End-User License Agreement

Active@ ZDelete 9

Copyright(c) 1999-2020 LSoft Technologies Inc. All Rights Reserved.

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 LSoft Technologies Inc. for the ZDelete 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.

LSoft Technologies Inc. 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

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

1. GRANT OF LICENSE. This EULA grants you the right to install and use one copy of the SOFTWARE or any prior version on a single computer; a license for the SOFTWARE may not be shared or used concurrently on different computers.

2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS. Limitations on reverse engineering, recompilation, disassembly, modify, translate SOFTWARE, make any attempt to discover the source code of the SOFTWARE.

3. RENTAL. You may not rent, lease, or lend the SOFTWARE.
**Disclaimer of Warranty.** This SOFTWARE and the accompanying files are provided "as is" and without warranties as to performance or merchantability or any other warranties whether expressed or implied. You use the SOFTWARE at your own risk. No liability for consequential damages. To the maximum extent permitted by applicable law, in no event shall the Lsoft Technologies Inc. or its suppliers be liable for any special, incidental, indirect, or consequential damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use this SOFTWARE, even if Lsoft Technologies Inc. has been advised of the possibility of such damages. In any case, the Lsoft Technologies inc. entire liability under any provision of this EULA shall be limited exclusively to product replacement.

Lsoft Technologies Inc. reserves all rights not expressly granted here.

---

**Introduction**

An overwhelming majority of people, businesses and organizations do not understand the importance of security in digital data storage. An average hard drive stores thousands of files written on it and many of them contain sensitive information. Over the course of a hard drives lifetime the likelihood for recoverable remnants of sensitive information left on a drive at its end of life is very high.

**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 using sophisticated channel coding techniques such as PRML (Partial Response Maximum Likelihood), 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. Almost all the data can also be easily restored with an off-the-shelf data recovery utility like Active@ File Recovery, making your erased confidential data quite accessible.

Using ZDelete all files on your hard drive or removable device can be destroyed without the possibility of future recovery. After using ZDelete the process of disposal, recycling, selling or donating your storage device can be done with peace of mind.

**Related information**

Using ZDelete on page 9
Erase Disk Concepts on page 19

**Erasing Confidential Data**

Modern methods of data encryption are deterring network attackers from extracting sensitive data from stored database files.

Attackers (who want to retrieve confidential data) become more resourceful and look for places where data might be stored temporarily. For example, the Windows DELETE command merely changes the files attributes and location so that the operating system will not look for the file. The situation with NTFS is similar.

One avenue of attack is the recovery of data from residual data on a discarded hard drive. When deleting confidential data from hard drives, removable disks or USB devices, it is important to extract all traces of the data so that recovery is not possible.
Most official guidelines regarding the disposal of confidential magnetic data do not take into account the depth of today's recording densities nor the methods used by the OS when removing data.

Removal of confidential personal information or company trade secrets in the past might have been performed using the **FORMAT** command or the **FDISK** command. 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 is 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.

**Related tasks**
- [Erase Files](#) on page 9
- [Related information](#)
- [Erase Disk Concepts](#) on page 19

---

**Wiping Confidential Data**

You may have some confidential data on your hard drive in spaces where the data is stored temporarily. You may also have deleted files by using the **Windows Recycle Bin** and then emptying it. While you are still using your local hard drive there may be confidential information available in these unoccupied spaces.

**Note:** Wiping the logical drive's deleted data does not delete existing files and folders. It processes all unoccupied drive space so that recovery of previously deleted files becomes impossible. Installed applications and existing data are not touched by this process.

**ZDelete** wipes unused data residue from file slack space, unused sectors and unused space in MTF records or directory records.

Wiping drive space can take a long time, so do this when the system is not being actively used. For example, this can be done overnight.

**Related tasks**
- [Wipe Drive](#) on page 12
- [Related information](#)
- [Wipe Disk Concepts](#) on page 20

---

**International Standards in Data Destruction**

**ZDelete** works with more than 20 international standards for clearing and sanitizing data including the **US DoD 5220.22-M** standard. You can be sure that once you erase a disk with **ZDelete** all the sensitive information is destroyed forever.

**Related information**
- [Erase & Wipe Methods (Sanitation Standards)](#) on page 23

© 1999 - 2020 LSoft Technologies Inc.
ZDelete is a data cleanup and erase utility that can delete selected folders and groups of files without any possibility of data recovery afterward. Access to the drive's data is made on the physical level via BIOS (Basic Input-Output Subsystem) bypassing the operating system's logical drive structure organization.

ZDelete is designed to help protect your privacy by deleting files in such a way as to prevent other people from recovering your private data after deletion. Its integrated Disk Wipe can clear out all free space on a hard disk so that recovery of deleted files becomes impossible. It is a powerful and flexible data shredder for information that must be permanently directed away from the hard drive.

ZDelete is a powerful software that delivers the following main features:

- Destroy data permanently with a choice of 20+ international disk sanitizing standards including US DoD 5220.22-M
- Sanitize external disks (USB drives, external HDD/SSD) connected to both USB 2.0 and 3.1 ports
- Wipe out unused clusters and metadata on live volumes, leaving existing data intact, cleaning up free and slack space according to the concepts
- Windows Drag-and-Drop functionality
- Graphical User Interface integrated with Windows Explorer
- Functions reside in context command menus
- ZDelete Bin - familiar, comfortable and reliable erasure mechanism

© 1999 - 2020 LSoft Technologies Inc.
System Requirements

ZDelete is designed to run on Windows operating system with the following minimum requirements:

**Workstation**
- IBM PC compatible machine
- Intel Pentium or higher
- 2 Gb of RAM
- 50Mb of free disk space

**Video**
- VGA (1024x768) resolution or better

**Operating Systems**
- Windows XP or higher

**Drive Storage**

Disk types supported:
- HDD via IDE, ATA, SATA I, SATA II, SATA III, SAS
- SSD via SATA I, SATA II, SATA III, SAS
- External eSATA & USB disks
- SCSI & iSCSI devices
- Onboard NVMe M.2 (SATA & PCI-E types)
- Removable media (USB drive, MemoryStick, SD card, Compact Flash, Floppy Disk, Zip Drive)

Software Updates

ZDelete has a built-in update client to ensure you always have an access to the latest version of the application, with the option to roll back to older versions if needed. To update, use the file menu bar to navigate to **Help > Updates**
Installation and setup

Figure 1: Checking for updates

Update dialog contains history of previously installed versions and updates.

If there is an available update, this window will notify and help you to install the latest version. If you've upgraded from an older version, you may also roll back to the older version using the Rollback current version to the previously installed version feature by selecting the checkbox.

Important Note: ZDelete stores your previously installed versions so you may roll back to any of your older versions at any time.

Installation and setup

In order to install ZDelete follow the steps below.

1. Download ZDeleteSetup.exe from our website: https://www.zdelete.com
2. Run ZDeleteSetup.exe as an administrator
3. Follow the **Setup Wizard** steps to successfully install the software

![ZDelete Setup Wizard](image)

**Figure 2: ZDelete Setup Wizard**

## Using ZDelete

ZDelete is a powerful tool to provide disk erasure solutions for personal use. This guide will help you to get started with configuring ZDelete for your system and using it to the full potential. ZDelete allows you to launch any of its actions from a graphical user interface:

![ZDelete Main View](image)

**Figure 3: Main View**

### Erase Files

ZDelete is an extremely powerful tool for file erasure. Individual files can be erased according to any desired standard with just a few clicks. The process to achieve this is described below.
1. Select files for erasure

Use **Erase Files** button or main menu **Action > Erase Files** to select 1 or more files. For multiple selection use **Ctrl+Left Mouse** click.

![Figure 4: Files’ multiple selection](image)

**Note:** If the selected drive/volume can not be locked exclusively by **ZDelete** the process of forcing dismount could be initiated:

![Figure 5: Force Dismount](image)

2. Confirm erasure in the dialog

![Figure 6: Initiating the Erase operation](image)

3. Observe erase process

When the **Erase** procedure begins you see the disk area representation as a progress bar as well as a chosen **erase method**. The progress bar represents the percentage of file(s) space processed. As the
procedure progresses the percentage increases and estimated time is recalculated. You are able to
**STOP** or **PAUSE** the process at any time.

![File(s) Erasure Progress](image)

**Figure 7: File(s) Erasure Progress**

A confirmation dialog appears at the end of successful erase:

![Confirmation Dialog](image)

**Note:** You may disable this dialogue from appearing every time. Simply check the box reading
**Don't show this dialog**

When erase is completed user is able to check the **Log file**.

**Related information**

Erase & Wipe Methods (Sanitation Standards) on page 23

---

**Erase Folder**

In addition to **files erase** an individual folder (with all the files) can be erased according to any **desired standard**. The process to achieve this is described below.

1. **Select folder to erase**

   ![Erase Folder Button](image)

   Use **Erase Folder** button or main menu **Action > Erase Folder** to select a folder to erase.

   **Note:** If the selected drive/volume can not be locked exclusively by **ZDelete** the process of forcing dismount could be initiated:

   ![Force Dismount](image)

   **Figure 8: Force Dismount**
2. Confirm erasure in the dialog

![Image of Confirm Erasure Dialog]

**Figure 9: Initiating the Folder Erase operation**

The erasure procedure starts

3. Observe erase process

When the *Erase* procedure begins you see the 2 progress bars represent the percentage of folder file(s) processed as well as a chosen erase method. As the procedure progresses the percentage increases and estimated time is recalculated. You are able to **STOP** or **PAUSE** the process at any time.

![Image of Erase Progress]

**Figure 10: Folder Erasure Progress**

A confirmation dialog appears at the end of successful erase:

![Image of Confirmation Dialog]

**Note:** You may disable this dialogue from appearing every time. Simply check the box reading **Don't show this dialog**

When erase is completed user is able to check the Log file.

**Related information**

Erase & Wipe Methods (Sanitation Standards) on page 23

---

**Wipe Drive**

In addition to files erase and Erase Folder on page 11 a powerful process of **wiping** can be applied to a drive/volume according to any **desired standard**. The process to achieve this is described below.
1. Select a drive to wipe

Use **Wipe Drive** or main menu **Action > Wipe Drive** to select a drive to wipe.

![Drive/Volume Selection](image1)

**Figure 11: Drive/Volume Selection**

- **Note:** If the selected drive/volume can not be locked exclusively by ZDelete the process of forcing dismount could be initiated:

![Force Dismount](image2)

**Figure 12: Force Dismount**

2. Observe erase process

When the **Wipe** procedure begins you see the disk area representation as a progress bar as well as a chosen erase method. The progress bar represents the percentage of drive space processed. As the procedure progresses the percentage increases and estimated time recalculated. You are able to **STOP** or **PAUSE** the process at any time.

![Wipe Drive Progress](image3)

**Figure 13: Wipe Drive Progress**

Related information

- **Erase & Wipe Methods (Sanitation Standards)** on page 23
- **Wipe Disk Concepts** on page 20

**ZDelete Bin**

**ZDelete Bin** is a convenient method for secure erasing files and folders according to international security standards while maintaining the comfort of having a Recycle Bin to drag these files into.

![ZDelete Bin](image4)
Note: Once files are deleted using the ZDelete Bin, they are unrecoverable by any file recovery software or data recovery laboratory.

In order to delete files/folders with ZDelete Bin mechanism do the following:

- Drag the selected file(s)/folder(s) into the ZDelete Bin desktop icon:

![Figure 14: Drag and drop a selected file to the Bin](image1)

![Figure 15: Drag and drop selected folders to the Bin](image2)

- Confirm erasure in the dialog for files(s) or folder(s) and proceed with the procedures

Note: Make sure the file(s) is not currently open or being used. This may prevent the erasure process from initiating.

ZDelete Context Menu Features

There is an option to use a Windows Explorer's context menu for file(s), folders and drives selection for the process of erasing or wiping.

For erasing a file(s) Right Mouse Click on selected file(s) in Windows Explorer and choose an option of ZDelete Item(s) in pop-up context menu:
For wiping a drive simply **Right Mouse Click** the desired drive in *Windows Explorer* and proceed with the option of **ZDelete Disk Wiper**:

**Figure 17: Drive selection for wiping**

**Related tasks**

*Erase Files* on page 9
Wipe Drive on page 12

Additional Options and Features

ZDelete also has a number of extra features to ensure the most complete sanitation operations, flexibility to meet the most strict requirements and compatibility with a wide range of systems. This section outlines these features.

Log Files

User is able to reach the log records (history) via main menu File > View Log

Right Mouse Click on Log window for Save Log and Clear Log options.

Figure 18: Main menu
System Tray

User is able to minimize ZDelete to System Tray (hide) via main menu File > Hide or simply by pressing a Close button.

Figure 19: Log file sample

Figure 20: Main menu

Use Right Mouse Click > Show on System Tray ZDelete icon for restoring.
Application Settings

ZDelete supports more than 20 international disk sanitation standards and a variety of other customizations to fit a wide range of requirements. These customizations are set in ZDelete main menu Action > Settings.

- **Erase Method** drop box with selection of all ZDelete available erase methods for files or folders
- **Wipe Method** drop box with selection of all ZDelete available wipe methods for drives.
- **Wipe unused clusters** option to wipe unused clusters according to the concepts
- **Wipe Metadata/System files area** option to wipe metadata and system files according to the concepts
- **Verification** option to run a verification on some of the erase methods. User is able to set a part (in percentage) of erased area to verify
- **Don't show report after erase** option to avoid showing of a report message box
- **Don't show confirmation dialog** option to avoid showing of erase/wipe confirmation dialog
Appendix

Erase Disk Concepts

Erasing Confidential Data

Modern methods of data encryption are deterring network attackers from extracting sensitive data from stored database files.

Attackers (who want to retrieve confidential data) become more resourceful and look for places where data might be stored temporarily. For example, the Windows DELETE command merely changes the files attributes and location so that the operating system will not look for the file. The situation with NTFS is similar.

One avenue of attack is the recovery of data from residual data on a discarded hard drive. When deleting confidential data from hard drives, removable disks or USB devices, it is important to extract all traces of the data so that recovery is not possible.

Most official guidelines regarding the disposal of confidential magnetic data do not take into account the depth of today's recording densities nor the methods used by the OS when removing data.

Removal of confidential personal information or company trade secrets in the past might have been performed using the FORMAT command or the FDISK command. 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 is 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.

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 using sophisticated channel coding techniques such as PRML (Partial Response Maximum Likelihood), 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. Almost all the data can also be easily restored with an off-the-shelf data recovery utility like Active@ File Recovery (https://www.file-recovery.com), making your erased confidential data quite accessible.

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

International Standards in Data Removal

Active@ ZDelete conforms to more than 22 international standards for clearing and sanitizing data (US DoD 5220.22-M, Peter Gutmann etc.). You can be sure that sensitive information is destroyed forever once you erase a disk with Active@ ZDelete.
Active@ ZDelete is a professional security application that destroys data permanently on any computer that can be started using a bootable CD/DVD-ROM or USB Flash Disk. Access to the drive's data is made on the physical level via the BIOS (Basic Input-Output System) bypassing the operating system's logical drive structure organization.

Wipe Disk Concepts

Wiping Confidential Data from Unoccupied Disk's Space

You may have confidential data on your hard drive in spaces where data may have been stored temporarily.

You may also have deleted files by using the Windows Recycle Bin and then emptying it. While you are still using your local hard drive, there may be confidential information available in these unoccupied spaces.

Wiping the logical drive's deleted data does not delete existing files and folders. It processes all unoccupied drive space so that 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 bootable CD/DVD 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.

ZDelete wipes unused data residue from file slack space, unused sectors, and unused space in MTF records or directory records.

Wiping drive space can take a long time, so do this when the system is not being otherwise utilized. For example, this can be done overnight.

Wipe Algorithms

The process of deleting files does not eliminate them from the hard drive. Unwanted information may still be left available for recovery on the computer. A majority of software that advertises itself as performing reliable deletions simply wipes out free clusters. Deleted information may be kept in additional areas of a drive. ZDelete therefore offers different wipe algorithms to ensure secure deletion: overwriting with zeros, overwriting with random values, overwriting with multiple passes using different patterns and much more. ZDelete supports more than 20 international data sanitizing standards, including US DoD 5220.22-M and the most secure Gutmann's method overwriting with 35 (!) passes.

![Figure 23: Disk free space and allocated clusters](image)

Wiping File Slack Space

This relates to any regular files located on any file system. Free space to be wiped is found in the "tail" end of a file because disk space is usually allocated in 4 Kb clusters. Most files have sizes that are not 4 Kb increments and thus have slack space at their end.
Figure 24: Disk free space and allocated clusters

Specifics of Wiping Microsoft NTFS File System

NTFS Compressed Files

Wiping free space inside a file: The algorithm NTFS uses to "compress" a file operates by separating the file into compressed blocks (usually 64 Kb long). After it is processed, each of these blocks has been allocated a certain amount of space on the volume. If the compressed information takes up less space than the source file, then the rest of the space is labeled as sparse space and no space on the volume is allocated to it. Because the compressed data often doesn't have a size exactly that of the cluster, the end of each of these blocks stays as unusable space of significant size. Our algorithm goes through each of these blocks in a compressed file and wipes the unusable space, erasing previously deleted information that was kept in those areas.

Figure 25: Compressed file structure

The MFT (Master File Table) Area

Wiping the system information:

The MFT file contains records, describing every file on the volume. During the deletion of these files, the records of their deletion are left untouched - they are simply recorded as "deleted". Therefore file recovery software can use this information to recover anything from the name of the file and the structure of the deleted directories down to files smaller than 1Kb that are able to be saved in the MFT directly. The algorithm used by ZDelete wipes all of the unused information out of the MFT records and wipes the unusable space, making a recovery process impossible.
Specifics of Wiping Microsoft FAT File System

Wiping Directory Areas

Each directory on a FAT/FAT32 or an exFAT volume can be considered as a specific file, describing the contents of the directory. Inside this descriptor there are many 32-byte records, describing every file and other inner folders.

When you delete files this data is not being fully erased. It is just marked as deleted (hex symbol \texttt{0xE5}). That's why data recovery software can detect and use these records to restore file names and full directory structures.

In some cases dependent on whether a space where item located has been overwritten yet or not, files and folders can be fully or partially recovered.

\texttt{Active@ ZDelete} makes data recovery impossible by using an algorithm that wipes out all unused information from directory descriptors. \texttt{Active@ ZDelete} not only removes unused information, but also \textit{defragments} Directory Areas, thus speeding up directory access.
Erase & Wipe Methods (Sanitation Standards)

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.

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. There is one final pass to verify random characters by reading.

Canadian CSEC ITSG-06

The write head passes over each sector, writing a random character. On the next pass, writes the compliment of previously written character. Final pass is random, proceeded by a verify.
Canadian OPS-II
The write head passes over each sector seven times (0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF, random). There is one final pass to verify random characters by reading.

British HMG IS5 Baseline
Baseline method overwrites disk's surface with just zeros 0x00. There is one final pass to verify random characters by reading.

British HMG IS5 Enhanced
Enhanced method - 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. There is one final pass to verify random characters by reading.

Russian GOST p50739-95
The write head passes over each sector two times. (0x00, Random). There is one final pass to verify random characters by reading.

US Army AR380-19
The write head passes over each sector three times. The first time with 0xFF, second time with zeros 0x00 and the third time with random characters. There is one final pass to verify random characters by reading.

US Air Force 5020
The write head passes over each sector three times. The first time with random characters, second time with zeros 0x00 and the third time with 0xFF. There is one final pass to verify random characters by reading.

NAVSO P-5329-26 RL
*RL method* - the write head passes over each sector three times (0x01, 0x27FFFFFF, Random). There is one final pass to verify random characters by reading.

NCSC-TG-025
The write head passes over each sector three times (0x00, 0xFF, Random). There is one final pass to verify random characters by reading.

NSA 130-2
The write head passes over each sector two times (Random, Random). There is one final pass to verify random characters by reading.

NIST 800-88
Supported three NIST 800-88 media sanitation standards:
1. The write head passes over each sector one time (0x00).
2. The write head passes over each sector one time (Random).
3. The write head passes over each sector three times (0x00, 0xFF, Random).

For details about this, the most secure data clearing standard, you can read the original article at the link below: [http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf](http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf)

German VSITR
The write head passes over each sector seven times.
Bruce Schneier
The write head passes over each sector seven times (0xFF, 0x00, Random, Random, Random, Random, Random). There is one final pass to verify random characters by reading.

Peter 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/%7Epgut001/pubs/se%0Acure_del.html

Australian ISM-6.2.93
The write head passes over each sector once with random characters. There is one final pass to verify random characters by reading.