Ultimate Data Security Tool

User's Manual

Version Number 4.0

Active@ Eraser 4.0 END-USER LICENSE AGREEMENT

~~~~~~

~~~~~~

IMPORTANT-READ CAREFULLY: This End-User License Agreement (“EULA”) is a legal agreement between you (either an individual or a single entity) and The Active Data Security Solutions for the Active@ Eraser later referred to as 'SOFTWARE'. By installing, copying, or otherwise using the SOFTWARE you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, do not install or use the SOFTWARE.

WE REQUIRE ALL OUR DEALERS TO PROVIDE EACH PURCHASER WITH FREE DEMO OF THE SOFTWARE TO GET A FULL UNDERSTANDING OF THE CAPABILITIES AND THE EASE OF USE OF THE SOFTWARE. OUR DEALERS HAD TO RECOMMEND YOU TO DOWNLOAD DEMO. WE WON'T ISSUE ANY REFUNDS AFTER PURCHASING FULL VERSION OF THE SOFTWARE.

Active Data Security Solutions may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. The furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

SOFTWARE LICENSE

1. The SOFTWARE is licensed, not sold. Copyright laws andinternational copyright treaties, as well as other intellectual property laws and treaties protect the SOFTWARE.

2. GRANT OF LICENSE.

(a) FREE DEMO COPY. You may use DEMO SOFTWARE without charge on an evaluation basis to erase any files, folders, partitions and hard drives using the only erasing method [One Pass Zeros]. You must pay the license fee and register your copy to erase data using any other methods including US DoD 5220.22-M.

(b) REDISTRIBUTION OF DEMO COPY. If you are using DEMO SOFTWARE on an evaluation basis you may make copies of the DEMO SOFTWARE as you wish; give exact copies of the original DEMO SOFTWARE to anyone; and distribute the DEMO SOFTWARE in its unmodified form via electronic means (Internet, BBS's, Shareware distribution libraries, CD-ROMs, etc.). You may not charge any fee for the copy or use of the evaluation DEMO SOFTWARE itself, but you may charge a distribution fee that is reasonably related to any cost you incur distributing the DEMO SOFTWARE (e.g. packaging). You must not represent in any way that you are selling the software itself. Your distribution of the DEMO SOFTWARE will not entitle you to any compensation from Active Data Security Solutions. You must distribute a copy of this EULA with any copy of the Software and anyone to whom you distribute the SOFTWARE is subject to this EULA.

(c) REGISTERED COPY. After you have purchased the license(s) for SOFTWARE, and have received the registration key and the SOFTWARE distribution package, you are licensed to use the SOFTWARE by number of persons corresponding to the number of licenses purchased. You can use SOFTWARE as many times as you need (erase as many files, partitions and hard drives as you need) without any limitations on time frame or on number of usages. “Home Use” means that you've purchased a software for personal use only. “Business Use” means that you've purchased a software for use in your business. “Site License” means that you can use SOFTWARE without limitations at one office (one physical location). “Enterprise License” means that you can use SOFTWARE without limitations at all company's branches (worldwide).

You may not duplicate the SOFTWARE in whole or in part, except that you may make one copy of the SOFTWARE for backup or archival purposes. You may terminate this license at any time by destroying the original and all copies of the SOFTWARE in whatever form. You may permanently transfer all of your rights under this EULA provided you transfer all copies of the SOFTWARE (including copies of all prior versions if the SOFTWARE is an upgrade) and retain none, and the recipient agrees to the terms of this EULA.

3. RESTRICTIONS. You may not reverse engineer, decompile, or disassemble the SOFTWARE, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation. You may not rent, lease, or lend the SOFTWARE. You may permanently transfer all of your rights under this EULA, provided the recipient agrees to the terms of this EULA. You may not use the SOFTWARE to perform any unauthorized transfer of information (e.g. transfer of files in violation of a copyright) or for any illegal purpose.

4. SUPPORT SERVICES. Active Data Security Solutions may provide you with support services related to the SOFTWARE. Use of Support Services is governed by the Active Data Security Solutions polices and programs described in the online documentation and web site, and/or other Active Data Security Solutions-provided materials, as they may be modified from time to time. Any supplemental software code provided to you as part of the Support Services shall be considered part of the SOFTWARE and subject to the terms and conditions of this EULA. With respect to technical information you provide to Active Data Security Solutions as part of the Support Services, Active Data Security Solutions may use such information for its business purposes, including for product support and development. Active Data Security Solutions will not utilize such technical information in a form that personally identifies you.

5. TERMINATION. Without prejudice to any other rights, Active Data Security Solutions may terminate this EULA if you fail to comply with the terms and conditions of this EULA. In such event, you must destroy all copies of the SOFTWARE.

6. COPYRIGHT. The SOFTWARE is protected by copyright law and international treaty provisions. You acknowledge that no title to the intellectual property in the SOFTWARE is transferred to you. You further acknowledge that title and full ownership rights to the SOFTWARE will remain the exclusive property of Active Data Security Solutions and you will not acquire any rights to the SOFTWARE except as expressly set forth in this license. You agree that any copies of the SOFTWARE will contain the same proprietary notices which appear on and in the SOFTWARE.

7. DISCLAIMER OF WARRANTY. Active Data Security Solutions expressly disclaims any warranty for the SOFTWARE. THE SOFTWARE AND ANY RELATED DOCUMENTATION IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OR MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. THE ENTIRE RISK ARISING OUT OF USE OR PERFORMANCE OF THE SOFTWARE REMAINS WITH YOU.

8. LIMITATION OF LIABILITY. IN NO EVENT SHALL ACTIVE DATA SECURITY SOLUTIONS OR ITS SUPPLIERS BE LIABLE TO YOU FOR ANY CONSEQUENTIAL, SPECIAL, INCIDENTAL, OR INDIRECT DAMAGES OF ANY KIND ARISING OUT OF THE DELIVERY, PERFORMANCE, OR USE OF THE SOFTWARE, EVEN IF Active Data Security Solutions HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ANY EVENT, ACTIVE DATA SECURITY SOLUTIONS'S ENTIRE LIABILITY UNDER ANY PROVISION OF THIS EULA SHALL BE LIMITED EXCLUSIVELY TO PRODUCT REPLACEMENT.

Contents

COMMON QUESTIONS

ERASING PARAMETERS

Standards Used in This Guide

The following standards are used to provide more concise documentation:

Table 0-1 User Input

Description	Example	Action
Bold text within square brackets	Press **[Enter]**.	Press the key on the keyboard that corresponds to the message within square brackets.
Bold text and operand within square brackets	Press **[Ctrl + B]**	Together, press the combination of keys within the square brackets.
Bold text	Click **OK**.	With the mouse pointer, find the icon or button indicated and left-click that icon.
Letter "i" in the left margin	***i***	Information worthy of noting.
Exclamation mark in the left margin	***!***	Important information that may cause the utility to behave incorrectly and may damage data as a result.

1 OVERVIEW

This chapter gives an overview of **Active@ Eraser** application.

Deleting Confidential Data

Modern methods of data encryption are deterring unwanted network attackers from extracting sensitive data from stored database files. Unfortunately, attackers wishing to retrieve confidential data are becoming more resourceful by looking into places where data might be stored temporarily. A hard drive on a local network node, for example, can be a prime target for such a search. One avenue of attack is the recovery of supposedly-erased data from a discarded hard disk drive. When deleting confidential data from hard drives or removable floppies, it is important to extract all traces of the data so that recovery is not possible.

Most official guidelines around disposing of confidential magnetic data do not take into account the depth of today's recording densities. The Windows DELETE command merely changes the file name so that the operating system will not look for the file. The situation with NTFS is similar.

Removal of confidential personal information or company trade secrets in the past might have used the FORMAT command or the DOS FDISK command. Ordinarily, using these procedures gives users a sense of confidence that the data has been completely removed.

When using the FORMAT command, Windows displays a message like this:

```
Important: Formatting a disk removes all information from the
disk.
```

The FORMAT utility actually creates new **FAT** and **ROOT** tables, leaving all previous data on the disk untouched. Moreover, an image of the replaced **FAT** and **ROOT** tables are stored, so that the UNFORMAT command can be used to restore them.

FDISK merely cleans the **Partition Table** (located in the drive's first sector) and does not touch anything else.

When you use Active@ Eraser, you can scan drives and view all files on them - including files that have been deleted using the Microsoft Windows **Delete** command.

Advanced Data Recovery Systems

Advances in data recovery have been made such that data can be reclaimed in many cases from hard drives that have been wiped and disassembled. Security agencies use advanced applications to find cybercrime-related evidence. Also there are established industrial spy agencies adopting sophisticated channel coding techniques such as **Partial Response Maximum Likelihood** (PRML), a technique used to reconstruct the data on magnetic disks. Other methods include the use of magnetic force microscopy and recovery of data based on patterns in erase bands.

Although there are very sophisticated data recovery systems available at a high price, data can easily be restored with the help of an off-the-shelf data recovery utility like **Active@ File Recovery** (www.file-recovery.net) or **Active@ UNERASER** (www.uneraser.com), making your erased confidential data quite accessible.

Using **Active@ Eraser**, our powerful and compact utility, all data on your hard drive or removable floppy drive can be destroyed without the possibility of future recovery. After using **Active@ Eraser**, disposal, recycling, selling or donating your storage device can be done with peace of mind.

International Standards in Data Removal

Active@ Eraser conforms to four international standards for clearing and sanitizing data. You can be sure that once you wipe a disk with **Active@ Eraser**, sensitive information is destroyed forever.

Active@ Eraser is a quality security application that destroys data permanently from any computer that can be started using a DOS floppy disk. Access to the drive's data is made on the physical level via the Basic Input-Output Subsystem (BIOS), bypassing the operating system's logical drive structure organization. Regardless of the operating system, file systems or type of machine, this utility can destroy all data on all storage devices. It does not matter which operating systems or file systems are located on the machine, it can be DOS, Windows 95/98/ME, Windows NT/2000/XP, Linux or Unix for PC.

Cookies, History and Internet Privacy

When you are surfing the web you may think you are anonymous, but there are various ways that information about you or your activities can be collected without your knowledge or consent. Active@ Eraser can protect you against this invasion of your privacy.

There are aspects of HTTP which may allow your surfing activities to be tracked. Whenever you request a web page, information about you may be sent out including your e-mail address and the last web page you looked at.

Most commonly-used browsers support the use of cookies. A cookie is a piece of information that an Internet Web site sends to your browser when you access information at that site. If your browser supports this process, it saves information on your hard-disk as a unique permanent identifier.

While cookies in themselves may not identify you, in the way a name or address does, a cookie could potentially be linked with other identifying information. For example, if you provide extra information about yourself to the Web site by buying something on-line or subscribing to a free service, then the cookies can be used to build up a profile of your buying habits and what you are interested in.

Disreputable Internet hackers can harvest personal information unlawfully from the computers of users and can sell it to people who may use it to get credit in your name, steal your assets, or to investigate or sue you. The US Federal Trade Commission (FTC) keeps records of Internet, telemarketing, and other fraud-related complaints in a secure, online database available to hundreds of civil and criminal law enforcement agencies worldwide.

2 SYSTEM REQUIREMENTS

This chapter outlines the minimum requirements for PCs using **Active@ Eraser**.

Personal Computer Minimum Requirements for DOS

- IBM PC/AT compatible CPU
  - Operates with processors as old as Intel 486
- 4 Mb of RAM
- Video must be EGA or better resolution

Drive Storage System

- 1.44 Mb floppy diskette drive
- Hard Disk Drive type IDE, ATA or SCSI with controllers

Other

- One blank 3.5-inch or 5.25-inch floppy disk suitable for formatting
- Alternately use a Windows 95/98/ME Startup Disk

Personal Computer Minimum Requirements for Windows

All that is required to run Active@ Eraser for Windows is a PC with Microsoft Windows installed. If the PC can run Windows, it can run Active@ Eraser for Windows.

Active@ Eraser Version

The performance of **Active@ Eraser** depends on the version of the application, as displayed in the table below:

Table 2-1 Active@ Eraser for DOS

Feature	FREE DEMO Version	Professional Version
Securely overwrites and destroys all data on physical drive or logical partition	✔	✔
Supports IDE / ATA / SCSI drives	✔	✔
Supports Fixed Disks, Floppies, Zip Drives, FlashMedia drives	✔	✔
Supports large format drives (more than 8GB)	✔	✔
Supports Command Line mode (can be run with no user interaction)	✔	✔
Operates from a floppy disk	✔	✔
Erases with one-pass zeros	✔	✔
Erases with one-pass random characters		✔
Erases with user-defined number of passes (up to 99)		✔
US Department of Defense 5220.22-M compliant		✔
German VISTR compliant		✔
Russian GOST p50739-95 compliant		✔
Gutmann method compliant		✔
Customized Security Levels	✔	✔
Supports all detected hard disk drives	✔	✔
Erasing report is created and can be saved as a file	✔	✔
Displays detected drive and partition information	✔	✔
Data verification performed after erasing is completed	✔	✔
Lightweight installation (only about 1MB)	✔	✔
Disk Viewer allows previewing of any sectors on a drive	✔	✔
Scans drives and previews files before erasing on FAT, FAT32 and NTFS file systems	✔	✔

Table 2-2 Active@ Eraser for Windows

Feature	FREE DEMO Version	Professional Version
Securely overwrites and destroys all data on physical drive or logical partition	✔	✔
Supports IDE / ATA / SCSI drives	✔	✔
Supports Fixed Disks, Floppies, Zip Drives, FlashMedia drives	✔	✔
Supports large format drives (more than 8GB)	✔	✔
Supports Command Line mode (can be run with no user interaction)	✔	✔
Operates from a floppy disk	✔	✔
Erases with one-pass zeros	✔	✔
Erases with one-pass random characters		✔
Erases with user-defined number of passes (up to 99)		✔
US Department of Defense 5220.22-M compliant		✔
German VISTR compliant		✔
Russian GOST p50739-95 compliant		✔
Gutmann method compliant		✔
Wipes a drive's free space clean of previously deleted data	✔	✔
Securely erases selected single or multiple files and folders	✔	✔
Erases Internet activities (temporary Internet files, cookies, history, etc.)	✔	✔
Erases local user activities (temporary files, recent file list, run list, etc.)	✔	✔
Supports all detected hard disk drives	✔	✔
Erasing report is created and can be saved as a file	✔	✔
Displays detected drive and partition information	✔	✔
Data verification performed after erasing is completed		✔
Installation is signed and protected with AuthentiCode signature	✔	✔
Personalized software package, including registration info can be downloaded immediately after purchase		✔
Lightweight installation (only about 1MB)	✔	✔
Integrated with Windows Explorer via context menus	✔	✔
Complete interactive help file includes "How to..." sections	✔	✔
Easy-to-use Microsoft-Explorer-style user interface	✔	✔
Create and schedule unique user profile for easy hard drive maintenance	✔	✔
Supports Internet Explorer, Netscape, Opera, AOL	✔	✔

What's New in Version 4.0

Active@ Eraser v4.0 for DOS

- When the cursor is positioned on the logical drive, pressing **[Enter]** scans the drive, allowing you to preview all files and folders. In this way, you can check one last time - to be certain you have selected the correct drive - before erasing data permanently.
- Scans and previews files in all major file systems (FAT, FAT32, NTFS, NTFS5)

Active@ Eraser v4.0 for Windows

- Runs minimized (does not appear on the Taskbar)
- System Tray icon allows easy and convenient activation
- Custom profile can be created and scheduled for periodic erasing
- Auto-launching features
- Supports different browsers such as Netscape, AOL, Opera

3 RUNNING ACTIVE@ ERASER FOR WINDOWS

This chapter describes how to use the application in the Microsoft Windows environment.

Overview

Recognizing that every user has his or her own unique preferences when using a personal computer, we have developed a number of interfaces through which you can use Active@ Eraser:

- Active@ Eraser Windows Explorer Plug-In
- Active@ Eraser Windows Desktop
- Active@ Eraser DOS Interactive
- Active@ Eraser DOS Command Line

This chapter covers the first two interfaces. DOS interfaces are covered in the following chapter.

In the Microsoft Windows environment, all procedures have a common, intuitive process, as listed below:

1. Click on the item or items to be erased.

   You may choose to erase:

   - Single files or folders or groups of files or folders
   - Internet and Local Activities data
   - An entire physical drive device
   - An entire logical drive device
   - All unoccupied space on an existing physical or logical drive

2. Confirm that the selection is correct.
3. Choose the erase method.
4. Start the erase process.

The remainder of this chapter describes distinct aspects of each choice in step number one, above.

Starting Active@ Eraser

In Windows, Active@ Eraser can be started a number of ways:

- From Windows Explorer, right-click a file, folder or drive. Click **Eraser...** in the context menu. See **Active@ Eraser Windows Explorer Plug-In** for more details (below).
- From the Windows **SystemTray**, right-click the Active@ Eraser icon. Click **Activate** in the context menu.
- From the Windows **Start** button, click **Programs**. Click **Active@ Eraser** from the programs menu.

Active@ Eraser Windows Explorer Plug-In

A “Plug-In” utility is one that is not included in the basic software, yet it can be used to provide extra features. For example, once Active@ Eraser is installed, different commands appear in the Windows Explorer context menu.

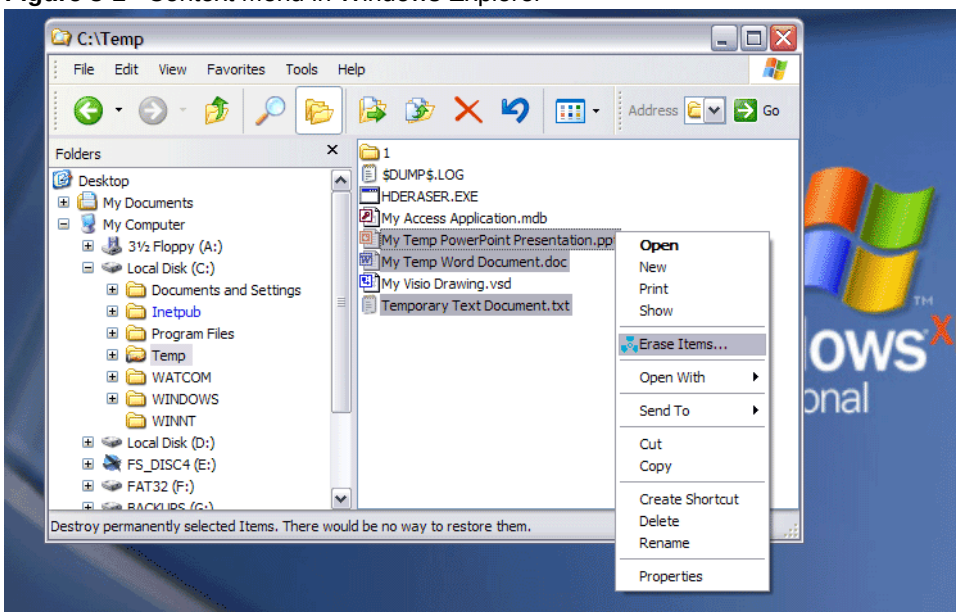
Follow the steps below to use Active@ Eraser as a Plug-In.

Erasing a File, a Folder or a Group of Items

To erase file, folder or a group of items using the Windows Explorer interface, follow these steps:

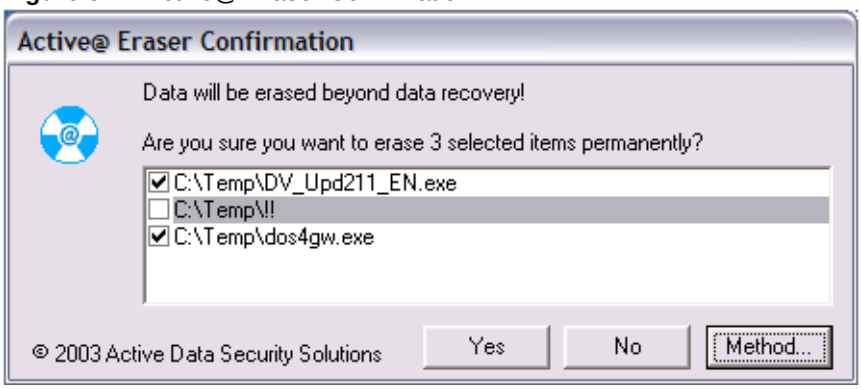
1. Select item(s) in Windows Explorer.
2. Right-click to display the context menu. The **Erase Items** command appears, as shown below:

Figure 3-1 Context Menu in Windows Explorer



3 Click **Erase Items**. The **Active@ Eraser Confirmation** screen pops up:

Figure 3-2 Active@ Eraser Confirmation



4 If you are sure that you want to erase the selected items, you may continue.

The erase operation is permanent and no data recovery is possible after the operation is engaged.

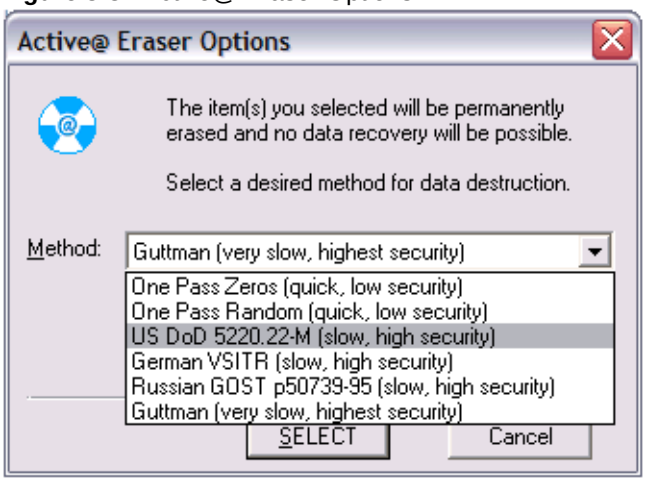
Checked boxes indicate those items selected for erasing. You can clear checkboxes for the items you do not want to erase.

The default method of data destruction is **One Pass Zeros**. For a detailed description of the data destruction methods, please see Chapter 5 in this guide.

Click **No** to cancel the erase procedure.

Click **Method** to change from the default data destruction method. The **Active@ Eraser Options** dialog appears:

Figure 3-3 Active@ Eraser Options



a Choose a method from the dropdown list.

b Click Cancel to discard changes and return to the Confirmation screen.

c Click SELECT to return to the Confirmation screen and change the data destruction method to the one you selected.

In the Confirmation screen, click **Yes** to confirm all choices and start erasing.

5 A progress dialog appears while the process is underway. You can cancel the process of data erasing by clicking the **Cancel** button on the progress dialog.

! *Important: Verify drives you want to wipe before engaging the process. Data recovery is not possible after erasing operation starts.*

Wiping Unoccupied Space

Your programs and data take up space on a hard drive. While your PC is operating, temporary files are written and erased many times in order to improve the performance of the system.

Unoccupied space on your hard drive may or may not contain residual data from files that have been deleted using the Windows delete command. Files are deleted deliberately when you highlight them and send them to the Recycling Bin. After files have been deleted from the Recycling Bin, the operating system no longer sees them.

Previously deleted files can be restored using a data recovery utility such as Active@ Uneraser, File Recovery, and others. Active@ Eraser locates all unoccupied areas and wipes them clean so that previously deleted files may not be reconstructed.

Follow these steps to wipe a drive:

1 In Windows Explorer, select the drive or drives to be wiped.

2 Right-click the selection to display the context menu. The Active@ Eraser **Wipe** command appears.

3 Click **Wipe** in the context menu. A confirmation screen appears.

4 Click **Yes** to confirm the wiping operation for the selected drive or drives. A progress window appears.

5 Watch the progress of the wiping procedure. You can cancel the process of drive wiping by clicking **Cancel** at any time.

Active@ Eraser Desktop

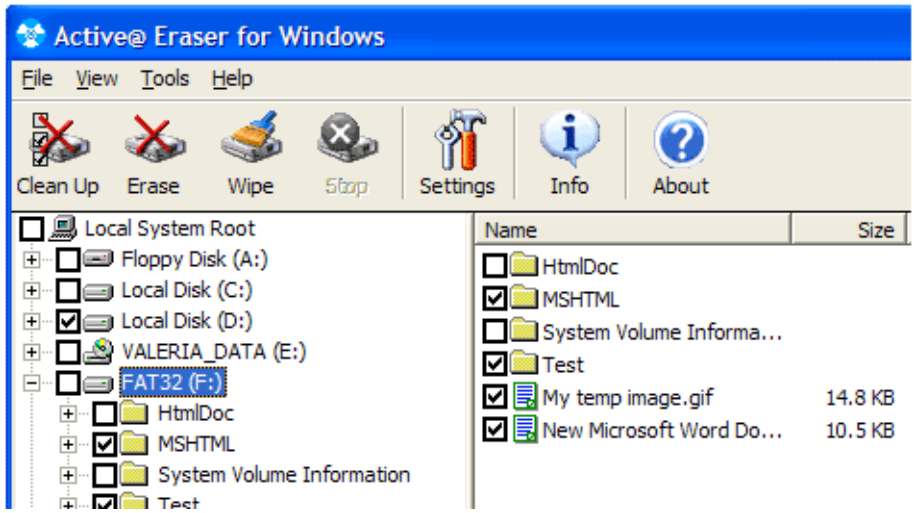
The Active@ Eraser Desktop window appears when your start the utility. Functions are intuitive and simple to perform. Descriptions of some of the erase features can be found below.

Configuring Active@ Eraser General Settings

After the Active@ Erase main screen appears, configure the utility default settings for automatic start, default erase method, confirm settings and hot keys. The steps below help with configuration settings:

1 Start Active@ Eraser. The main screen appears, similar to the screen in the figure below:

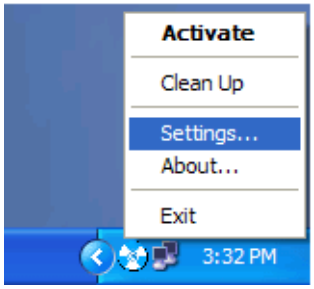
Figure 3-4 Active@ Eraser Desktop



2 Open the Active@ Eraser Settings dialog one four ways:

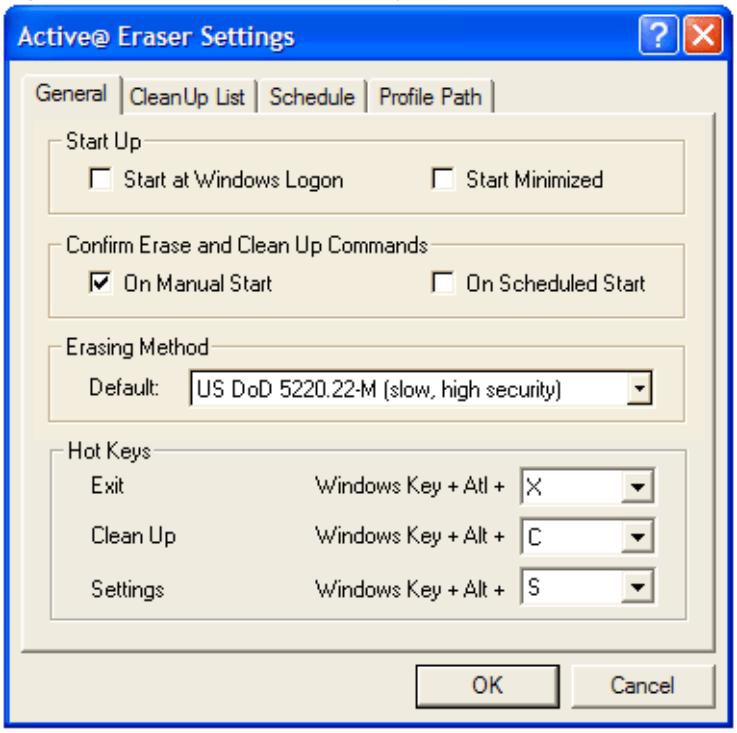
- Click **Settings** on the icon toolbar.
- Click **View** > **Settings** on the command toolbar.
- Press **[Windows Key + Alt + S]** key combination.
- Click the Active@ Eraser icon in the SysTray. Click **Settings** from the context menu.

Figure 3-5 Active@ Eraser SysTray Icon



The **Active@ Eraser Settings** dialog appears:

Figure 3-6 Active@ Eraser Settings



3 Adjust settings according to information in the table below:

Table 3-1 Active@ Eraser General Settings

Item	Description
Start at Windows Logon	When checked, Active@ Eraser starts automatically every time you log onto Windows. Check this option if you have scheduled start enabled.
Start Minimized	After Active@ Eraser starts, it appears only in the Windows Taskbar.
Confirm Erase and Clean Up Commands	Erasing data with Active@ Eraser is a permanent operation. We recommend that you confirm selected files and folders before engaging the process. **On Manual Start** - A confirmation dialog is displayed by default before any manual Erase, Wipe or Clean Up command is executed. **On Scheduled Start** - A confirmation dialog is displayed before a scheduled Clean Up command is executed.
Erasing Method	Select a default method for data destruction from the dropdown list: One pass zeros: 1 pass, quick, low security One pass random: 1 pass, quick, low security US DoD 5220.22-M: 3 passes, slow, high security German VSITR: 7 passes, slow, high security Russian GOST p50739-95: 5 passes, slow, high security Gutmann: 35 passes, very slow, highest security
Hot Keys	Assign hot keys for standard operations. Combination consists of **[Windows Key + Alt Key + User Defined Key]**. These hot keys are assigned when Active@ Eraser is running (tray icon is displayed).

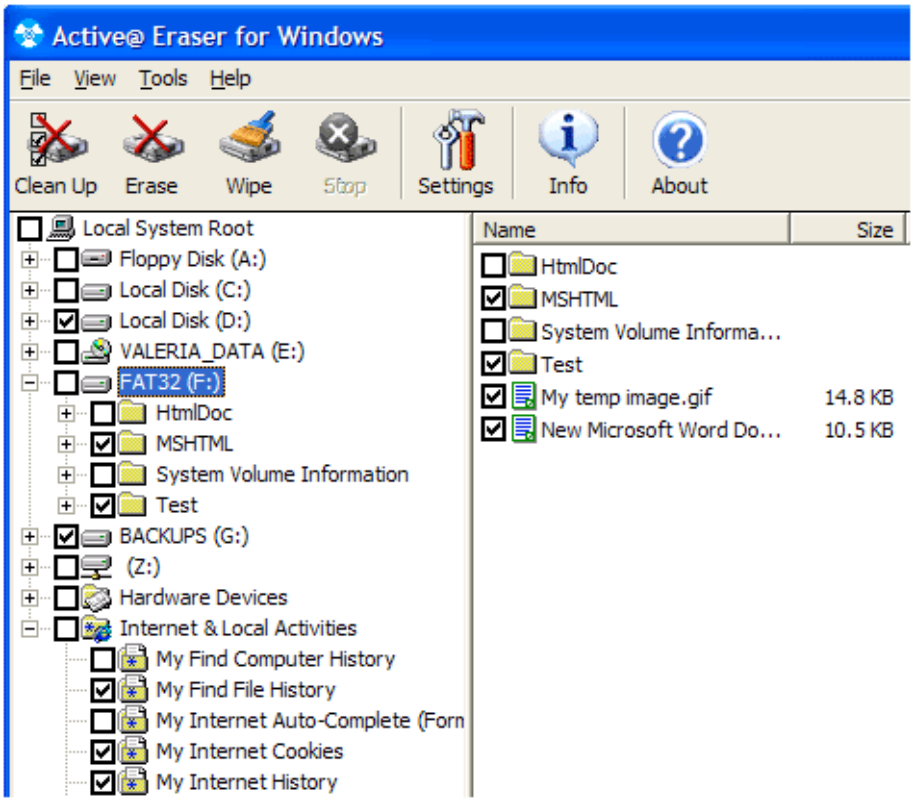
4 After settings are complete, click **OK** to apply the settings.

Creating a Clean Up Profile

The Clean Up feature was created to simplify hard drive file maintenance. With this feature, you can configure Active@ Eraser to perform a number of file deletion activities all at the same time.

You can create a profile for Clean Up from the Active@ Eraser desktop screen. Check empty boxes on the screen lists to indicate the items to be erased, wiped or cleaned up, similar to the figure below:

Figure 3-7 Check Items to be Cleaned Up



The example above shows a number of procedures for this profile. Consult the table below for further explanations:

Table 3-2 Clean Up Profile Options

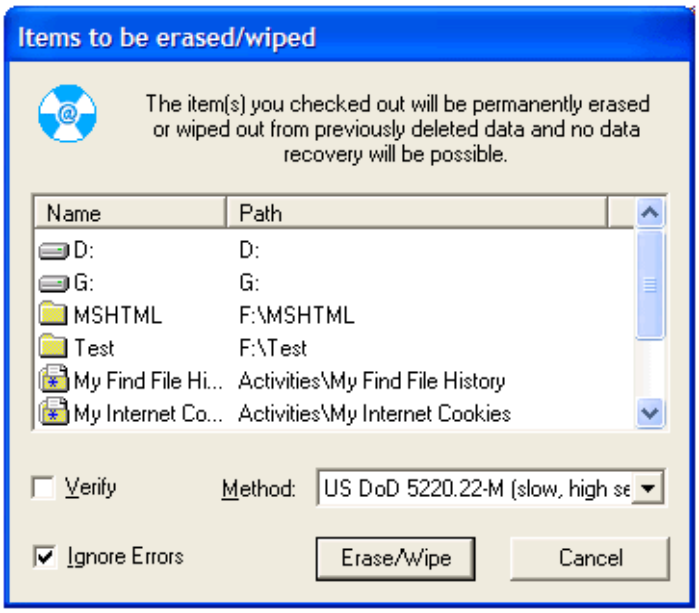
Checked Folder or File	Active@ Eraser Operation	Description
F:\MSHTML	Erase permanently	Folder and all files contained in it are erased
F:\Test	Erase permanently	Folder and all files contained in it are erased
F:\My temp image.gif	Erase permanently	File is erased
F:\New Microsoft Word Document.doc	Erase permanently	File is erased
Logical Drive D:	Wipe	Blank areas containing previously deleted files are wiped clean of residual data
Logical Drive G:	Wipe	Blank areas containing previously deleted files are wiped clean of residual data
Find File History	Clean Up	File cache data is removed, leaving the folder intact
Internet Cookies	Clean Up	File cache data is removed, leaving the folder intact
Internet History	Clean Up	File cache data is removed, leaving the folder intact

After a profile has been created, you can execute it right away by running the Clean Up command. Use one of the following methods:

- Click **Clean Up** on the icon toolbar
- Click **Tools** > **Clean Up** on the command toolbar
- Right-click the Active@ Eraser icon in the SystemTray. Click **Clean Up** from the context menu
- Press **[Windows Key+Alt+C]** combination (by default)

Depending on the utility default settings, a confirmation dialog may appear. Verify items to be erased and change erasing options, if needed:

Figure 3-8 Items to be Erased or Wiped



Click Erase/Wipe to execute the processes.

Close Active@ Eraser to save this profile. The profile is loaded each time you start the utility.

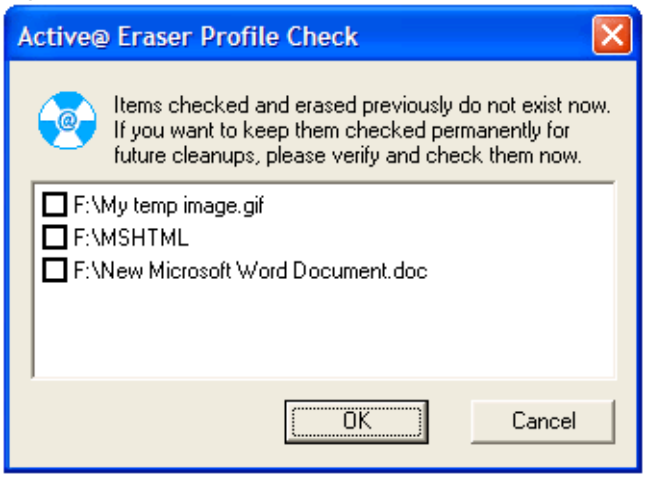
This Clean Up profile can be scheduled to run automatically. See How to Schedule Clean Ups, later in this chapter.

! *Important: Please verify files and folders you want to erase before erasing starts. Data recovery is not possible after erasing operation starts!*

Once a profile has been cleaned, selected files and folders are kept in the profile for future cleanups. The next time Active@ Eraser starts, it checks all items in the profile. If some items are missing (previously erased) the utility

suggests that you remove them from the profile. A Profile Check screen appears, similar to the one in the figure below:

Figure 3-9 Active@ Eraser Profile Check



If you want to keep these items in the profile forever, check the boxes. When boxes are checked in this screen, data is saved in a file named ERASER.INI in a section named ItemsToKeep. If these items appear on drive again, they appear on the main screen with boxes checked. They will be included in the next cleanup automatically.

Erasing Internet & Local Activities Manually

Active@ Eraser automatically scans your system and lists locations containing Internet and local activity files. Erasing these areas improves the personal security of your system.

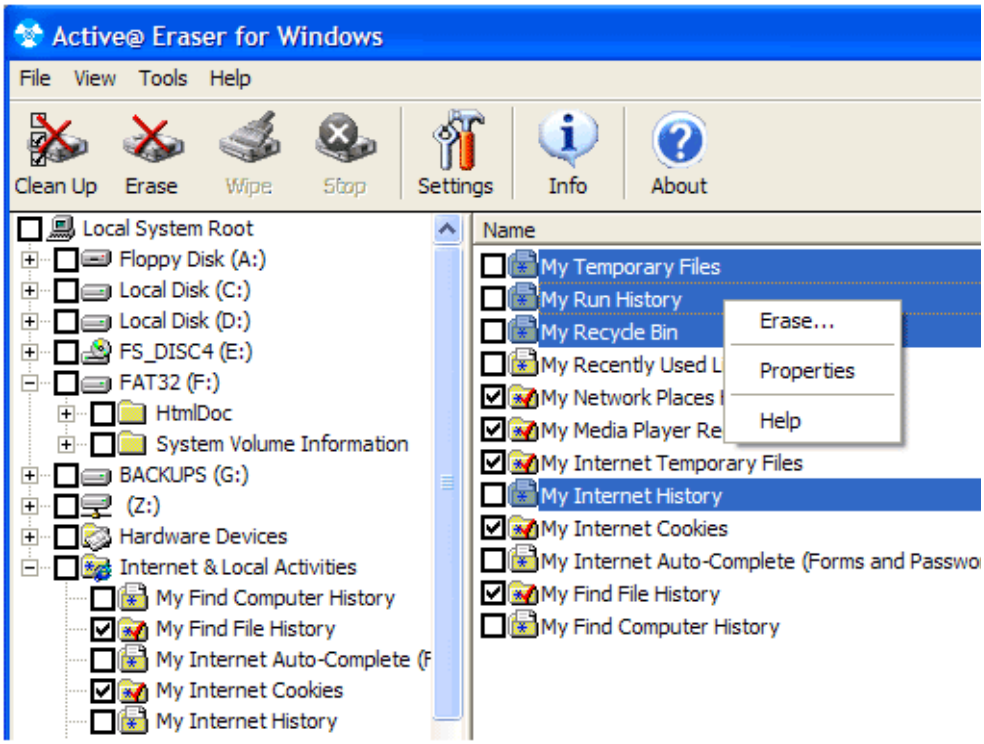
To erase data in these locations, follow these steps:

1. Start Active@ Eraser. The left pane contains a list of logical and physical locations on the system.
2. Click **Internet & Local Activities** in the left pane. Details of the selection appear in the right pane.

   With this item selected, all contents of the node are erased. To permanently erase the entire contents of this node, continue with the next step.

If you want to permanently erase only selected items from this node, click an item or multiple items in the right pane by pressing **[Shift]** or **[Ctrl]** key while clicking.

Figure 3-10 Select Items to be Permanently Erased

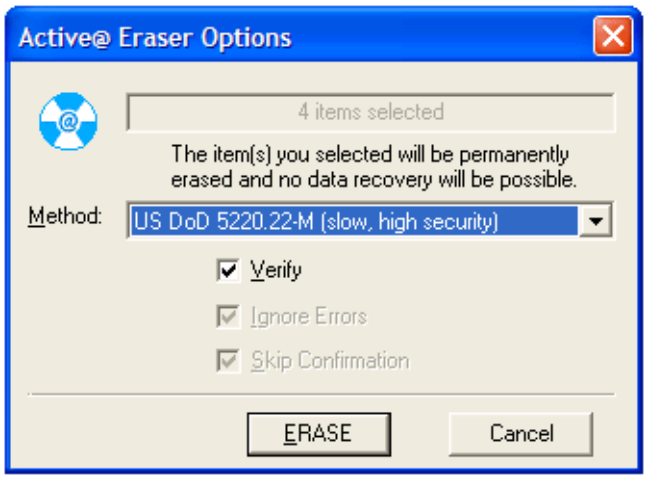


3 When all items have been selected, you are ready to perform the erasing process. Start the process by doing one of the following:

- Click **Erase** on the icon toolbar.
- Right-click selected item(s), and click **Erase** on the context menu.
- Click **Tools** in the Command toolbar. Click **Erase** from the Tools menu.

The **Active@ Eraser Options** dialog appears.

Figure 3-11 Active@ Eraser Options



4 Choose appropriate erasing options.

- **Method:** - Choose the erasing method from the drop-down list.
- **Verify** - Check data after deletion and confirm the action is complete.
- **Cancel** - Close this dialog and abandon the erasing process.
- **ERASE** - Confirm all selections and begin the erasing process.

5 A progress dialog appears during the operation. You can cancel the process of data erasing anytime by clicking the Stop button on the toolbar.

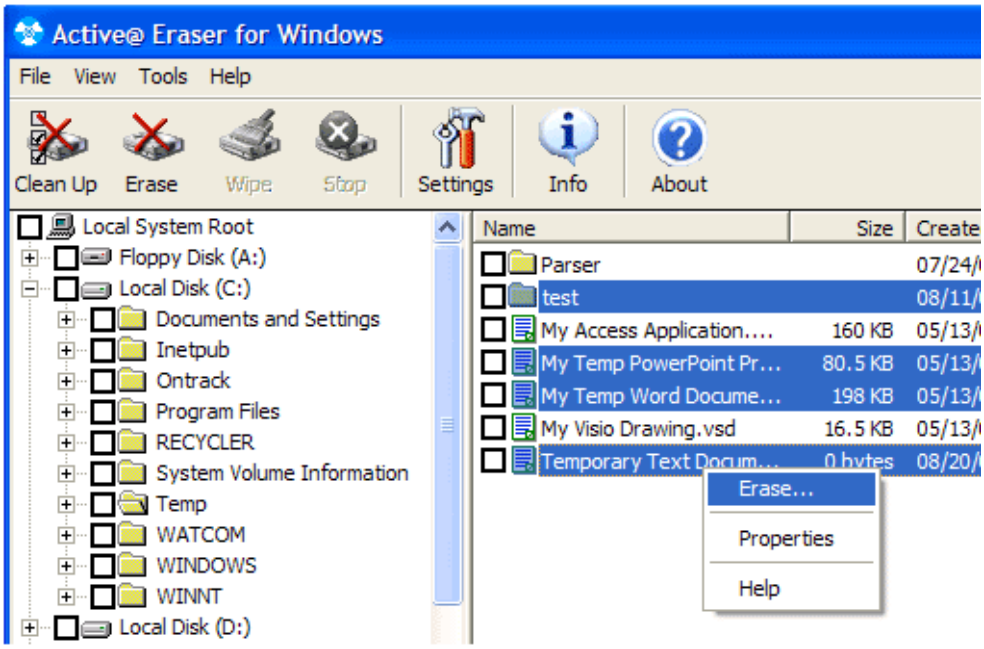
Erasing Files or Folders Manually

Active@ Eraser Desktop displays the contents of all physical and logical drives. Any selected item can be erased permanently.

Follow these steps to erase selected files or folders:

1 Start Active@ Eraser and select one file or multiple files and folders.

Figure 3-12 Select Files and Folders

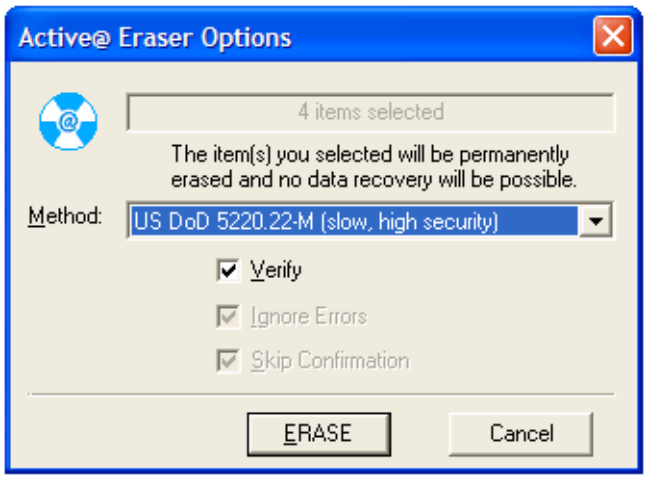


2 After all files and folders have been selected, run the Erase command by doing one of the following:

- Click **Erase** on the icon toolbar.
- Right-click selected item(s), and click **Erase** on the context menu.
- Click **Tools** in the Command toolbar. Click **Erase** from the Tools menu.

The **Active@ Eraser Options** dialog appears.

Figure 3-13 Active@ Eraser Options



3 In this dialog, choose the appropriate erasing options.

- **Method:** - Choose the erasing method from the drop-down list.
- **Verify** - Check data after deletion and confirm the action is complete.
- **Cancel** - Close this dialog and abandon the erasing process.
- **ERASE** - Confirm all selections and begin the erasing process.

4 After ERASE has been clicked, a progress dialog appears. Watch the progress and wait until erasing is complete.

You can cancel the process of data erasing anytime by clicking **Stop** on the toolbar.

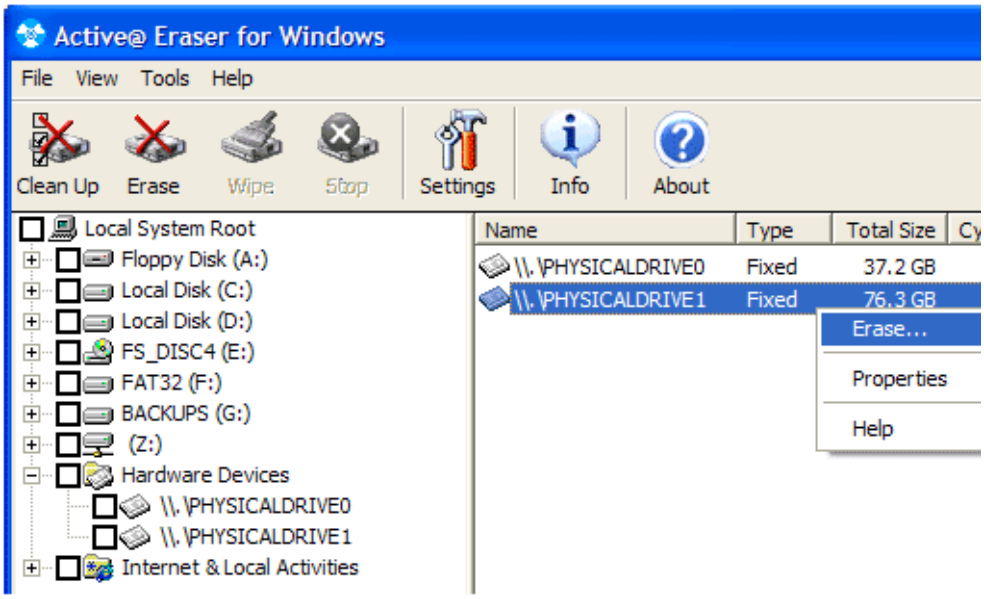
Erasing a Physical Device (HDD) Manually

Erasing the physical device removes ALL information from the hard disk drive or floppy, including files, folders, MBR, partitions and file systems. No data recovery is possible from the device after erasing operation is complete!

To erase a physical device:

1 Start Active@ Eraser and select the Hard Disk Drive to be erased beneath **Hardware Devices** node, as in the figure below:

Figure 3-14 Start Active@ Eraser

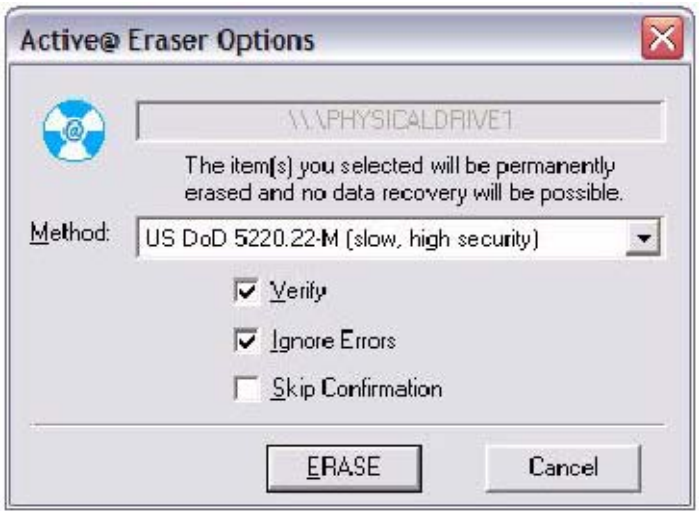


2 After all devices have been selected, run the Erase command by doing one of the following:

- Click **Erase** on the icon toolbar.
- Right-click selected item(s), and click **Erase** on the context menu.
- Click **Tools** in the Command toolbar. Click **Erase** from the Tools menu.

The Active@ Eraser Options dialog appears.

Figure 3-15 Active@ Eraser Options

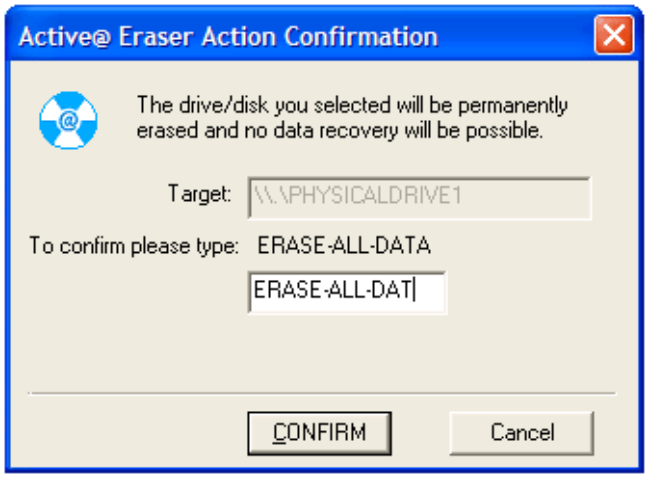


3 In this dialog, choose the appropriate erasing options.

- **Method:** - Choose the erasing method from the drop-down list.
- **Verify** - Check data after deletion and confirm the action is complete.
- **Ignore Errors** - Check this box to avoid displaying an error message every time a read/write error is encountered. Leave the box unchecked if you want to see each read/write error. Whether this box is checked or unchecked, all detected errors and warnings are logged into the Event Log file independently of this option.
- **Skip Confirmation** - Check this box to skip the next dialog where you are to confirm the erasing command. Leave the box unchecked for the best insurance against erasing a drive by mistake.
- **Cancel** - Close this dialog and abandon the erasing process.
- **ERASE** - Confirm all selections and advance the erasing process.

4 After ERASE has been clicked, the Active@ Eraser Action Confirmation dialog appears, as below:

Figure 3-16 Action Confirmation



5 This is the final step before erasing all data permanently. Verify the erasing action by typing: **ERASE-ALL-DATA** in the text field.

Click CONFIRM to engage the erase process. A progress screen appears.

Watch the erasing progress and wait while erasing is complete.

You can cancel the process of wiping deleted data anytime by clicking **Stop** on the toolbar.

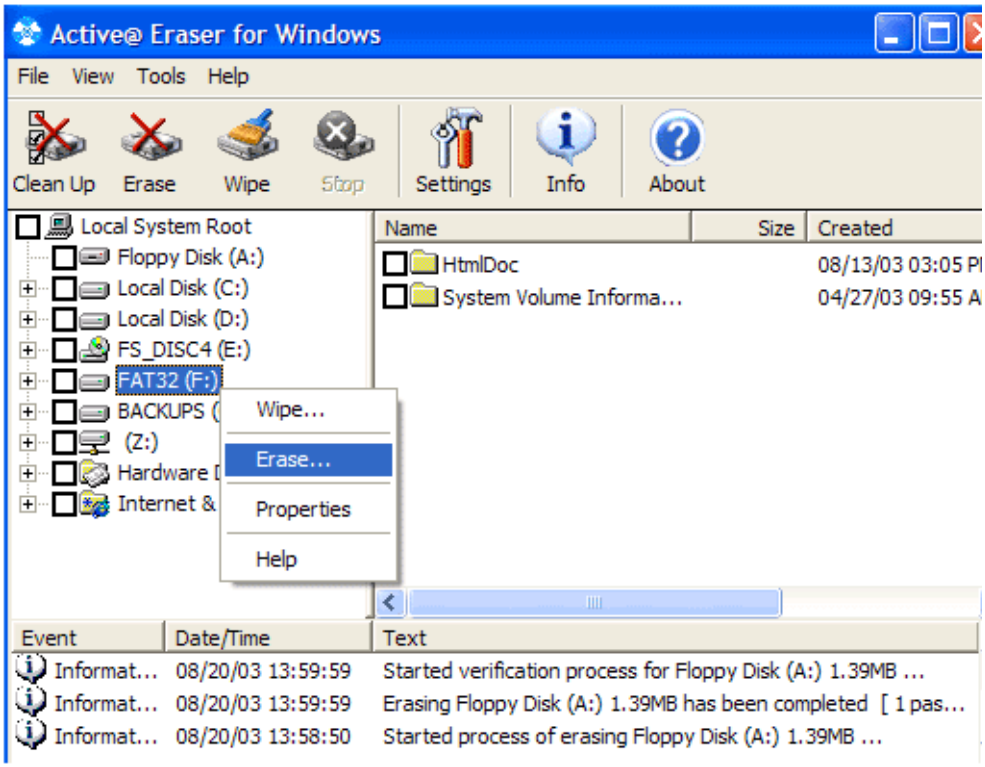
Erasing a Logical Drive Manually

Erasing a logical drive removes ALL information from the drive, including files, folders and file system itself. No data recovery is possible from the drive after the erasing operation is complete.

To erase a logical drive follow these steps:

1 Start Active@ Eraser and select the logical drive to be erased:

Figure 3-17 Select Logical Drive



2 After all drives have been selected, run the Erase command by doing one of the following:

- Click **Erase** on the icon toolbar.
- Right-click selected item(s), and click **Erase** on the context menu.
- Click **Tools** in the Command toolbar. Click **Erase** from the Tools menu.

The Active@ Eraser Options dialog appears.

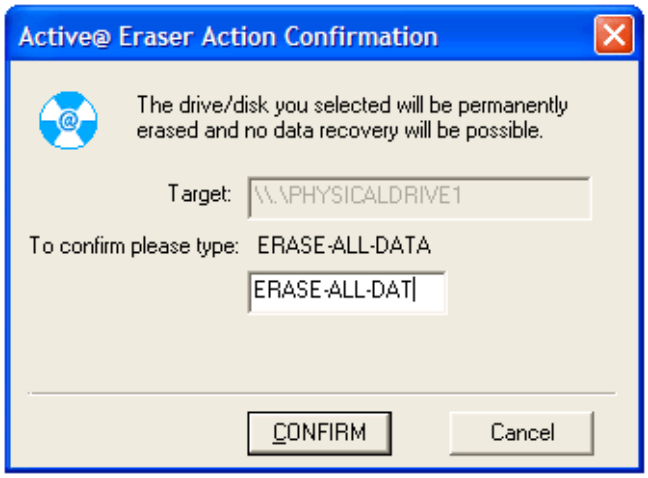
3 In this dialog, choose the appropriate erasing options.

- **Method:** - Choose the erasing method from the drop-down list.
- **Verify** - Check data after deletion and confirm the action is complete.
- **Ignore Errors** - Check this box to avoid displaying an error message every time a read/write error is encountered. Leave the box unchecked if you want to see each read/write error. Whether this box is checked or unchecked, all detected errors and warnings are logged into the Event Log file independently of this option.

- **Skip Confirmation** - Check this box to skip the next dialog where you are to confirm the erasing command. Leave the box unchecked for the best insurance against erasing a drive by mistake.
- **Cancel** - Close this dialog and abandon the erasing process.
- **ERASE** - Confirm all selections and advance the erasing process.

4 After ERASE has been clicked, the **Active@ Eraser Action Confirmation** dialog appears.

Figure 3-18 Active@ Eraser Action Confirmation



This is the final step before erasing all data permanently. Verify the erasing action by typing: ERASE-ALL-DATA in the text field.

Click **CONFIRM** to engage the erase process. A progress screen appears.

Watch the erasing progress and wait while erasing is complete.

You can cancel the process of wiping deleted data anytime by clicking **Stop** on the toolbar.

! *Important: After the Erasing process starts, it can be a long process. Be prepared to wait. If you decide to cancel the operation before it has completed, it is likely that Windows will not recognize your drive anymore. Even if some of your data still resides on the drive, it will be impossible to access files through the Windows Explorer. Specialized recovery software, like UNERASER (www.uneraser.com) might help you recover files in a case like this.*

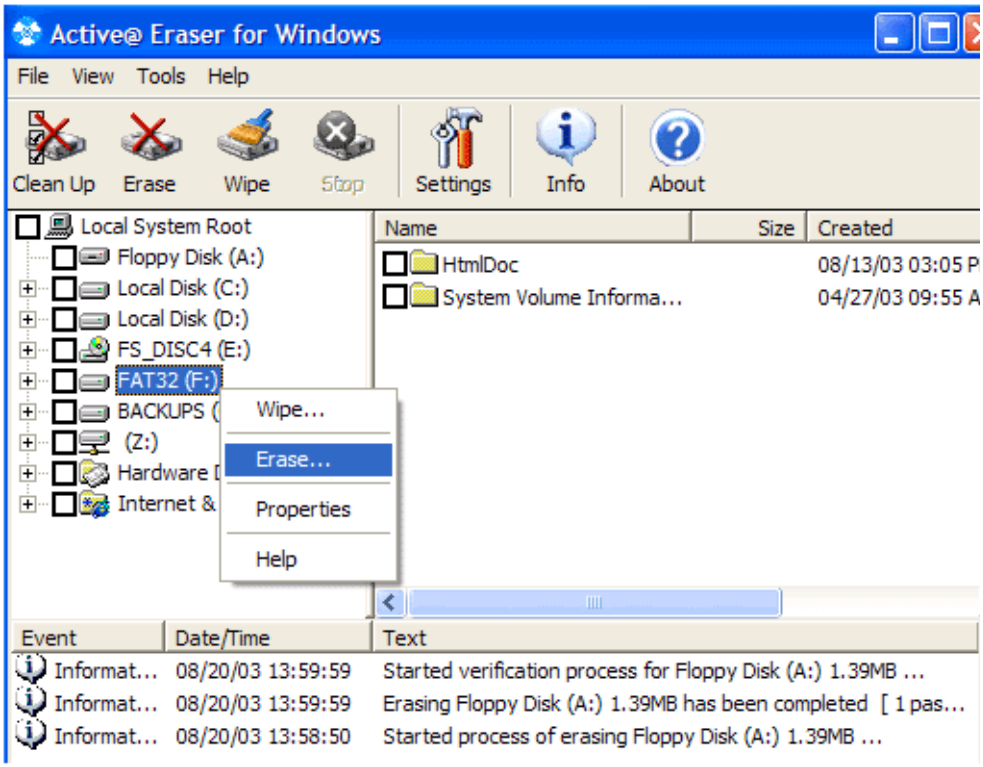
Wiping Unoccupied Space Manually

Wiping a the logical drive of deleted data does not delete existing files and folders. It processes all drive space designated as unoccupied so that future data recovery of previously deleted or temporary files becomes impossible.

To wipe a drive's unoccupied space:

1 Start Active@ Eraser and select the logical drive to be wiped.

Figure 3-19 Select Drive to be Wiped



2 Run the **Wipe** command by doing one of the following:

- Click **Wipe** on the icon toolbar.
- Right-click selected item(s), and click **Wipe** on the context menu.
- Click **Tools** in the Command toolbar. Click **Wipe** from the Tools menu.

After the wiping process has started, a progress window appears.

3 Watch the progress and wait until wiping is complete.

You can cancel the process of wiping deleted data anytime by clicking **Stop** on the toolbar.

! *Important: The wiping action can be a long process. Be prepared to wait.*

At the end of the wiping operating, the system might post a message similar to this:

```
Low disk space notification! Do you want to clean up your
drive to free more space?
```

Ignore this message. Click **No** to resolve the question.

Scheduling Automatic Clean Ups

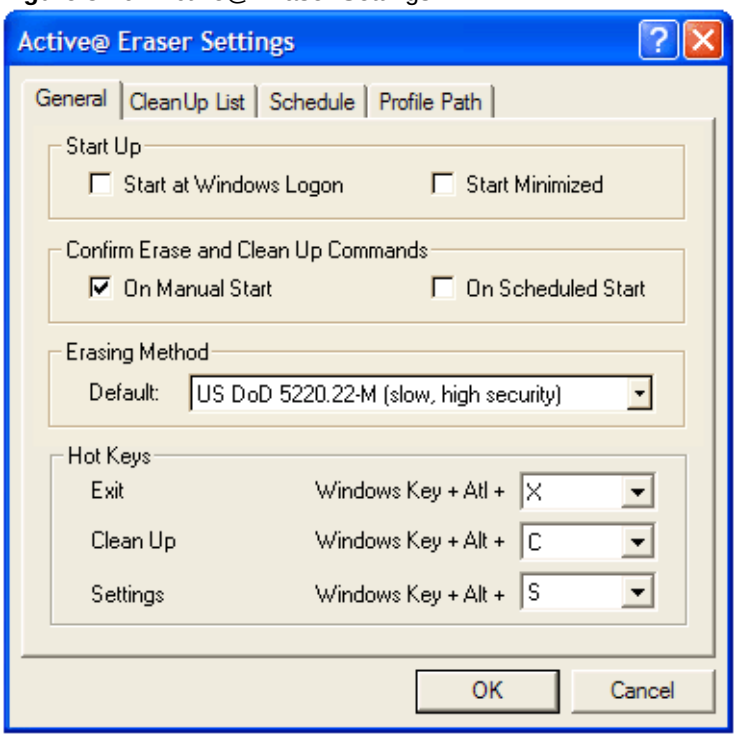
Scheduling Active@ Eraser Clean Up to run automatically reduces work on your part and effectively secures confidential data on your PC.

To run Clean Up procedures each time you logon to Windows, follow these steps:

1. Start Active@ Eraser.
2. Open the Active@ Eraser Settings dialog using one of the following:
   - Click **Settings** on the icon toolbar
   - Click **View** > **Settings** on the command toolbar
   - Press **[Windows Key + Alt + S]** key combination.
   - Click the Active@ Eraser icon in the SysTray. Click **Settings** from the context menu.

   The Active@ Eraser Settings dialog appears:

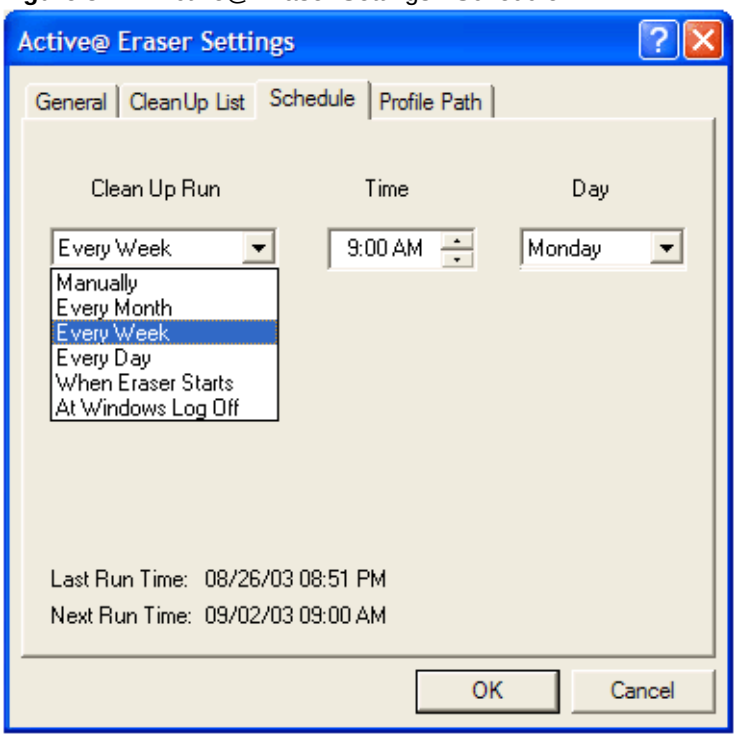
Figure 3-20 Active@ Eraser Settings



3. When **Start at Windows Logon** option is checked, Active@ Eraser is launched automatically each time you log onto Windows.
4. Click the **Clean Up List** tab and verify files, drives and folders to be processed.

5 Click the **Schedule** tab:

Figure 3-21 Active@ Eraser Settings - Schedule



6 Use descriptions in the table below to help configure an appropriate schedule:

Table 3-3 Options for Schedule Settings

Run Options	Description
Manually	Scheduling is not active.
Every Month	Set time and day of the week. For example if Monday is chosen, utility runs on the first Monday of each month.
Every Week	Set time and day of the week that the utility runs.
Every Day	Set time for daily process.
When Eraser Starts	Each time you launch Active@ Eraser, the utility runs automatically.
At Windows Log Off	Each time you shut down or log off Windows, the utility runs automatically.

7 Click **OK** to apply the scheduling options.

Security Tips

Follow the security tips below as a general precaution when dealing with sensitive or confidential data.

DO NOT DISCARD OR DONATE UNUSED HARD DISK DRIVES, REMOVABLE DRIVES OR FLOPPIES WITHOUT REMOVING CONFIDENTIAL DATA!

Data recovery software can be used to retrieve private information from recording media that has been erased using the Windows Delete command.

Destroy devices physically or use software like Active@ Eraser to clean it up before discarding or donating to anyone.

DO NOT TRUST YOUR CONFIDENTIAL OR SENSITIVE DOCUMENTS TO THE WINDOWS RECYCLE BIN OR STANDARD DELETE COMMAND!

Deleted documents can be easily restored from the Recycle Bin, even after you have emptied it. Use software like Active@ Eraser or ZDelete (www.zdelete.com) to ensure that important documents are erased permanently from the media storage.

PERFORM A REGULAR CLEAN-UP OF YOUR CONFIDENTIAL INTERNET AND LOCAL ACTIVITIES FILES!

Unwanted hackers can follow your trail through all activities on the Internet through the saved list of visited web sites. Similarly, all local activities on your hard drive are recorded in a list of recently opened files. Maintain your privacy by performing complete cleanup regularly.

Troubleshooting

The following scenarios are provided from help service offered to actual customers.

Problem 1

I have purchased your software and copied it onto a floppy. When starting Active@ Eraser, I get a message that says: “UNREGISTERED VERSION.”

Possible Cause: You forgot to copy SETTINGS.INI. This file contains your registration key.

Solution 1: Look for SETTINGS.INI in the installation folder and copy it to the same folder where you start Active@ Eraser.

Solution 2: Install the software directly to the floppy disk. All necessary files are copied there.

Problem 2

I removed your software from my PC, however I can still see the Erase... command in my Windows Explorer context menu.

Possible Cause: You removed the software bypassing the standard Uninstall procedure, i.e. by deleting the installation folder.

Solution 1: Locate and manually delete the file EraserD.dll located in WINDOWS\SYSTEM32 folder.

Solution 2: Install the software again and perform proper Uninstall procedure by executing the Uninstall Software menu command.

Frequently Asked Questions (FAQ)

Does Active@ Eraser software comply with any industry standards for data removal?

Yes, Active@ Eraser complies with the US DoD 5220.22-M, German VSITR, Russian GOST p50739-95 standards for cleaning and sanitizing. Other advanced methods, like the most secure Gutmann's method, have also been implemented.

How can I download the trial version of Active@ Eraser utility?

You can download the trial version from the www.active-eraser.com Web site. The DEMO version is a utility with full functionality of the final program. The only limitation is that only one erasing method is available.

Does Active@ Eraser for Windows work under Windows 2000 or Windows XP?

Yes, it does.

Does Active@ Eraser for Windows work under Windows 3.x?

No. Support of 16-bit operation systems like Windows 3.1 is not implemented. However you can use Active@ Eraser for DOS to remove data in DOS mode from any operating system.

I have Netscape Navigator 4.6 as my default browser. Will I be able to install and use Active@ Eraser?

Yes, to download and install software you need to have Internet Explorer or Netscape Navigator, or any other browser that supports file download. After software installation you will not use your browser to run the program.

Does Active@ Eraser support localized (e.g. French, Spanish) files names?

Yes, provided the OS and file system support localized file names.

Do I need special OS permissions to install and use the software?

To install software on Windows 95/98/ME you do not need special permission. To install software on Windows NT/2000/XP you need permission (i.e. as an Administrator or in the Power Users group). The same rules apply to erasing drives and devices. To erase files and activities you do not need any special permissions, unless the file is located on an NTFS partition. You must have permissions to “write” to the particular file in order to destroy it (you can not destroy the data if you do not have access to it).

I want to clear the search history that pops up when I try to search the internet using Google or any other internet search engine. How can I do it?

It is a standard Auto-Complete feature in Internet Explorer, which tries to fill html forms on a web page automatically (if turned on). To clear Auto-Complete history in the Active@ Eraser Desktop, go to the Internet & Local Activities and erase My Internet Auto-Complete (Forms and Passwords) node.

Can Active@ Eraser software be installed and run from floppy?

Yes. Active@ Eraser is relatively compact utility, it can be installed and run from a floppy if you indicate the floppy as the destination path while installing.

4 Running Active@ Eraser for DOS

This chapter describes how to use the application. The chapter's sections are:

- Preparing a DOS-bootable Floppy Disk
- Modes of Operation:
  - DOS Interactive Mode
  - DOS Command Line Mode
  - DOS Autoexecute Mode

Preparing a DOS-Bootable Floppy Disk

Active@ Eraser is a powerful utility with a small footprint. It is small enough to operate from a single floppy drive in a Microsoft DOS environment. This can be useful in a number of situations. For example, a computer technician who is assigned to erase the data on PCs with hard drives containing Windows operating systems or operating systems other than DOS or Windows, can use a single DOS-bootable floppy to erase all data.

This chapter describes the steps to create a DOS-bootable floppy (a startup disk) and run the utility. If you have a bootable floppy, skip to the **Copying Active@ Eraser to a Floppy** section, below.

System Formatting

To prepare a bootable floppy from MS-DOS, Windows 95/98/ME/XP, put a blank 3.5-inch floppy in the floppy drive (drive a:) and follow the appropriate instructions below:

Windows 95/98 MS-DOS or Command Prompt Mode

1. On the screen, type the format command as follows:

   ```
   FORMAT A: /S
   ```

2. Follow on-screen messages until process is complete.

Windows 95/98/ME Operating System

1. Click the **Start** button and click **Settings > Control Panel**.
2. From the **Control Panel** screen, click **Add/Remove Programs**.
3. In the **Add/Remove Programs** screen, click the **Startup Disk** tab.
4. Click **Startup Disk...** and follow the screen instructions until the process is complete.

Windows XP Operating System

1. Click **Start**. Click **My Computer**.
2. Right-click **A:** drive.
3. From the drop-down menu, click **Format...**
4. Enable the checkbox beside **Create an MS-DOS startup disk**.
5. Click the **Start** button and follow the screen instructions until the process is complete.

Copying Active@ Eraser to a Floppy

Copy the **Active@ Eraser** file (HDERASER.EXE) to the bootable floppy disk or startup disk in drive a:.

If you don't have the **Active@ Eraser** file, download it from **http://www.active-eraser.com**.

After copying the file onto the floppy disk, remove it from the floppy drive.

Labeling the Disk

If you plan to use **Active@ Eraser** in Command Line mode, please skip the next section and read **Boot to DOS (Command Line Mode**).

Once preparation of the bootable 3.5-inch floppy disk is complete, you are ready to begin removing data.

One-Step Method

Combine all the above steps into one by navigating to our Web site.

Download and run **Bootable Floppy Disk Creator for Active@ Eraser**.

Once you have installed Active@ Eraser on the floppy, you are ready to boot from the floppy and use the software for disk erasing.

Modes of Operation

Active@ Eraser can be used three ways:

- DOS Interactive Mode
- Command Line Mode
- Autoexecute Mode

It is wise to label the floppy disk to identify the way you plan to use **Active@ Eraser**.

DOS Interactive Mode and Command Line Mode are similar in that you can control what happens after the utility has started. In Autoexecute Mode, however, **Active@ Eraser** starts immediately upon completion of the bootstrap startup (depending on the automatic settings).

DOS Interactive Mode

This section describes using the DOS Interactive screens. For “hands-off” operation, please see the next section, below.

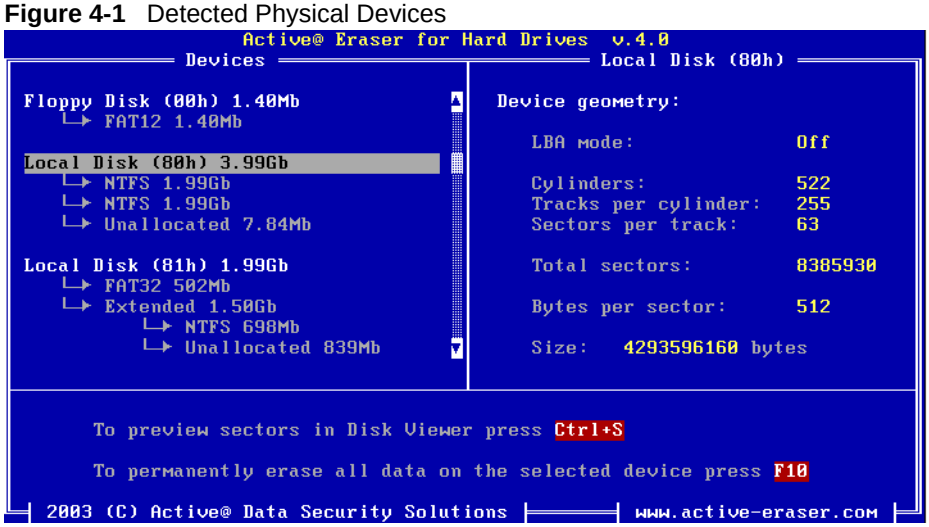
Here are the steps for interactive operation:

1. With the PC power off, insert the **Active@ Eraser** floppy disk into drive A:.
2. Start the PC by turning on the power. The screen displays the Microsoft DOS prompt.
3. At the DOS prompt, run **Active@ Eraser** by typing:

```
HDERASER.EXE
```

The **Detected Physical Devices** screen appears as below:

Figure 4-1 Detected Physical Devices



All system hard drives and floppy drives are displayed in the left pane along with their system information in the right pane.

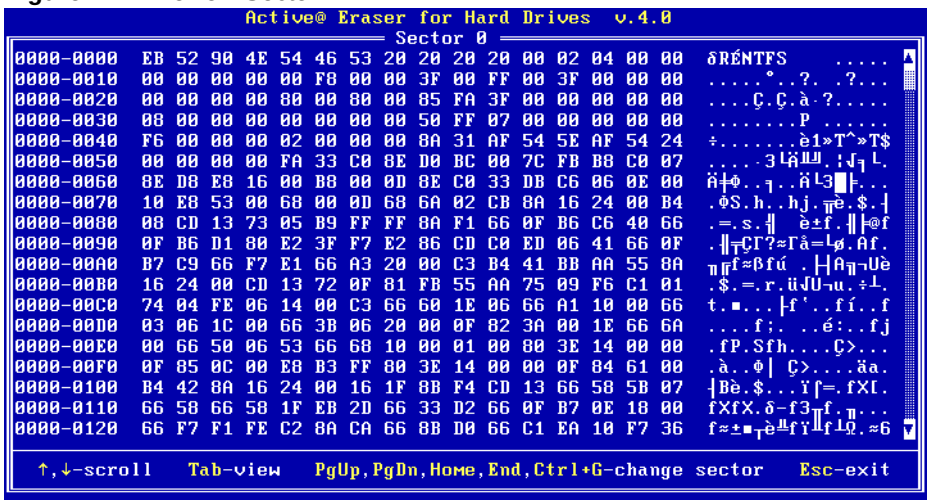
4. Change the position cursor using the keyboard **[Down]** and **[Up]** arrow keys. Information in the right pane changes according to the structure of the detected devices.

   Hard drive devices are numbered by the system BIOS. A system with a single hard drive displays it as number 80h. Subsequent hard drive devices are numbered consecutively. For example the second device is shown as 81h.

5. Be certain that the drive you are pointing to is the one that you want to erase. All data is permanently erased with no chance for recovery.

If there is any doubt about which drive to select, preview the sectors in the device by pressing **[Ctrl + s]**. The screen appears, as below:

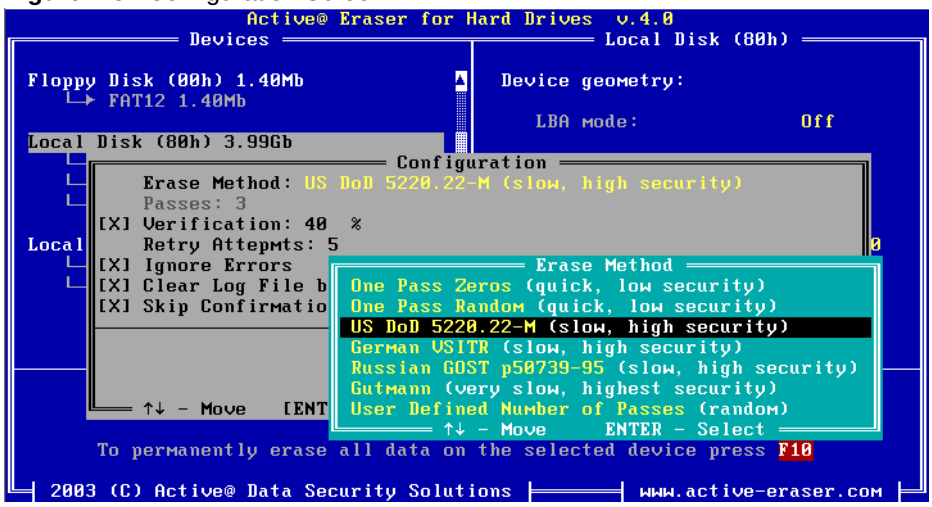
Figure 4-2 Preview Sector



Scroll up and down using the keyboard arrow keys, **[Page Up]**, **[Page Down]**, **[Home]** and **[End]** navigation keys. Jump to a specific sector using **[Ctrl + g]**. When you are satisfied with the identification of the device, press **[Esc]** to exit this screen.

6 When you have selected the device to erase, move the cursor to that device and press **[F10]** on the keyboard. The **Configuration** screen appears.

Figure 4-3 Configuration Screen



Using the keyboard arrow keys, select the feature that you want to configure. Press **[Enter]** to make a change.

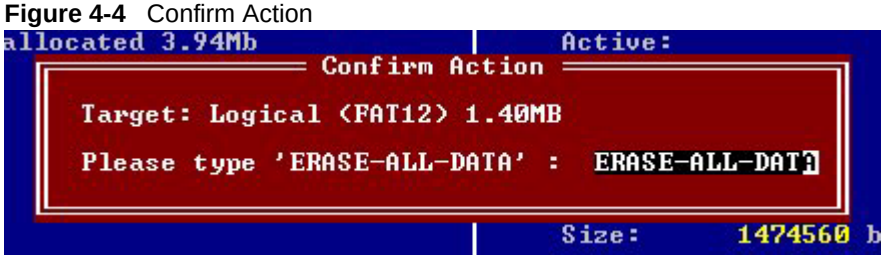
To assist with options presented in this screen, please refer to the table on the following page.

Table 4-1 Erase Parameters Configuration

Feature	Default	Options
Erase Method	US DoD 5220.22M	One pass zeros One pass random US DoD 5220.22M German VSITR Russian GOST p-50739-95 Gutmann User Defined Number of Passes (For descriptions of these options see ANOTHER PLACE, below.)
Passes	3	If **User Defined Number of Passes** is selected in the line above, this number may be changed. Otherwise this line displays the standard number of passes for the selected erase method.
Verification	Enabled / 40%	Enabled: Utility inspects the work done by HDERASER to verify that the attempt was successful. The percentage shown indicates how much of the drive is verified. Disabled: Verification is not performed
Retry Attempts	5	If the process encounters an IO error, the number of times the operation repeats before displaying an error message. Repeating the operation sometimes helps to overcome IO problems.
Ignore Errors	Disabled	Enabled: Each time the read heads encounter a read-write error, a message appears that requires confirmation by the user. Disabled: Error messages are not displayed.
Clear Log File before Start	Enabled	
Skip Confirmation	Disabled	Next step confirmation screen does not appear.

The **Confirm Action** screen appears.

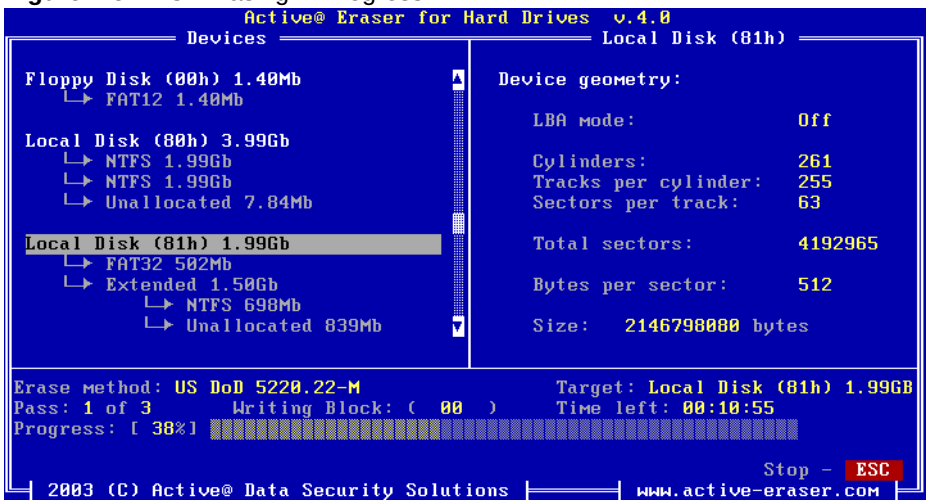
Figure 4-4 Confirm Action



7 This is the final step before removing data from the selected drive for ever. Once the process has started, you may stop it by pressing the **[Esc]** key.

Type **ERASE-ALL-DATA** and press **[F10]**. Progress of the erasing procedure is monitored in the **Disk Erasing** screen, similar to the one below:

Figure 4-5 Disk Erasing in Progress



8 If you wish to stop the process for any reason after it has begun, press the **[Esc]** key. Please note, however that erased data is not recoverable.

There is nothing more to do until the end of the disk erasing process. The application operates on its own without user intervention.

If there are any errors, for example due to bad clusters, they are reported on the Interactive screen. If such a message appears, it is possible to cancel the operation (by pressing **[Esc]**), or continue erasing data.

DOS Command Line Mode

This section describes running **Active@ Eraser** in Command Line mode.

Follow these steps:

1. With the PC power off, insert the **Active@ Eraser** floppy disk into drive A:
2. Start the PC by turning on the power. The screen displays the Microsoft DOS prompt.
3. At the DOS prompt, display **Active@ Eraser** parameters by typing:

   ```
   A:\>hderaser -?
   ```

   A list of parameters is displayed. Explanations of the parameters can be found in the table on the following page.
4. Key the command and parameters into the DOS screen at the prompt. Here is an example:

   ```
   A:\hderaser -eraseallhdds -erasemethod=6 -passes=7
   -noconfirmation
   ```

   In the example above, data on all hard drives is erased in seven passes without user confirmation.
5. Press **[Enter]** to complete the command and start the process.

   After operation has completed successfully information on how drives have been erased is displayed on the screen.

Table 4-2 Command Line Parameters

Parameter	Default	Options
no parameter		With no parameter, the DOS Interactive screens appear.
-erasemethod=[0-6]	0	0 - One pass zeros (quick, low security) 1 - One pass random (quick, low security) 2 - US DoD 5220.22-M (slow, high security) 3 - German VSITR (slow, high security) 4 - Russian GOST p50739-95 (slow, high security) 5 - Gutmann (very slow, highest security) 6 - User Defined Number of Passes (random)
-passes=[1 - 99]	1	Number of times the write heads pass over a disk area to overwrite data. Valid only if erasemethod = 6.
-verification=[1 - 100]	40	After the data erasing process is complete, the utility reads the disk space to verify that the actions performed by the write head comply with the chosen erasemethod (reading 40% of the area by default). It is a long process. Set the verification to the level that works for you.
-retryattempts=[1 - 99]	5	When the drive write head encounters an error in the sector, the utility tries to write in the sector 5 times by default.
-erasehdd=[80h - 83h]		By default, the utility erases the first logical drive encountered. Use this parameter to direct the erasing procedure to the correct target.
-ignoreerrors	ON	By default, the erasing process stops each time a disk error is encountered. You have the option to continue erasing or to stop the process and deal with the error. When this parameter is used, all errors are ignored.
-clearlog	ON	When a drive is erased, a log file is kept. By default, this log is cleared at the start of the erasing process. The log file is stored in the same folder where the software is located.
-noconfirmation	ON	Skip confirmation steps before erasing starts. By default, confirmation steps appear in command line mode for each hard drive or floppy as follows: Are you sure?
-test		If you are having difficulty with Active@ Eraser, use this parameter to create a hardware info file to be sent to our technical support specialists.
-eraseallhdds		Erase all detected hard disk drives
-help or -?		Display this list of parameters.

Autoexecute Mode

You can start **Active@ Eraser** with a DOS auto-executable batch file. Include the command line containing call of the program and parameters.

Follow these steps:

1. In the Microsoft DOS screen, open a new autoexec.bat file or edit an existing one with the following command:

   ```
   A:\>edit autoexec.bat
   ```

   The Microsoft DOS file edit screen appears.
2. Enter the command line and parameters as needed. Here is an example:

   ```
   hderaser -erasehdd=80h -erasemethod=6 -passes=1 -ignoreerrors
   ```

   In the example above, the first detected hard disk is erased in one pass. Confirmations are encountered and errors are ignored.
3. Save the autoexec.bat file in the root directory of the system floppy disk and exit the edit utility.
4. Remove the floppy from this floppy drive.
5. The floppy is now ready for automatic data erasing.

Erasing Data Using Autoexecute

To erase data using Autoexecute Mode, follow these steps:

1. Go to the machine that requires data erasing
2. With the PC power off, insert the **Active@ Eraser** Automatic Mode floppy disk into drive A:
3. Start the PC by turning on the power.
4. The PC indicates booting into DOS. The data erase process begins.

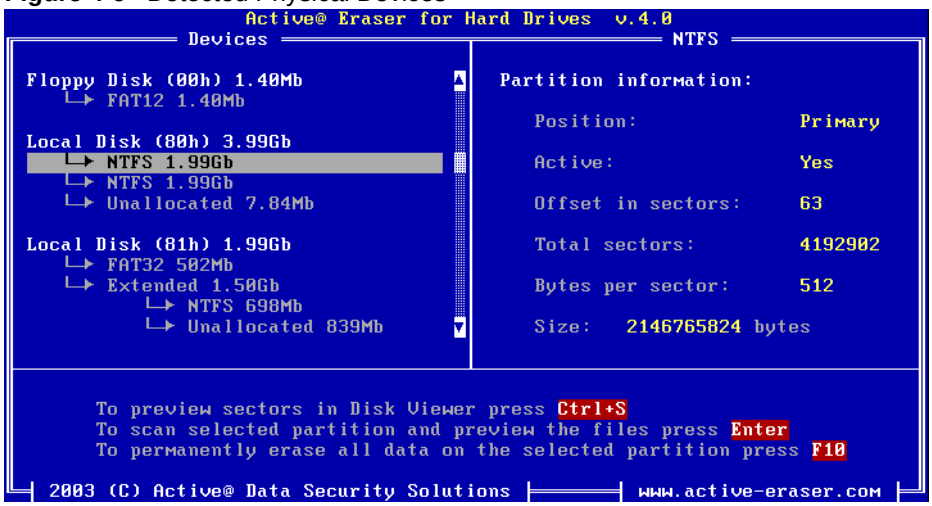
Erasing Logical Drives (Partitions)

In all previous examples in this chapter, the process has removed data from a physical drive. Using a similar method, you can erase logical disks and partitions, and even “Unallocated” areas where partitions existed and the area was damaged, or the area is not visible by the current operating system.

Open the DOS Interactive Mode screen and follow the steps below.

1 The **Detected Physical Devices** screen appears as below:

Figure 4-6 Detected Physical Devices



All system hard drives and floppy drives are displayed in the left pane along with their system information in the right pane.

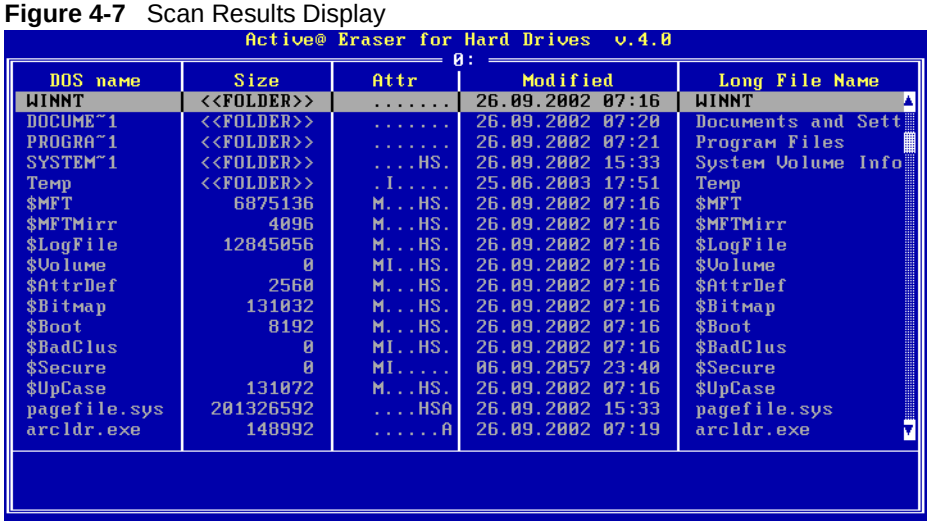
2 Position the cursor over a logical disk or an Unallocated area. A set of options appears in the lower pane of this window.

3 Press **[Ctrl + S]** to open **Disk Viewer** and preview all sectors of this drive

4 When positioned on a logical drive, press **[Enter]** to scan the drive and preview files and folders on the drive. This option allows you to thoroughly check the drive’s folders, hidden and visible files and previously deleted files before erasing data.

When you press **[Enter]**, an activity bar appears while the drive contents are scanned. After the scan has completed, the contents of the drive are displayed similar to the figure below:

Figure 4-7 Scan Results Display



Navigate up and down the displayed list using up and down arrows or Page Up and Page Down keys. Press **[Enter]** to open a folder and view the contents. Similarly, press **[Enter]** to open Disk Viewer and view the contents of a file.

Press **[Esc]** when finished viewing to return to the **Detected Physical Devices** window.

5 In the Detected Physical Devices window, press **[F10]** to securely remove data.

Erase Operation Complete

After operation is completed successfully, information on how drives have been erased is displayed similar to the data below:

```
------------- Erase Session ----------------------
Active@ Eraser started at: Thu Feb 20 11:56:51 2003
     Target:  Floppy (00h) 1.40MB
 Erase method: US DoD 5220.22-M   Passes:3
Verification:40% (completed successfully)
Time taken: 00:01:26
Total number of erased device(s), partition(s): 1
```

If the process encountered errors, for example from bad clusters, a summary of errors would be presented in this report. Use the keyboard arrow keys to scroll through the report.

Details of this report are saved to a log file located in the same order from which you started Active@ Eraser.

5 COMMON QUESTIONS

I cannot boot the machine from a floppy. What is wrong?

There are many possible reasons that you cannot boot from a floppy. Please consult this troubleshooting chart:

Table 5-1 Troubleshooting Floppy Disk Problems

Problem	Solution
Floppy disk is not bootable or damaged.	With the floppy in drive A:, verify whether or not system files (COMMAND.COM, etc.) are located on floppy. If the disk directory can be read and system files appear by name, the disk or some files on the disk may be damaged. On a DOS or Windows PC, run SCANDISK.EXE to check for damaged areas on the disk surface. Alternately, prepare and test another bootable floppy disk.
Machine has boot priority for Hard Disk Drives, or another device set higher than for Floppy Drives.	Open the low-level setup screen, usually by pressing **[F1]** or **[Delete]** on the keyboard during PC startup. These setup parameters build structure in the BIOS. Locate the section about Boot Device Priority, or similar. This section allows you to set the search order for types of boot devices. When the screen opens, a list of boot devices appears. Typical devices on this list are Hard Drives, CD ROM drives, Floppy Drives and Network Boot option. If the floppy device has been disabled, enable it (provided you have a floppy disk installed). The priority should indicate that the floppy device is the number one device the BIOS consults when searching for boot instructions. If Floppy Drives is at the top of the list, that is usually the indicator.

Which operating systems are supported by Active@ Eraser?

Active@ Eraser runs in the Microsoft DOS environment. As it can be installed easily onto a bootable floppy disk, it does not matter which operating system is installed on the machine hard drive. If you can boot in DOS mode from the boot diskette, you can detect and erase any drives independent of the installed Operating System.

How is the data erased?

Active@ Hard Drive Eraser communicates with the system board Basic Input-Output Subsystem (BIOS) functions to access hardware directly. It uses Logical Block Addressing (LBA) access if necessary to clean FAT32 drives more than 8 Gb in size. To erase data it overwrites all addressable locations on the drive with a character or character set defined for a particular method.

For example, to conform to US DoD 5220.22-M security standard, it overwrites locations on the drive three times using the following:

- First time with zeros (0x00)
- Second time with 0xFF
- Third time with random characters

When using **User Defined Number of Passes**, it overwrites each time with random characters.

6 ERASING PARAMETERS

This chapter describes the parameters used with various erasing methods.

Number of Passes

One Pass Zeros or One Pass Random

When using **One Pass Zeros** or **One Pass Random**, the number of passes is fixed and cannot be changed.

When the write head passes through a sector, it writes only zeros or a series of random characters.

User Defined

For **User Defined** method, the user can indicate the number of times the write head passes over each sector. Each overwriting pass is performed with a buffer containing random characters.

US DoD 5220.22-M

The write head passes over each sector three times. The first time with zeros (0x00), second time with 0xFF and the third time with random characters. Final pass is to verify random characters by reading.

German VSITR

The write head passes over each sector seven times.

Russian GOST p50739-95

The write head passes over each sector five times.

Gutmann

The write head passes over each sector 35 times. For details about this, the most secure data clearing standard, you can read the original article at the link below: <http://www.cs.auckland.ac.nz/~pgutool/pubs/secure_del.html>

Verification

After erasing is complete you can direct software to perform verification of the surface on the drive to be sure that the last overwriting pass was performed properly and data residing on drive matches data written by the erasing process.

Because verification is a long process, you can specify a percentage of the surface to be verified. You can also turn the verification off completely.

Retry Attempts

If an error is encountered while writing data onto the drive (for example, due to physical damage on the drive's surface), Active@ Eraser tries to perform the operation again. You can specify number of retries to be performed.

Sometimes a damaged sector can be overwritten if the drive is not completely damaged, after several retries.

Ignore Errors

If this option is turned on, error messages will not be displayed while data erasing or verification is in progress.

While displaying error messages have been ignored, all information about these errors are written to the HDERASER.LOG file. They are displayed after the process is complete in the final Erasing Report.

Clear Log File before Start

If this option is turned on, HDERASER.LOG log file truncates before erasing starts. After erasing is completed, the log file contains information only about the last session.

If this option is turned off, HDERASER.LOG log file will not be truncated and information about the last erasing session appends to the end of the file.

Skip Confirmation

The confirmation step happens when the user types ERASE-ALL-DATA as the final step before the erasing process starts. If **Skip Confirmation** is turned on, the request for confirmation is skipped. This option is typically to be used by advanced users in order to speed up the process.

Turning off this option (default state) is safer because you have one last chance to ensure that data from the correct drive location is going to be erased completely with no possibility of future data recovery.