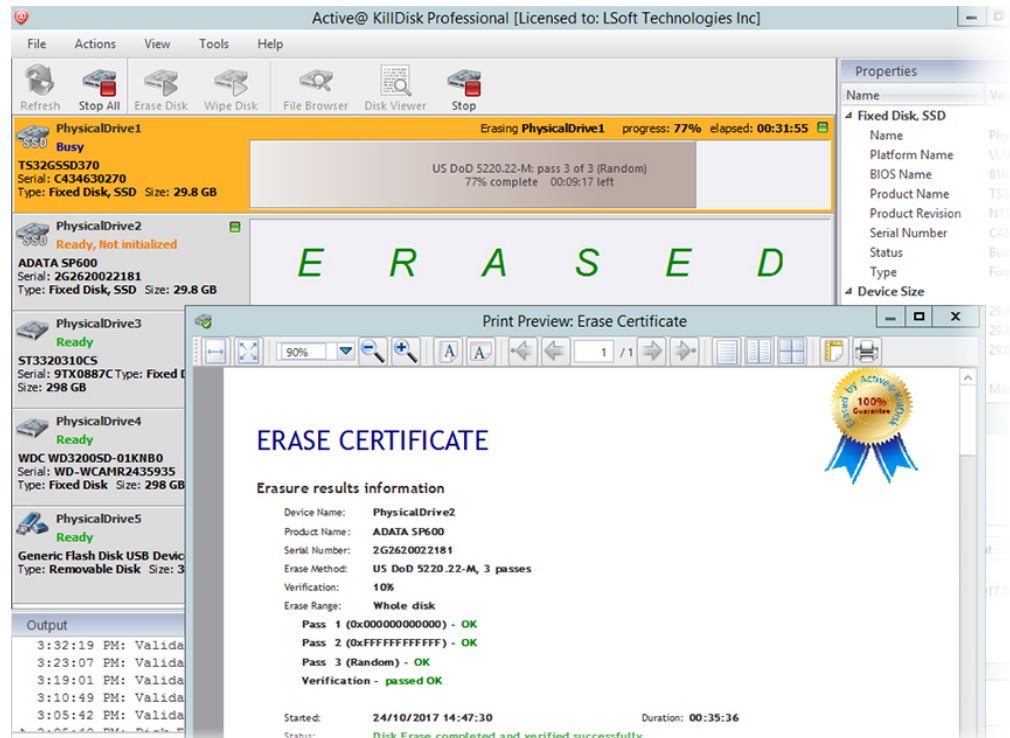


Active@ KillDisk is a powerful and compact software utility that can completely and securely destroy all data on hard drives, removable disks, and flash media devices, without the possibility of future recovery.



Exposing Confidential Data

Confidential data stored on a hard drive can reside in spaces where data may have been stored temporarily.

Files may have been deleted by conveniently using the Windows Recycle Bin and then subsequently emptied but data can still reside on the storage media.

Attackers who want to retrieve confidential data are becoming more resourceful by looking into places where data might be stored temporarily.

An avenue of attack is the recovery of data from residual data on a discarded hard disk drive.

Commands such as DELETE, FORMAT, and FDISK do not remove data as they merely change the FAT/MFT and ROOT table of contents on the file system leaving all the actual data on the disk untouched.

Wiping Confidential Data

Active@ KillDisk's Wipe method processes all unoccupied drive space so that data recovery of previously deleted files becomes impossible.

Installed applications and existing data are not touched by this process.

When you wipe unoccupied drive space, the process is run from the provided bootable operating system.

As a result, the wipe or erase process uses an operating system that is outside the local hard drive and is not impeded by Windows system caching.

This means that deleted Windows system records can be wiped clean.

Active@ KillDisk wipes unused data residue from file slack space, unused sectors, and unused space in MTF records or root records.

Complete Disk Erasing

When you erase data with Active@ KillDisk, you destroy data permanently, conforming to any one of more than 20 methods including international standards, DoD 5220.22-M and your own custom settings.

Regardless of the operating system, file systems or type of machine, Active@ KillDisk can be started using a variety of bootable media to destroy all data on all storage devices.

It does not matter which operating systems or file systems are located on the machine.

By using Active@ KillDisk all data on your Hard Disk Drive, Solid State Drive, USB disk or Memory Card can be destroyed.

Disposal, recycling, selling or donating your storage device can be done with peace of mind that no confidential data has been left behind.



How is the data erased?

Active@ KillDisk communicates with the system Basic Input-Output Subsystem (BIOS) functions directly to access hardware and bypassing the Operating System & File System. This means that disk can be sanitized independently of installed OS & FS .

Active@ KillDisk Console runs in a console text mode, providing the same functionality as GUI version. It is a replacement for the obsolete DOS version. This edition comes with a bootable TinyCore-based ISO image used to create a bootable CD/DVD/USB stick being able to boot both modern UEFI Secure Boot 64-bit systems and legacy 32-bit BIOS PC. Console application also has a support for **Secure Erase** – low-level ATA command providing hardware data sanitation.

To erase data it overwrites all addressable locations on the drive. **Active@ KillDisk Professional** complies to the US DoD 5220.22-M security standard requiring an overwrite of all addressable storage and indexing locations on the drive three times.



Bootable Media Creation

The software package includes a Universal Boot Disk Creator for the creation of CD/DVD/USB bootable media for all targets: Windows, Linux & Console.

Active@ Boot Disk Creator helps you prepare a bootable CD, DVD, Blu-ray or USB mass storage device that you may use to start a machine and repair security access issues or destroy all data on the hard drives.

Run **Bootable Disk Creator** from the Windows Start menu (Windows platform) and follow the wizard steps to prepare a bootable media.

Besides standard BIOS boot, Linux-based boot disk (LiveCD) and Windows-based Boot Disk support UEFI secure boot on x64 systems. Console boot disks supports also x86 BIOS boot for legacy 32-bit systems.



Logging and Reporting

Erase sessions can be logged to keep a record of the storage device erasure including model number/serial number, erase method used and time/data occurred.

A Custom Logo & Info can be embedded into erase/wipe Certificate and saved in a PDF format. Notifications and reports can be sent by e-mail.



Automated Mode

The utility has a command line mode. It allows scripting of the erase procedure for automated execution without user intervention.

Example: `A:\killdisk -ea -em=2 -nc -bm`

In this example it will automatically detect and erase all detected hard drives using DoD 5220.22 M data destruction method (3 passes) with no user interaction and return control to the calling application.

Application returns exit code is 0 (zero) if no errors detected, **1 (one) or 2 (two)** - if errors or warnings occurred.

An option to save the log and shutdown the PC after erase completes is also available.

Disk Viewer

Browse the contents, files and folders, before erasing. View raw disk sectors with use of **Disk Viewer** (displaying hex/ASCII symbols) to reveal disk data before or after an erase session.

Feature Set

- ✓ Parallel erasing of multiple disks at the same time, independent erase & wipe sessions
- ✓ Erasing disks with **One Pass Zeros** sanitizing standard
- ✓ Support for more than **20 international erasing standards** including **US DoD 5220.22 M** and User Defined method
- ✓ Command Line parameters used in scripting allow to automate erase procedures (Batch Mode)
- ✓ Certificates can be customized with company's logo & comments can be easily added to certificates for each session
- ✓ Included Windows-based boot disk supporting UEFI secure boot on x64 systems
- ✓ Included Linux-based boot disk (LiveCD) supporting UEFI secure boot on x64 systems
- ✓ Console application supports Secure Erase (ATA command) for SSD/HDD
- ✓ User defined erase method can specify custom pattern for each pass using even hexadecimal (HEX) values
- ✓ Ability to send e-mail reports via pre-configured FREE SMTP account at **www.smtp-server.com**
- ✓ Save Log & Shutdown PC option after erase completed
- ✓ Fingerprint (sanitizing status: date, erase method) can be placed to first disk's sector & displayed after boot up the disk
- ✓ Displays information about all volumes, partitions, hard disks, external USB disks & Memory cards currently connected
- ✓ Wipes out unused space on all disks completely by securely overwriting data on the physical level
- ✓ Detects, displays and erases disk hidden zones (HPA/DCO areas)
- ✓ Support for wiping out unused sectors on Apple HFS+, Linux Ext2/Ext3/Ext4, Unix UFS/XFS/JFS & MS FAT/exFAT/NTFS
- ✓ Supports all possible I/O interfaces: IDE / USB / SATA / eSATA / SSD / SCSI disks, LUN / RAID disk arrays
- ✓ Supports large-size disks (more than 4TB in size) & new disks having 4kb sector size
- ✓ Built-in Hex Viewer allows to inspect raw disk's sectors: MBR, volume boot sectors, file system records & data file clusters
- ✓ Very easy to use: intuitive user interface for beginners, as well as a powerful command line mode for advanced users
- ✓ Supports fixed disks (HDD), Solid State Disks (SSD), Memory Cards and USB/USB3 external devices
- ✓ Utility can be placed on a bootable disk and used from it. You do not even need to boot from the hard drive to erase it
- ✓ Supports MBR and GPT (GUID Partition Table) style partitioning for wiping/erasing of volumes
- ✓ Certificate can be displayed after erase/wipe completion and saved as PDF
- ✓ Erases physical disks, partitions, logical drives & even unused disk space
- ✓ Boot Disk Creator can pre-configure KillDisk startup process on the Boot Disk using Command Line parameters
- ✓ Universal Boot Disk Creator prepares CD/DVD/BD/ISO/USB media for bootable Windows/Linux/Console environment

New! ATA Secure Erase command – low-level hardware sanitation - available in Ultimate package

Erase and Wipe Methods supported:

1. Erases with one-pass zeros
2. Erases with one-pass random characters
3. Erases with user-defined number of passes (up to 99)
4. US Department of Energy M205.1-2
6. US Department of Defense 5220.22 M
7. US Department of Defense 5220.22 M (ECE)
8. German VISTR compliant
9. Russian GOST p50739-95 compliant
10. Gutmann compliant
11. Bruce Schneier's algorithm
12. Canadian OPS-II
13. Canadian CSEC ITSG-06
14. British HMG IS5 Baseline
15. British HMG IS5 Enhanced
16. Navso P-5329-26 (RL)
17. Navso P-5329-26 (MFM)
18. NCSC-TG-025
19. US Army AR380-19
20. US Air Force 5020
21. NIST 800-88 erase 1 standard
22. NIST 800-88 erase 2 standard
23. NIST 800-88 erase 3 standard
24. Australian ISM-6.2.93
25. Secure Erase ATA low-level command

System Requirements:

<http://www.killdisk.com/system.htm>

Helpful Online Resources:

<http://www.killdisk.com/features.htm>

<http://www.killdisk.com/history.htm>

<http://www.killdisk.com/screen.htm>

<http://www.killdisk.com/killdisk-faq.htm>

http://www.killdisk.com/automating_erasure_1.htm

Active@ KillDisk
www.killdisk.com
sales@lsoft.net
(877) 477-3553