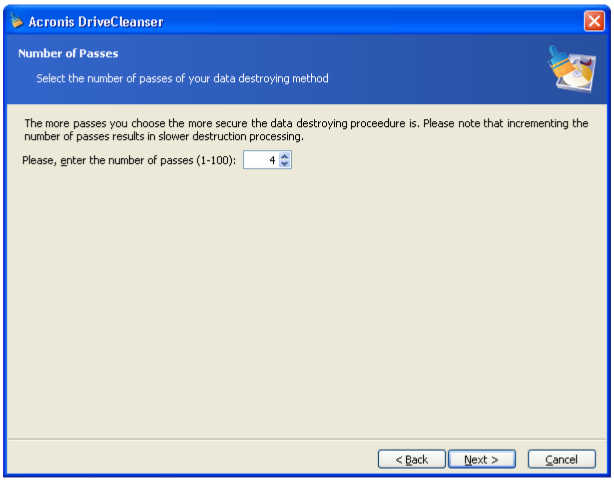
- U.S. Standard, DoD 5220.22-M
- NAVSO P-5239-26 (RLL)
- NAVSO P-5239-26 (MFM)
- German Standard, VSITR
- Russian Standard, GOST P50739-95
- Peter Gutmann
- Bruce Schneier
- Fast
- Custom...
- Load from file...

The selection of custom method creation

Click the Next button to continue.

The window with the script for wiping a hard disk partition (the partition and/or hard disk was selected during a previous step) shows after the selection of one of the predefined wiping methods. This time the Custom method wizard will be started and you will see the **Number of passes** window.

As an example, let's create a simple custom method similar to the U.S. Department of Defense standard., This standard assumes three passes for a hard disk during which different symbols are written to it, plus one more pass for verification — i.e. four passes total.



Number of Passes

Select the number of passes of your data destroying method

The more passes you choose the more secure the data destroying proceedure is. Please note that incrementing the number of passes results in slower destruction processing.

Please, enter the number of passes (1-100): 4

The window with number of passes of the custom method

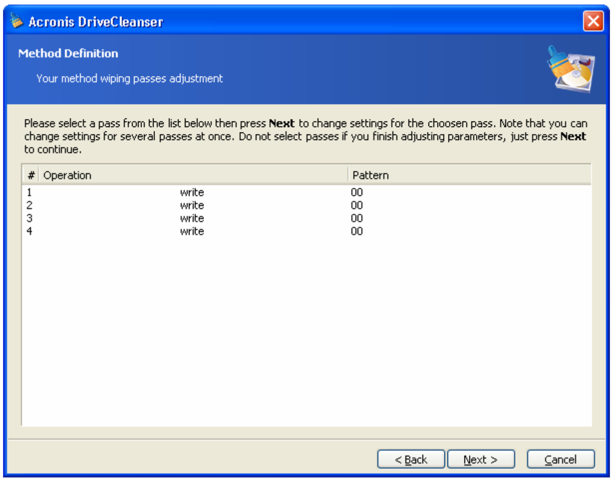
Remember, the predefined wiping methods perform from one (fast method, the Russian standard) to up to 35 passes (Peter Gutmann's method).

You may enter any value into the spinner field of the wizard window with the keyboard or mouse. For our example, enter 4 into this field.

Click the Next button to continue.

6.4.2 Method definition: template

The **Method definition** window shows you a template of the future method; the list contains many elements, including the defined method at the previous stage.



Please select a pass from the list below then press **Next** to change settings for the choosen pass. Note that you can change settings for several passes at once. Do not select passes if you finish adjusting parameters, just press **Next** to continue.

#	Operation	Pattern
1	write	00
2	write	00
3	write	00
4	write	00

The method definition window

The window has the following legend: The first column of the list contains the number of passes for a disk; the second contains the type of operation on a disk (there are just two: to write a symbol to disk, «writing», and to verify written, «verification»); the third column contains the pattern of data to be written to disk.

The pattern to be written is always a hexadecimal value, for example, a value of this kind: 0x00, 0xAA, or 0xCD, etc. These values are 1 byte long, but they may be up to 512 bytes long. Except for such values, you may enter a random hexadecimal value of any length (up to 512 bytes). Your method may also include one more value for writing that is designated as the «complementary value» – the value that is complementary to the one written to disk during the previous pass.

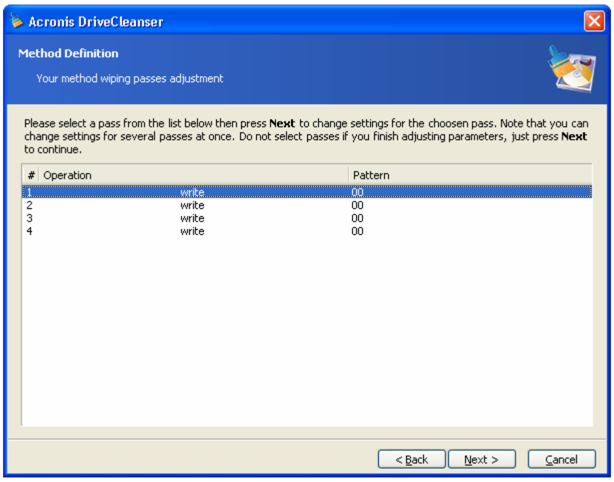
If the binary value is represented by 10001010 (0x8A) sequence, then the complementary binary value will be represented by 01110101 (0x75) sequence.

Thus you may include the following values in method:

- Any hexadecimal value 1 – 512 bytes long
- Random hexadecimal values 1 – 512 bytes long
- Hexadecimal values, complementary to those written to hard disk during the previous pass

The **Method definition** window offers you the template for the method only. You should define exactly what the software should write to disk to destroy the confidential data according to your method.

To do this, click your mouse on the line representing pass #1.



Method Definition

Your method wiping passes adjustment

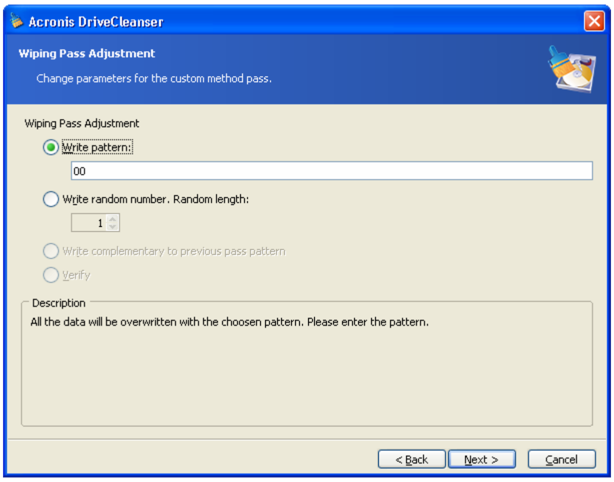
Please select a pass from the list below then press **Next** to change settings for the choosen pass. Note that you can change settings for several passes at once. Do not select passes if you finish adjusting parameters, just press **Next** to continue.

#	Operation	Pattern
1	write	00
2	write	00
3	write	00
4	write	00

The selection of the first pass for pattern definition

Click the Next button to continue.

You will see the window that allows you to define the pattern to be written to disk (hexadecimal value).



Wiping Pass Adjustment

Change parameters for the custom method pass.

Wiping Pass Adjustment

● Write pattern:

00

○ Write random number. Random length:

1

○ Write complementary to previous pass pattern

○ Verify

Description

All the data will be overwritten with the choosen pattern. Please enter the pattern.

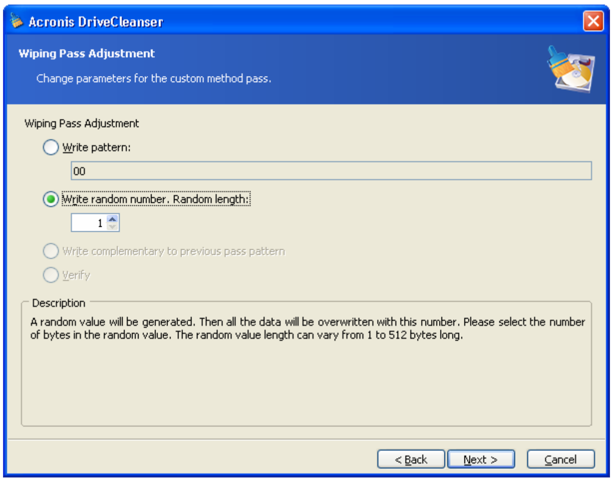
The wiping pass adjustment window for definition of patterns to be written

In this figure, the switch is set to **Write a value** position by default, the hexadecimal value 0x00 is entered into the field.

This is what the window control elements means: You may enter any hexadecimal value into the field under the **Write a value** switch to write it to a hard disk during any pass (during the first pass in this case).

By setting the switch to **Write a random value** position, you first will select write a random value to disk, and specify the length of random value in bytes in the spinner field below.

The U.S. standard provides the writing of random values to each byte of each disk sector during the first pass, so set the switch to **Write a random value** position and enter 1 into field.



Wiping Pass Adjustment

Change parameters for the custom method pass.

Wiping Pass Adjustment

○ Write pattern:

00

● Write random number. Random length:

1

○ Write complementary to previous pass pattern

○ Verify

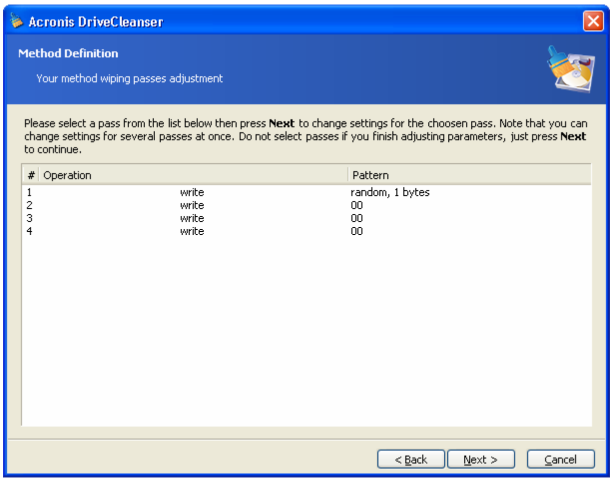
Description

A random value will be generated. Then all the data will be overwritten with this number. Please select the number of bytes in the random value. The random value length can vary from 1 to 512 bytes long.

The input of a random 1-byte value as the pattern for writing

Click the Next button to continue.

You will be taken to the method definition window again and will see that the former record (1 – write – 00) was replaced by 1 – write – random value, 1 byte.



Method Definition

Your method wiping passes adjustment

Please select a pass from the list below then press **Next** to change settings for the choosen pass. Note that you can change settings for several passes at once. Do not select passes if you finish adjusting parameters, just press **Next** to continue.

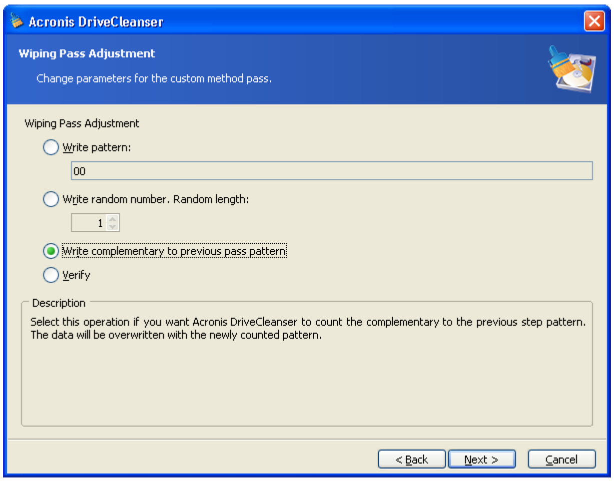
#	Operation	Pattern
1	write	random, 1 bytes
2	write	00
3	write	00
4	write	00

The first pass of the custom method is defined

To define the next pass, select the second line of the list and click the Next button.

You will see the already-familiar window, but this time there will be more switch positions available: two additional positions will be available for selection:

- **Previous step complementary value**
- **Verify.**



Wiping Pass Adjustment

Change parameters for the custom method pass.

Wiping Pass Adjustment

○ Write pattern:

00

○ Write random number. Random length:

1

● Write complementary to previous pass pattern

○ Verify

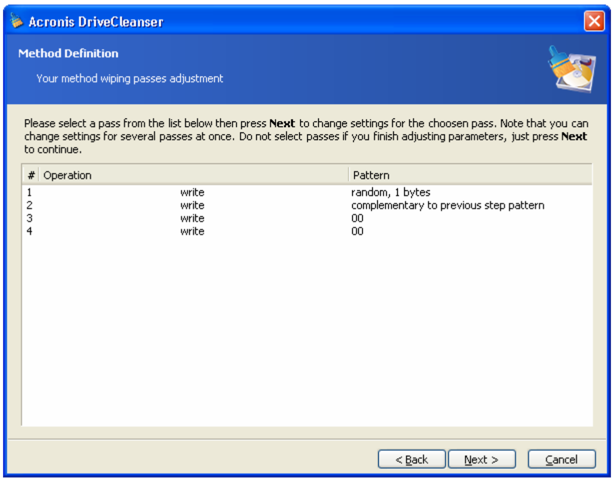
Description

Select this operation if you want Acronis DriveCleanser to count the complementary to the previous step pattern. The data will be overwritten with the newly counted pattern.

The input of value complementary to the one written during the previous pass

As during the second pass of the U.S. standard each disk sector is filled with hexadecimal values that are complementary to those written during the previous pass. Therefore you should set the switch to the **Previous step complementary value** position and click the Next button.

You will be taken to the method definition window again. In this window the second record looked like this before: 2 – write – 00, and it was replaced by: 2 – write – previous step complementary value**.**



Method Definition

Your method wiping passes adjustment

Please select a pass from the list below then press **Next** to change settings for the choosen pass. Note that you can change settings for several passes at once. Do not select passes if you finish adjusting parameters, just press **Next** to continue.

#	Operation	Pattern
1	write	random, 1 bytes
2	write	complementary to previous step pattern
3	write	00
4	write	00

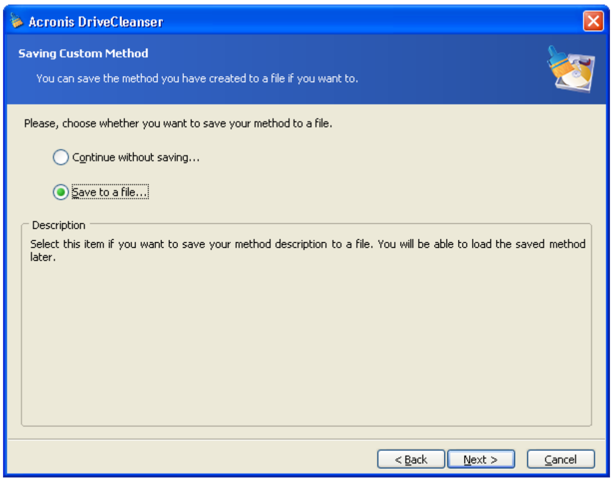
The second pass of the custom method is defined

Following the U.S. data destruction standard specification, define third and fourth data overwriting passes.

In the same way, you can create any data destruction method to match your security requirements.

6.4.3 Saving a custom method to file

In the next **Saving custom method** window, you will be able to save the method you have created. This will be useful if you are going to use it again.



Saving Custom Method

You can save the method you have created to a file if you want to.

Please, choose whether you want to save your method to a file.

○ Continue without saving...

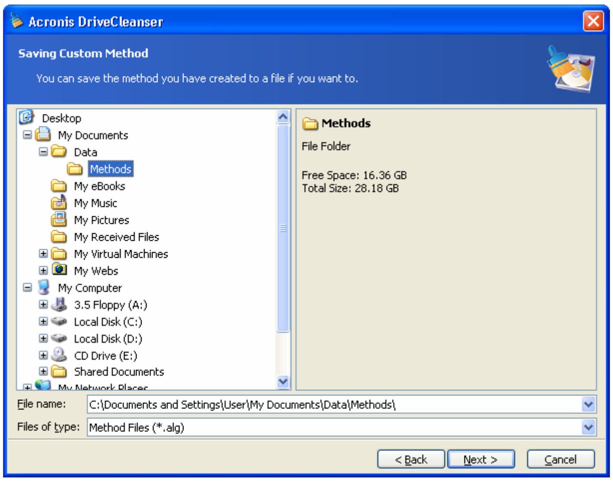
● Save to a file...

Description

Select this item if you want to save your method description to a file. You will be able to load the saved method later.

The saving custom method window

In order do save your method, you need to give it a filename and define the path in the Select file field or click the Browse button to locate an existing file on the disk. You should also enter a brief description of your method.



Saving Custom Method

You can save the method you have created to a file if you want to.

Methods

File Folder

Free Space: 16.36 GB
Total Size: 28.18 GB

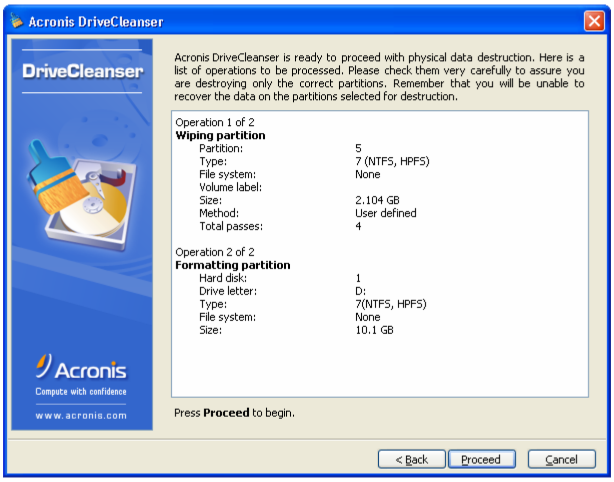
File name: C:\Documents and Settings\User\My Documents\Data\Methods\

Files of type: Method Files (*.alg)

The method filename and description window

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

As all passes of your method are defined and the method is saved to file, clicking the Next button will let you see the window with the generated wiping script based on your custom method.



Acronis DriveCleanser is ready to proceed with physical data destruction. Here is a list of operations to be processed. Please check them very carefully to assure you are destroying only the correct partitions. Remember that you will be unable to recover the data on the partitions selected for destruction.

Operation 1 of 2
Wiping partition

Partition:	5
Type:	7 (NTFS, HPFS)
File system:	None
Volume label:	
Size:	2.104 GB
Method:	User defined
Total passes:	4

Operation 2 of 2
Formatting partition

Hard disk:	1
Drive letter:	D:
Type:	7(NTFS, HPFS)
File system:	None
Size:	10.1 GB

Press **Proceed** to begin.

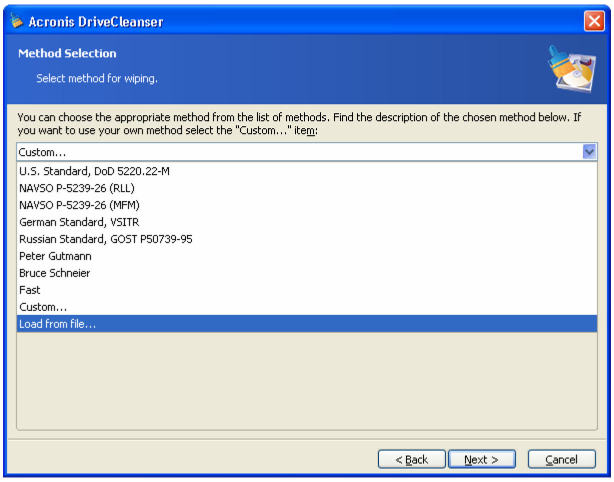
The script of data destruction, based on the custom method

By clicking the Proceed button, you will execute the generated script.

6.4.4 Loading an method from a file

If you created and saved your method for data destruction while working with Acronis Privacy Expert Suite software, you can use it in the following way:

In the **Select Method** window, choose **Load from file…** from the drop-down list and select the file with custom data destruction method parameters. By default, such files have *.alg extension.



Method Selection

Select method for wiping.

You can choose the appropriate method from the list of methods. Find the description of the chosen method below. If you want to use your own method select the "Custom..." item:

Custom...

- U.S. Standard, DoD 5220.22-M
- NAVSO P-5239-26 (RLL)
- NAVSO P-5239-26 (MFM)
- German Standard, VSITR
- Russian Standard, GOST P50739-95
- Peter Gutmann
- Bruce Schneier
- Fast
- Custom...
- Load from file...

Method selection: loading from file

6.5 Creating a bootable diskette or CD with Acronis Drive Cleanser

If you haven't created a bootable diskette or CD with Acronis Drive Cleanser during installation Acronis Privacy Expert Suite, you can do it later using the **Bootable Media Builder.**

This diskette or CD will allow you to easily and permanently destroy data on your PC that doesn’t have Acronis Privacy Expert Suite installed.

To create a bootable diskette, select **Bootable Media Builder** on sidebar and follow the **wizard** instructions.

Appendix A. Hard Disk Wiping methods

Information removed from a hard disk drive by non-secure means (for example, by simple Windows delete) can easily be recovered. Utilizing specialized equipment, it is possible to recover even repeatedly overwritten information. Therefore, guaranteed data wiping is more important now than ever before.

The **guaranteed wiping of information** from magnetic media (e.g. a hard disk drive) means it is impossible to recover data by even a qualified specialist with the help of all known tools and recovery methods.

This problem can be explained in the following way: Data is stored on a hard disk as a binary sequence of 1 and 0 (ones and zeros), represented by differently magnetized parts of a disk.

Generally speaking, a 1 written to a hard disk is read as 1 by its controller, and 0 is read as 0. However, of you write 1 over 0, the result is conditionally 0.95 and vice versa – if 1 is written over 1 the result is 1.05. These differences are irrelevant for the controller. However, using special equipment, one can easily read the «underlying» sequence of 1 and 0.

It only requires specialized software and inexpensive hardware to read data «deleted» this way by analyzing magnetization of hard disk sectors, residual magnetization of track sides and/or by using current magnetic microscopes.

Writing to magnetic media leads to subtle effects summarized as follows: every track of a disk stores **an image of every record** ever written to it, but the effect of such records (magnetic layer) becomes more subtle as time passes.

A.1 Information wiping methods functioning principles

Physically, the complete wiping of information from a hard disk involves the switching of every elementary magnetic area of the recording material as many times as possible by writing specially selected sequences of logical 1 and 0 (also known as samples).

Using logical data encoding methods in current hard disks, you can select **samples** of symbol (or elementary data bit) sequences to be written to sectors in order to **repeatedly and effectively wipe confidential information.**

Methods offered by national standards provide (single or triple) recording of random symbols to disk sectors that are **straightforward and arbitrary decisions, in general**, but still acceptable in simple situations. The most effective information-wiping method is based on deep analysis of subtle features of recording data to all types of hard disks. This knowledge speaks to the necessity of complex multipass methods to **guarantee** information wiping.

The detailed theory of guaranteed information wiping is described in an article by Peter Gutmann. Please see:

http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html.

A.2 Information wiping methods used by Acronis

The table below briefly describes information wiping methods used by Acronis. Each description features the number of hard disk sector passes along with the number(s) written to each sector byte.

The description of built-in information wiping methods

NN	Algorithm (writing method)	Passes	Record
1.	United States Department of Defense 5220.22-M	4	1st pass – randomly selected symbols to each byte of each sector, 2 – complementary to written during the 1st pass; 3 – random symbols again; 4 – writing verification.
2.	United States: NAVSO P-5239-26 (RLL)	4	1st pass – 0x01 to all sectors, 2 – 0x27FFFFFF, 3 – random symbol sequences, 4 – verification.
3.	United States: NAVSO P-5239-26 (MFM)	4	1st pass – 0x01 to all sectors, 2 – 0x7FFFFFFF, 3 – random symbol sequences, 4 – verification.
4.	German: VSITR	7	1st – 6th – alternate sequences of: 0x00 and 0xFF; 7th – 0xAA; i.e. 0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF, 0xAA.
5.	Russian: GOST P50739-95	1	Logical zeros (0x00 numbers) to each byte of each sector for 6th to 4th security level systems. Randomly selected symbols (numbers) to each byte of each sector for 3rd to 1st security level systems.
6.	Peter Gutmann's method	35	Peter Gutmann's method is very sophisticated. It's based on his theory of hard disk information wiping (see http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html).
7.	Bruce Schneier's method	7	Bruce Schneier offers a 7-pass overwriting method in his Applied Cryptography book. 1st pass – 0xFF, 2nd pass – 0x00, and then five times with a cryptographically secure pseudo-random sequence.
8.	Fast	1	Logical zeros (0x00 numbers) to all sectors to wipe.