

KillDisk 11 - User Manual



Contents

KillDisk 11 - User Manual.....	4
Legal statement.....	5
Introduction.....	6
Advanced Data Recovery Systems.....	6
Erasing Confidential Data.....	6
Wiping Confidential Data.....	7
International Standards in Data Destruction.....	7
KillDisk overview.....	8
Software Licensing.....	9
Registering the Software (Online).....	9
Registering the Software (Offline).....	11
Deactivating a Registration.....	13
Software Updates.....	14
System requirements.....	15
Security hardware.....	16
Getting Started with KillDisk.....	17
KillDisk Installation and Distribution.....	17
Active@ Boot Disk Creator.....	18
Launching and initial configuration.....	21
Navigating through the Application.....	21
Disk Bay Layout Overview.....	24
Create a new Disk bay layout.....	25
Save and Import Disk bay layout.....	26
Formatting disk bay layout.....	27
Advanced features.....	28
Disk Explorer View.....	30
Disk Bays view.....	30
Disk Bays tree view.....	31
Local Disks tree view.....	33
Using KillDisk.....	35
Disk Erase.....	35
Selecting Disk Area for Erasure & Erasing Partitions.....	37
Disk Wipe.....	38
Examine disks physical integrity.....	40
Additional Options and Features.....	41
Mapping Network Shares.....	41
Changing Disk Serial Number.....	42
Reset Hidden Areas.....	43
Property views.....	43

Dynamic Disks, Virtual Drives and Windows Storage Spaces.....	45
Preferences.....	46
Disk examination options.....	48
General Preferences.....	49
Disk Erase Options.....	50
Disk Wipe Options.....	52
Disk examination preferences.....	53
Certificate Options.....	54
Report Options.....	56
Erase labels preferences.....	58
Disk Viewer Settings.....	60
Error Handling.....	60
Clone preferences.....	61
Disk copy options.....	62
Email Notifications.....	62
Disk cloning.....	63
Mount Disk Image.....	64
Processing Summary.....	65
Reports and Certificates.....	66
Erase Certificate.....	66
Reports.....	67
Erase labels (KillDisk Desktop & Industrial only).....	68
Command Line and Batch Modes.....	72
Command Line Mode.....	72
Batch Mode.....	76
Disk batches.....	77
Using disk batches.....	77
Add disk bays to disk batch.....	78
From Batch control toolbar.....	78
In Disk Bays view.....	79
From main file menu bar.....	80
Edit disk batch attributes.....	80
Advanced Tools.....	87
File Browser.....	87
Disk Viewer.....	89
SMART Monitor.....	91
Application Settings.....	94
Troubleshooting, Backup and System Recovery.....	99
Common Troubleshooting Tips.....	99
Application Log.....	99
Hardware Diagnostic File.....	101
Appendix.....	102
Glossary.....	102
Erase Methods and Sanitation Standards.....	103
File Name Tags.....	105

KillDisk 11 - User Manual

KillDisk



Legal statement

Copyright © 2017, LSOFT TECHNOLOGIES INC. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from LSOFT TECHNOLOGIES INC.

LSOFT TECHNOLOGIES INC. reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of LSOFT TECHNOLOGIES INC. to provide notification of such revision or change.

LSOFT TECHNOLOGIES INC. provides this documentation without warranty of any kind, either implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. LSOFT may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

All technical data and computer software is commercial in nature and developed solely at private expense. As the User, or Installer/Administrator of this software, you agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Active@ KillDisk, the Active@ KillDisk logo, KillDisk, KillDisk for Industrial Systems, KillDisk Desktop and Erasers Software are trademarks of LSOFT TECHNOLOGIES INC.

LSOFT.NET logo is a trademark of LSOFT TECHNOLOGIES INC.

Other brand and product names may be registered trademarks or trademarks of their respective holders.

Introduction

As a relatively new technology, an overwhelming majority of people, businesses and organizations do not understand the importance of security in digital data storage. The average hard drive sees thousands of files written to it, many of which contain sensitive information. Over the course of a hard drive's lifetime, the likelihood for **recoverable** remnants of sensitive information left on a hard drive at its' end of life is very high. To see this firsthand, simply try out KillDisk's *File Browser* on page 87 on your system drive. You'll be surprised to see what you find!



Note: Additionally, try formatting a USB drive with files on it and browse it with KillDisk's *File Browser* on page 87 as well. Data breaches are not limited to hard drives!

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 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, data can also be easily restored with the help of an off-the-shelf data recovery utility like Active@ File Recovery (<http://www.file-recovery.com>), making your erased confidential data quite accessible.

Using KillDisk, 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 KillDisk, disposal, recycling, selling or donating your storage device can be done with peace of mind.

Erasing Confidential Data

Modern methods of data encryption are deterring unwanted network attackers from extracting sensitive data from stored database files. Attackers who want 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 data from residual data on a discarded hard disk drive. When deleting confidential data from hard drives, removable floppies or USB devices, 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, nor the methods used by the operating system when removing data. For example, 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 give 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.

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

Wiping Confidential Data

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.

KillDisk wipes unused data residue from file slack space, unused sectors, and unused space in MFT 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.

International Standards in Data Destruction

KillDisk conforms to dozens of 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 KillDisk, sensitive information is destroyed forever.

KillDisk is a quality security application that destroys data permanently from any computer that can be started using a bootable CD or DVD-ROM. Access to the drive's data is made on the physical level via the BIOS (Basic Input-Output Subsystem), 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.

KillDisk overview

KillDisk for Industrial Systems

This edition of KillDisk is designed to provide a software solution for industrial workstations, configured to service disks in high volumes. KillDisk for Industrial Systems is distributed as a software package that may be installed on a disk erase workstation and used to examine, erase and even write images to individual or batches of disks. Highly customizable, the software is able to conform to any company standards - erasure standards, examination type, reporting, error handling are only a subset of the configurable settings KillDisk supports. All elements of KillDisk's operations may be documented in XML reports, PDF certificates, or even printable labels for erased hard drives. Versatile, easy to navigate and rich in features, KillDisk for Industrial Systems is the ideal KillDisk solution for recyclers and corporations to securely erase hard drives - simply and efficiently.

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

- Erase data on the entire hard disk drive surface, supports parallel erasing of large numbers of disks (hardware-limited);
- Destroy data permanently with a choice of dozens of international disk sanitizing standards;
- Sanitize external disks (USB drives, external HDD/SSD) connected to both USB 2.0 and 3.0 ports;
- Examine disk integrity and overall stability, disk verification and detect bad sectors;
- Auto-erase mode sanitizes disks and prints certificates without of any user interaction;
- Hot-swap operations are fully supported, erase could be auto-initiated upon HDD plug-in;
- Browse file systems on disk volumes and inspect particular sectors Hex Viewer on a low level;
- Issue customizable certificates and detailed reports for disk erase and examination;
- Print different types of labels to be attached to hard disks after erase completion;
- Provides enhanced information about disks and their attributes including S.M.A.R.T. Monitoring;
- and more...

KillDisk 11

KillDisk 11 is the most powerful consumer edition released to date. With the development and release of KillDisk Industrial, KillDisk 11 benefits from industrial stability, improved disk handling, interface layout and several new features including:

- Redesigned and improved user interface
- Enhanced visualization of physical disks and erase processes
- Improved handling of disks with controller malfunctions
- Stable handling of hot-swappable and dynamic disks
- Sound notifications for completed erase jobs with different results
- Auto hibernate or shutdown the system after all jobs are completed
- Enhanced certificates and reports for disk erase and wipe
- Advanced Disk Viewer with flexible Search for low-level disk inspection
- Customizable file names for certificates & XML reports
- Unique Computer ID can be displayed in certificates/reports
- Disk health - S.M.A.R.T. information can be displayed and monitored
- Customizable look & feel: four different application styles included
- ATA Secure Erase command - available in Ultimate package

This release is available as an executable to run in your desktop environment, or in a bootable format with the help of the Active@ Boot Disk Creator - the bootable disk creation tool included in the installation package.

KillDisk maintains the highest standards in disk erasure, and with that, provides extensive documentation options for its' operations through [Reports](#) and printable [Erase Certificate](#) on page 66 and [Erase labels \(KillDisk Desktop & Industrial only\)](#) on page 68.

Software Licensing

KillDisk is licensed **per concurrent use of the software** and for **each concurrent disk being wiped**, outlined in the EULA. The maximum number of disks erased in parallel corresponds to the number of purchased licenses.

One Corporate license grants you the ability to run the software on one machine and erase one disk at any given time. **To run on several machines in an office or multiple drives concurrently on one machine, you require the corresponding number of licenses.**

Site and Enterprise licenses grant the license holder *unlimited* use of the software in a geographical location and worldwide respectively.

This licensing is maintained through software registration and activation. Once the full version of KillDisk is purchased, the license holder will receive an email with their **Registered Name** and **Registration Key**. Any machine that needs to use the full version of the software needs to be activated with this key.

Activations are limited to the number of licenses held. To transfer from one machine to another, they must be deactivated from decommissioned hardware first.

For boot disks to be created, the Active@ Boot Disk Creator must be registered with an active registration key.

Registering the Software (Online)

For this task you require an active internet connection on the machine you wish to register the product on.

After installation, Active@ KillDisk still starts as FREE version (unregistered), you need to register it first to have all professional features activated. To register the software with an active internet connection:

1. Select **Register or Upgrade Software** in the initial Registration & Licensing dialog launched on application start up, or click **Registration...** from the Help menu to access it from the application.

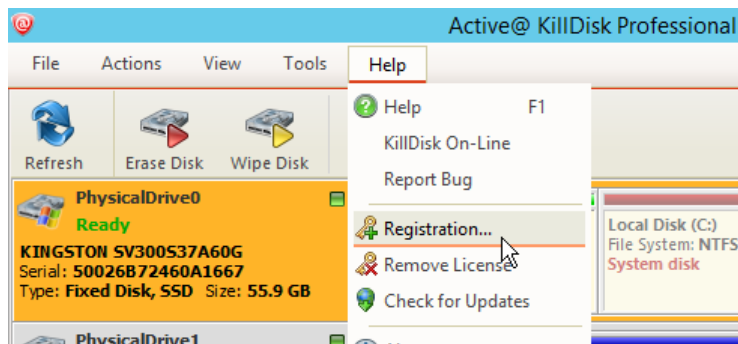


Figure 1: Accessing the registration window

2. Select the **Register or Upgrade Software** radio button
3. Read the License agreement and activate the check box to agree to the terms of the license
4. Click **Next** to proceed with the registration



Figure 2: Registration window

5. Copy & Paste your 30-digit registration key into the field called **Registration Key**:
6. You should receive a response that the software has been registered. The registration is now complete. You may click **Next** and exit the registration window

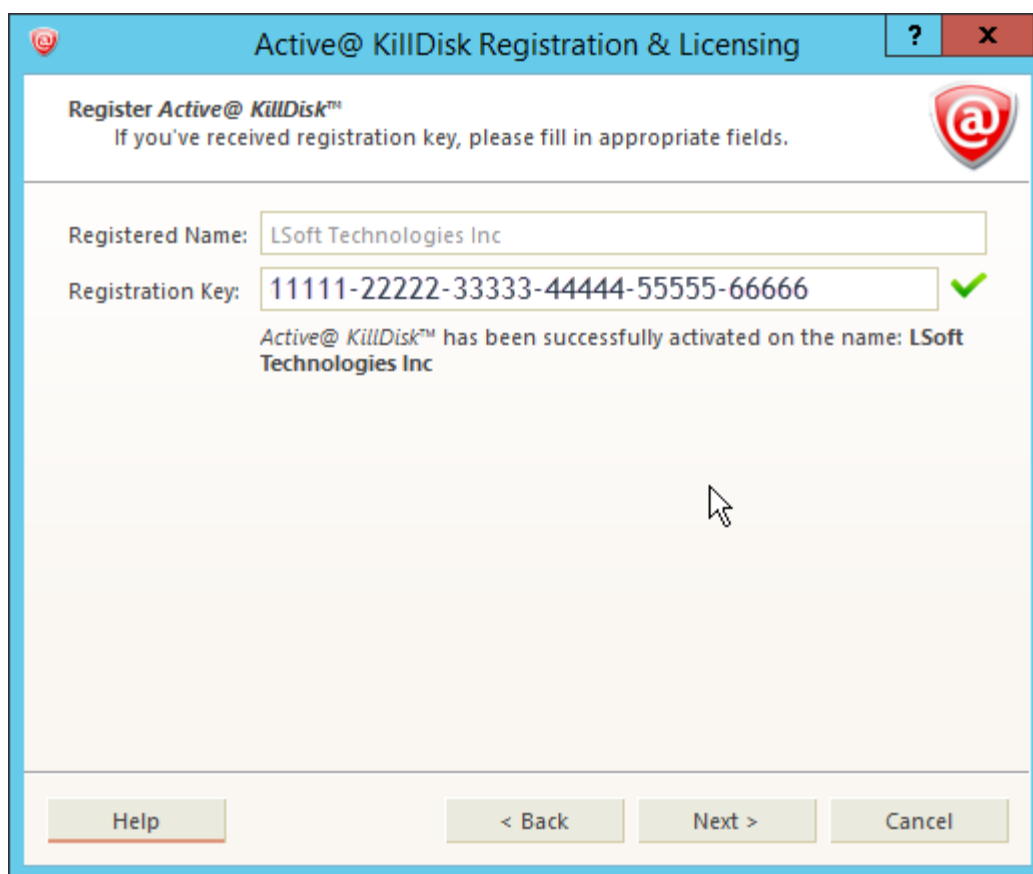


Figure 3: Completed registration

You now have access to the full features of the application.



Note: If your registration key is too long, you are using the key for an earlier version. Ensure you update to the latest version by making sure your support and updates are active and use the key to this latest version. This can be done through your client profile.



Note: You can also load registration information from a text file, (either INI or TXT type) where the first line is the name and second line is the key.

Registering the Software (Offline)

For this method of activation, you need any computer with a web browser and active internet connection and a USB. **Use this method only if the computer you are activating does not have internet access.**

In some cases, such as security or lack of access, you may not have access to an internet connection on the machine you wish to install the software on. For offline activation:

1. Select **Register or Upgrade Software** in the initial Registration & Licensing dialog launched on application start up, or click **Registration...** from the Help menu to access it from the application.
2. Select the **Register or Upgrade Software** radio button
3. Read the license agreement and activate the check box to agree to the terms of the license
4. Click **Next** to proceed with the registration
5. Copy & Paste your 30-digit registration key into the **Registration Key:** field. The Activation Request and Activation Response boxes will appear

Active@ KillDisk Registration & Licensing

Register Active@ KillDisk™
If you've received registration key, please fill in appropriate fields.

Registered Name: LSoft Technologies Inc

Registration Key: [blurred] ✓

Activation Request: VEWTVGAPYJ47DPT6L3R8GAWQZZ3XMGZMKE17
FJEYZWWLYEP5WXXGFYHF9W58HVP84M2Q7YFV4
55A6EOTG5UT42TCJ76FV9HK5N3Z1O1EQMM9R
AQQLP1L6J9ORA65XP5G19WTPWDL5AZV81GQX
U7NAL2MAUKOC9A6XARQHRY3Y3W8UX456NPHQ
INFEFA29PLIEF

Save...

Activation Response:

Load...

License auto-activation isn't available, network or server is down.
Email us a request file, or upload it from another PC to www.lsoft.net/act Then download and insert response above.

Help Activate < Back Next > Cancel

Figure 4: Offline activation boxes appearing

6. Click **Save...** to generate a registration request file. Copy this file to a USB.
7. Bring the USB to a computer with an active internet connection
8. Open the web browser and navigate to lsoft.net/act
9. Import the request file using the **Choose File** button and click **Load**
10. Click **Process!** to generate the Activation Response
11. Save the response to your USB by clicking **Save to *.licenseActivated**

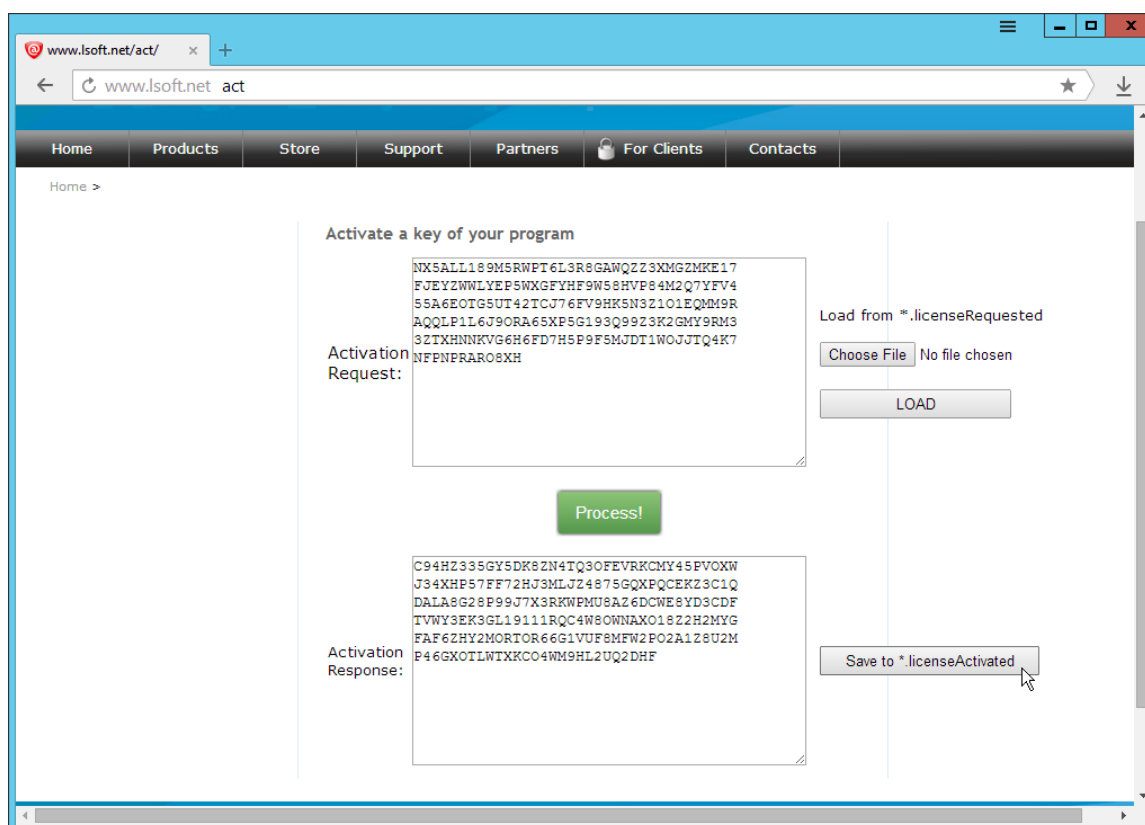


Figure 5: Generating an offline activation

12. Bring the USB to the machine with KillDisk installed
13. Import the activation response in the registration window and click **Activate**

You have now activated the software on your offline machine.

Deactivating a Registration

To transfer licenses from one machine to another, you will need to free up your activation on the licensed machine. You may do this by deactivating the registration from within the KillDisk application:

1. Click **Help > Remove License** in the file menu bar
2. Click **Deactivate Registration** in the pop-up licensing window

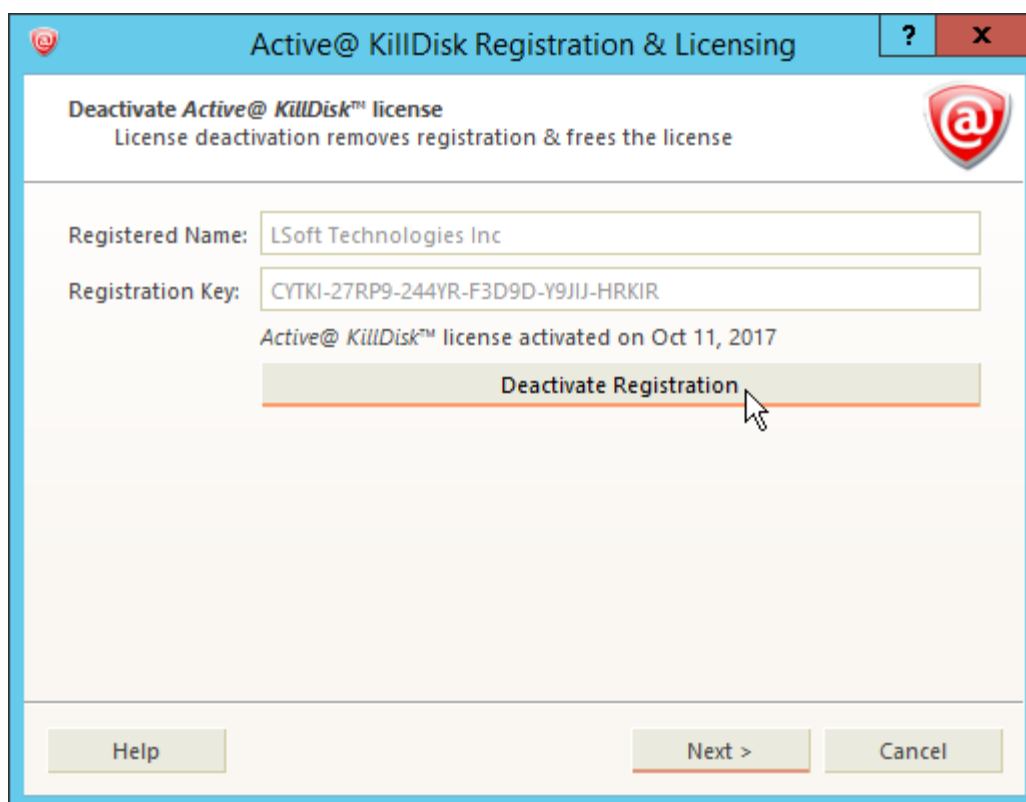


Figure 6: Deactivating a registration

Your active license is now revoked from your machine and may be used to activate a different computer.



Note: Uninstalling the application from the computer using the uninstaller will also deactivate your license from the machine, provided the machine has an active internet connection

Software Updates

KillDisk has a built-in update client to ensure you always have access to the latest version of the application. To update, use the file menu bar to navigate to **Help > Check for Updates**

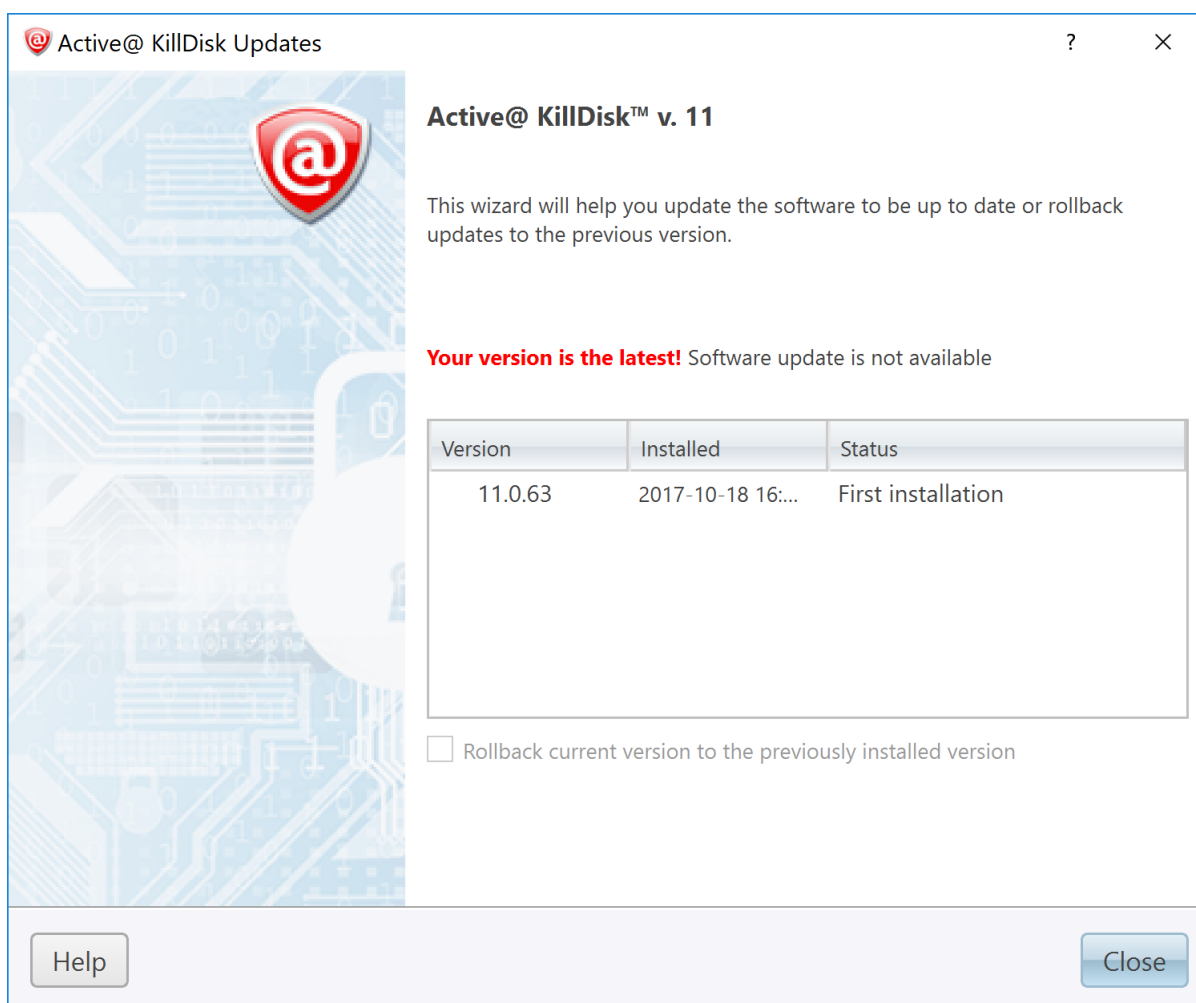


Figure 7: Checking for updates



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

System requirements

KillDisk Industrial is design to run on Linux and Windows operating systems with the following minimum requirements:

Workstation:

- IBM PC compatible machine
- Intel Pentium or higher
- 2 Gb of RAM
- 86Mb of disk space

Video:

- VGA (800x600) resolution or better

Operating System:

- Windows XP or higher

- Linux Kernel 2.x or higher

Drive Storage:

- Hard disk types supported:
 - IDE
 - ATA
 - SSD
 - SATA
 - eSATA
 - SCSI
- Removable media (memory stick, SD card, compact flash, floppy disk)
- KillDisk Industrial supports all drives seen by the Operating System with read/write access

KillDisk 11 is design to run on Linux and Windows operating systems with the following minimum requirements:

Workstation:

- IBM PC compatible machine
- Intel Pentium or higher
- 512 Mb of RAM (Windows), 1 Gb of RAM (Linux)
- 86Mb of disk space

Video:

- VGA (800x600) resolution or better

Operating System:

- Windows XP or higher (Windows version)
- Linux Kernel 2.x or higher (Linux version)

Drive Storage:

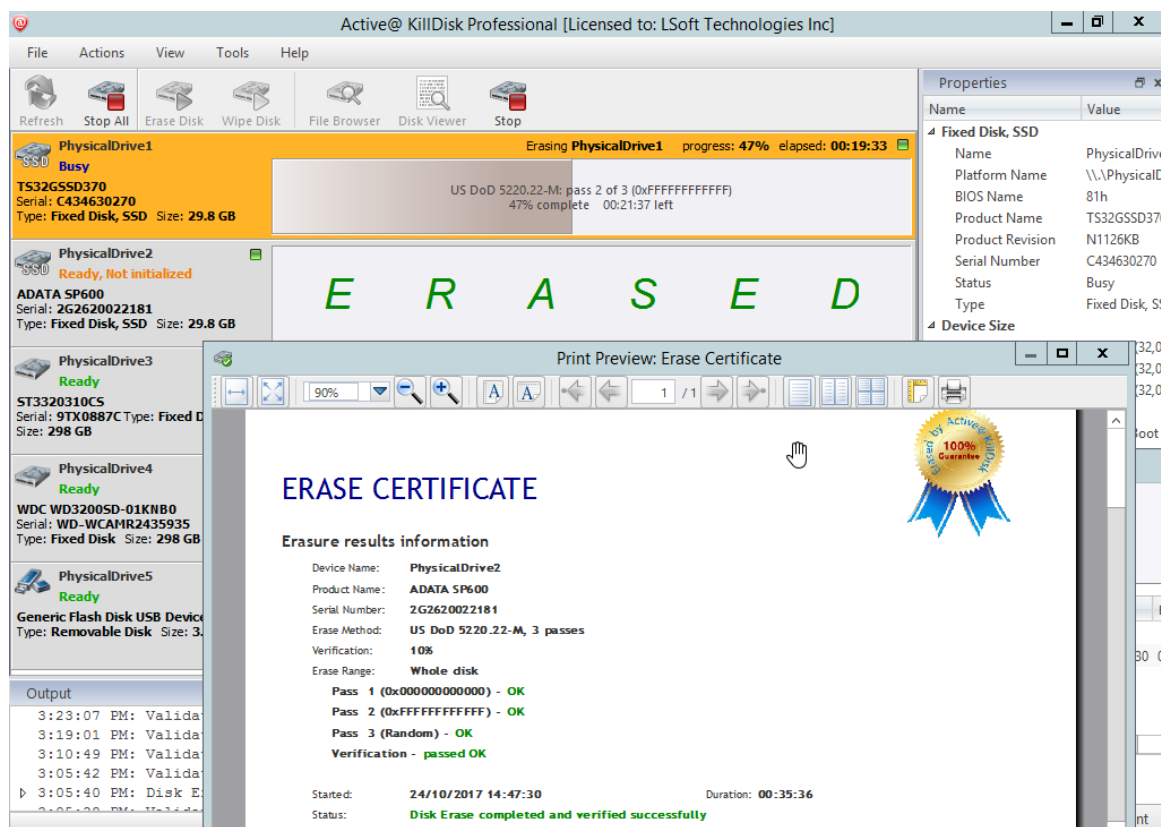
- CD/DVD-ROM or Blu-Ray optical drive (for applicable boot disk features)
- USB 2.0 or 3.0 storage device (for applicable boot disk features)
- Hard disk types supported:
 - IDE
 - ATA
 - SSD
 - SATA
 - eSATA
 - SCSI
 - Removable media (memory stick, SD card, compact flash, floppy disk)
- KillDisk 11 supports all drives seen by the Operating System with read/write access, additional drivers can be loaded onto the boot disk for drivers not included by default in the bootable environment

Security hardware

KillDisk authorization provided by external or internal removable USB key with license and user information. This USB key must be inserted all the times to make KillDisk software operable.

Getting Started with KillDisk

This section outlines the essential features of KillDisk and explains basic functionality to get you started.



KillDisk Installation and Distribution

KillDisk Industrial distribution overview

KillDisk Industrial is distributed as a software solution, with a DVD-ROM and security USB license. Simply install the application into your data erasure workstation environment and [configure it to your system](#).

KillDisk 11 distribution overview

After purchasing Active@ KillDisk license, you will be emailed a registration key and an installation file named KILLDISK-<VERSION>-SETUP.EXE. This file contains everything you need to get started - double click on the file and the installation wizard will take you through the setup process.

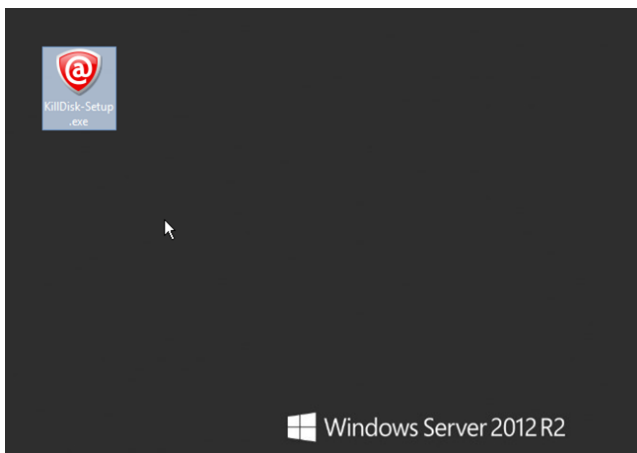


Figure 8: Installation file



Note: If you purchased the Ultimate version, you will receive the Windows executable file. To access the Linux installation files, install it on your Windows machine and navigate to the root directory of the application where you will find the Linux installation files. The path to the linux application will look something like: C:\Program Files\LSoft Technologies\Active@ KillDisk Ultimate 11\Linux\KillDisk_Linux_Installer.tar.gz

After installation, Active@ KillDisk still starts as FREE version (unregistered), you need to register it first to have all professional features activated.

Windows or Ultimate versions:

To install the application, double-click KILLDISK-SETUP.EXE and follow the instructions in the installation wizard.

The installed application contains two main applications:

- Active@ KillDisk for Windows (KillDisk.exe) — Run this application from your Windows operating system to inspect local disks and erase/wipe your data. KillDisk.exe contains both the 32-bit and 64-bit applications.
- Active@ Boot Disk Creator (BootDiskCreator.exe) — Create a bootable Windows PE CD/DVD/BD or USB disk to boot from it and run Active@ KillDisk for Windows. Using Active@ KillDisk this way allows you to wipe confidential data from the system volumes while gaining exclusive use of a partition because the operating system runs outside the partition that you are securing.

Linux versions:

To setup the application, make sure you found the Linux file, as mentioned in the note above. Double-click **KillDisk_Linux_Installer.tar.gz** in your Linux environment and unpack the archive to a proper location. To install, simply run the following command in the directory where the archive was unpacked:

```
sudo ./KillDisk_Linux_Installer.run
```

Active@ Boot Disk Creator

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.

To prepare a bootable device:

1. Run **Bootable Disk Creator** from the Windows Start menu (Windows platform). The Active@ Boot Disk Creator setup wizard will appear.

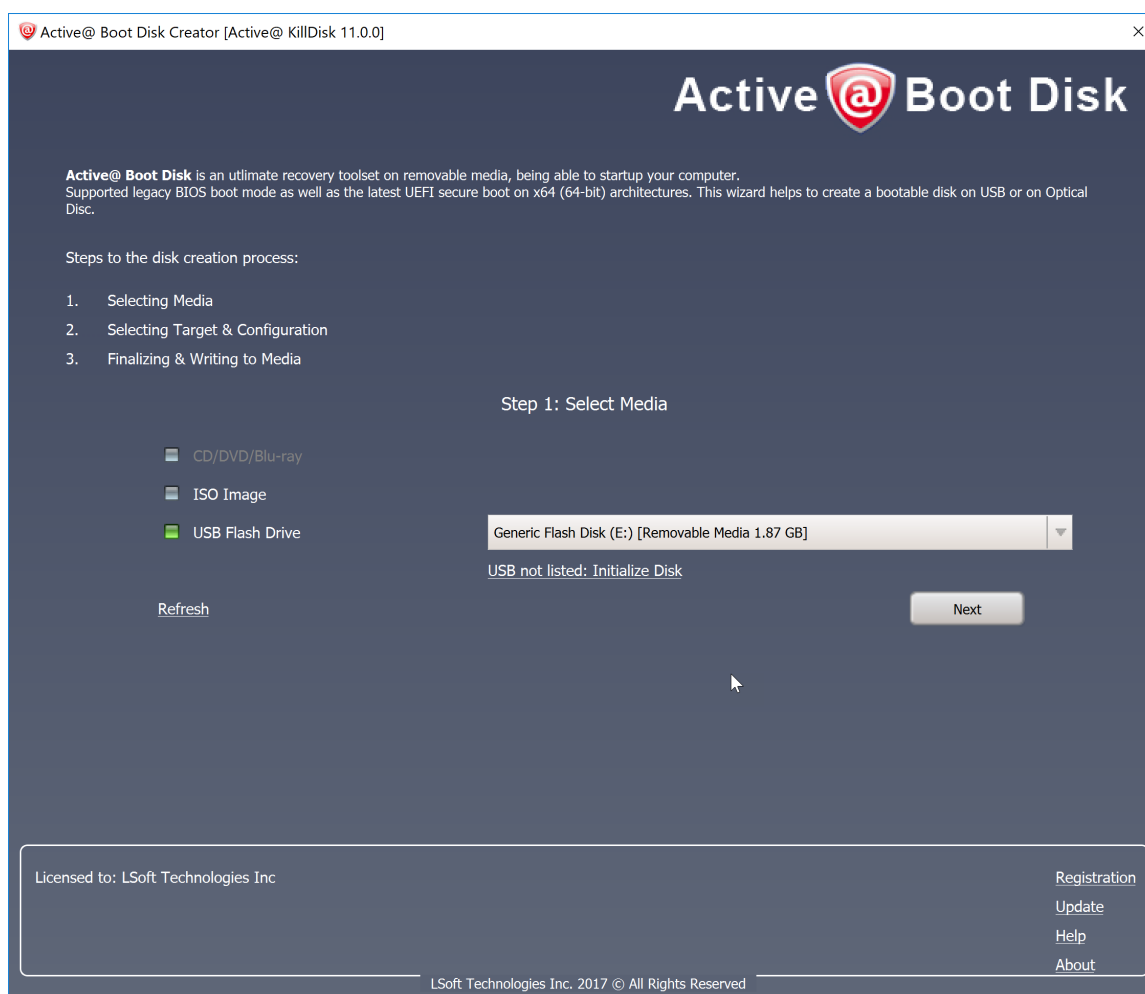


Figure 9: Boot disk creator applet

2. If Active@ KillDisk has not been registered yet, you need to register software first by clicking **Register** in the bottom-right corner and [Registering the Software](#)
3. In the Active@ Boot Disk Creator main page, select the desired bootable media: a **CD/DVD/Blu-ray**, a **USB Flash Drive** or an **ISO Image file** to be burned later. If several media drives are inserted, click the ellipsis button (...) and choose a particular device. Click **Next**.


 **Note:** If your bootable media device does not appear in the drop-down list, click **Initialize Disk**. You should be able to find the device in the setup menu and initialize it to be compatible with the application. This process **will** erase all data on the selected device.
4. Select the target platform for booting up. Depending on Active@ KillDisk version you purchased, one or more target platforms will be available for selection (Windows, Linux GUI or Console).



Figure 10: Creating a Linux boot disk

5. At this step you can specify additional boot disk options:
 - a) To customize boot options, click the **System Boot Settings** tab. You can change the default settings to be used: Time Zone, Additional Language Support, Default Application Start and Auto-Start Delay. You can also change these options in the Active@ Boot Disk initialization screen while booting (Windows version). Additional Network and Security sub-tabs allow to configure static IP & Firewall settings, as well as to protect your Boot Disk with a password at boot time.
 - b) To add your custom files to the bootable media, click the **User's Files** tab. Add files or folders using the related buttons at the right side. Added items will be placed in the User_Files root folder
 - c) To add specific drivers to be loaded automatically, click the **Add Drivers** tab. Add all files for the particular driver (*.INF, *.SYS, ...). Added items will be placed in the BootDisk_Drivers root folder. At boot time all *.INF files located in this folder will be installed.
 - d) To add specific scripts to be launched after Active@ Boot Disk is loaded, click the **Add Scripts** tab. Add your scripts (*.CMD files). Added files will be placed in the BootDisk_Scripts root folder. At boot time all *.CMD files located in this folder will be executed.
 - e) To add command line parameters for KillDisk startup after the boot, click **Application Startup** tab and type desired parameters. This tab is available only if Default Application Start option is turned ON on the **System Boot Settings** tab
6. Click **Next**. Verify the selected media, sizes and boot up environment.
7. Click **Create**. A progress bar appears while the media is being prepared.



Note: Not all additional boot disk options are accessible for all platforms. For example, Add Drivers section applies only to Windows Operating System, and is available for Windows target only.



Note: A USB Drive or blank CD/DVD/BD must be inserted and explicitly chosen on the first step before you can proceed further.



Note: If you've created an ISO Image file, you can burn it to a disk later on using either our free Active@ ISO Burner utility (www.ntfs.com/isoburning.htm) or a utility of your choice.

Launching and initial configuration

Upon launching the application you will see the Welcome dialogue, shown here:

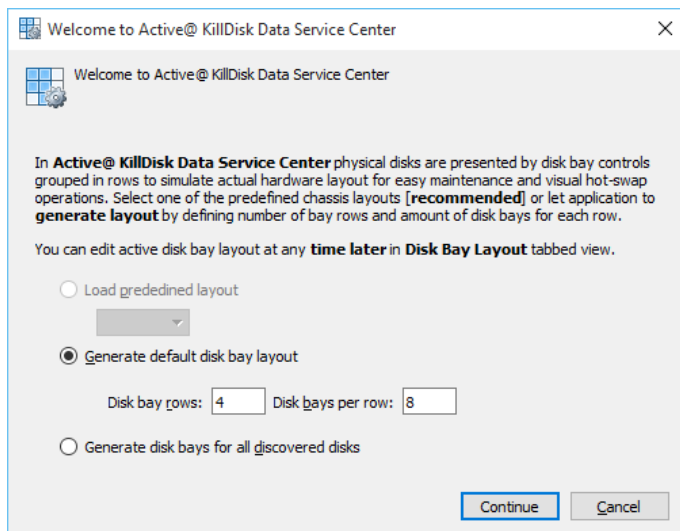


Figure 11: KillDisk Data Service Center Welcome dialogue

This menu allows you to initialize KillDisk to display your hardware in an intuitive way. To illustrate the purpose of this, read this section on [Disk Bay Layouts](#). This initial configuration can be done in one of three ways:

Load predefined layout

Here you can find one of our predefined layouts that may fit your system. If an appropriate layout is not listed, you may try the next option.

Generate layout by definition

Define your systems in terms of a disk array, arranged in a X by Y grid of disks. You may make adjustments to this later, so this may just be a base to start from.

Generate layout automatically

Defines your Disk bay layout based on the disks recognized by your system's device manager. The disks will be placed in their own individual row when the layout is generated.

Navigating through the Application

Once the KillDisk application is launched, you will be presented with the main KillDisk application dashboard. From here you can use any of KillDisk's tools with your system. This section will outline the main components of the application. The full functionality and features of these components are discussed in their corresponding sections later in this documentation:

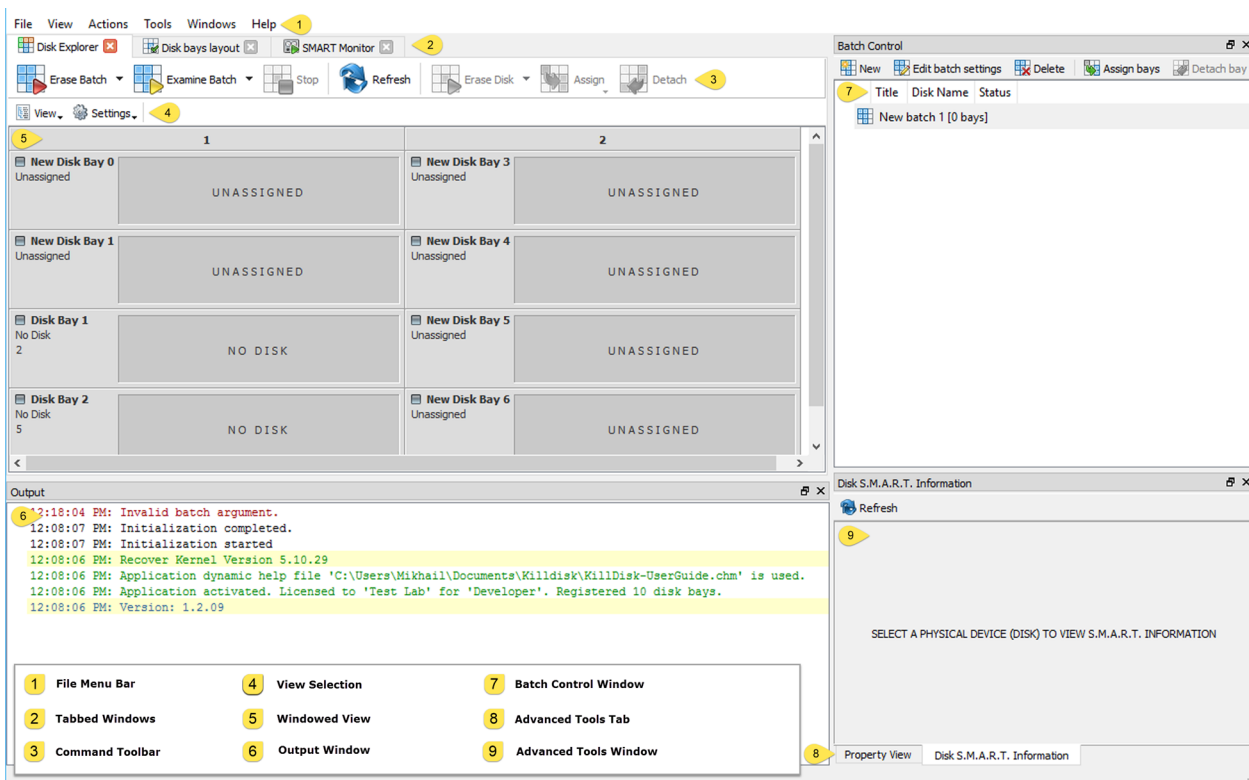


Figure 12: KillDisk application dashboard

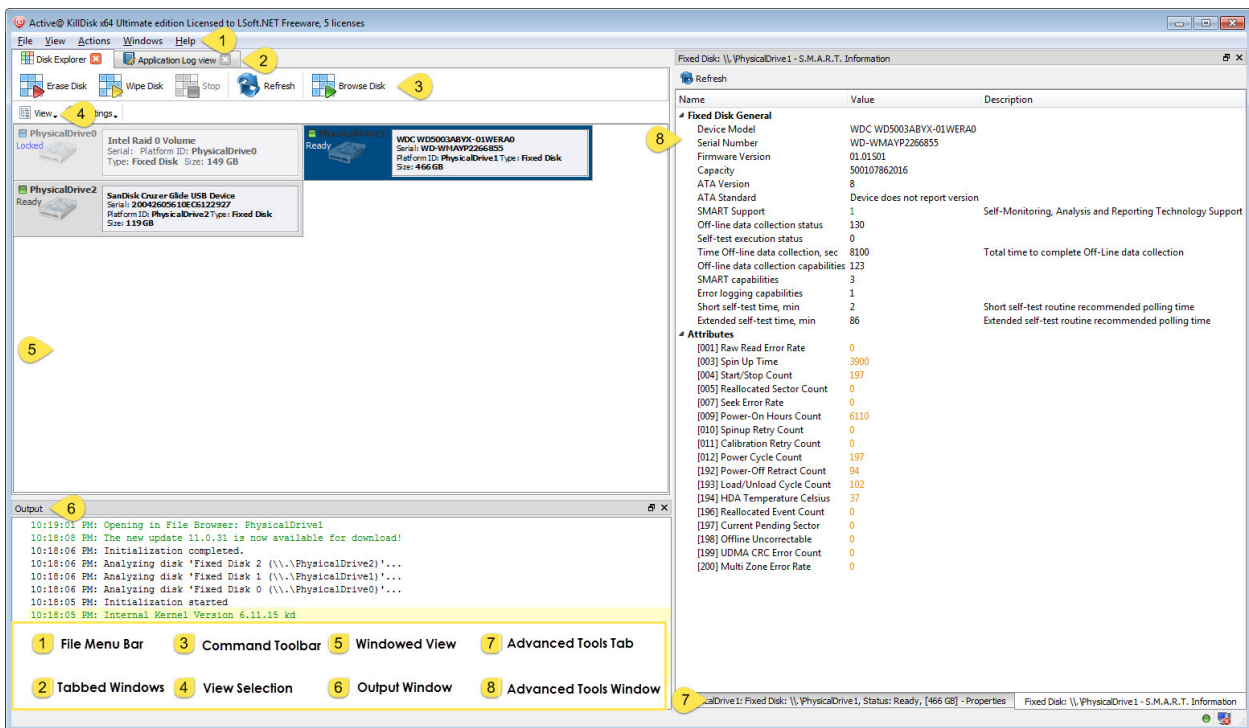


Figure 13: KillDisk application dashboard

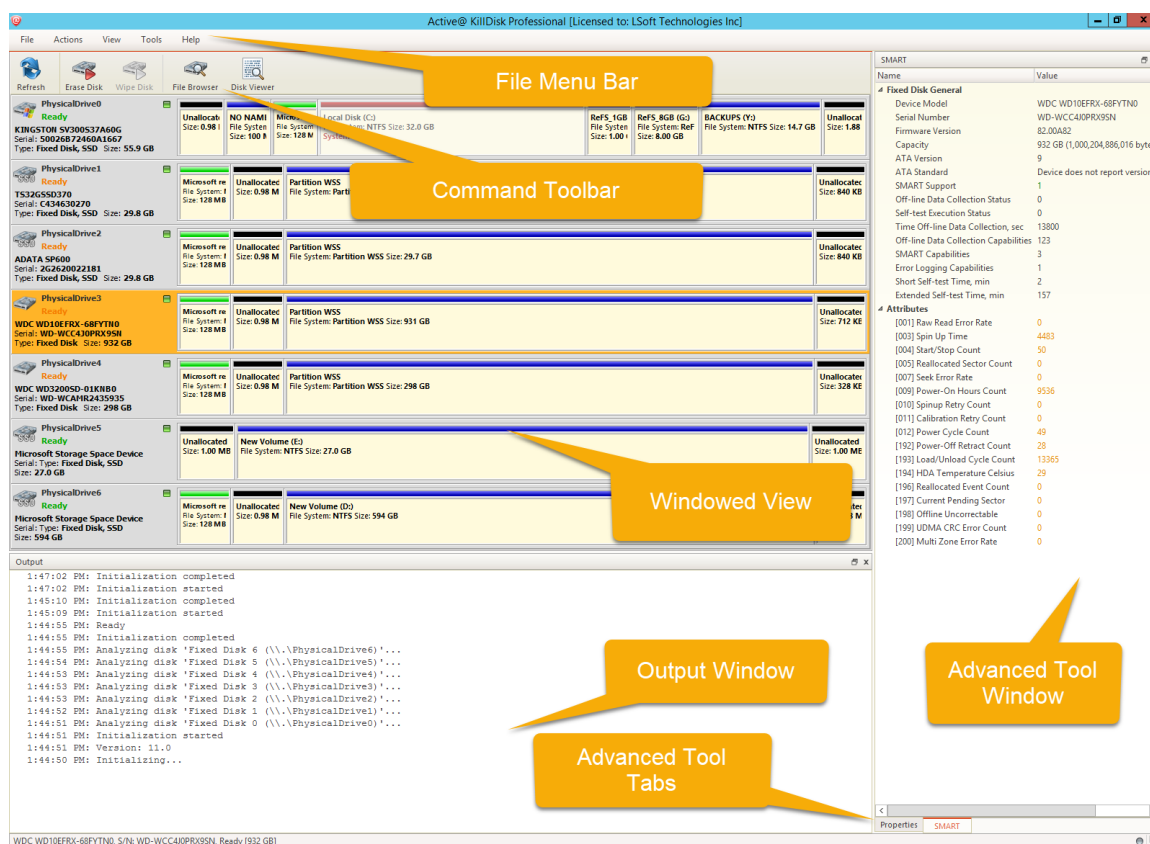


Figure 14: Navigating the KillDisk application

File menu bar

The file menu bar contains can be manipulated to perform nearly any operation in KillDisk, such as accessing elements of the program such a settings and help, changing views and what is visible in the dashboard, opening tools, and navigating between KillDisk's windows.

Tabbed Windows

Here, you may move between KillDisk tabbed windows, the main windows being *Disk Explorer*, *Application Log* etc..

Command Toolbar

The command toolbar is a dynamic toolbar that allows the user to perform Tabbed Window-specific actions, depending on what window the user is in and what element is selected.

View Selection

Only available in the Disk Explorer View, this View Selection allows you to manipulate how the bays are displayed in the Windowed view, manipulating the type of graphics used to show the bays and the cardinality of the bays in the Disk Bay View.

Windowed view

Contains the window that is currently open.

Output window

Contains the log of operations KillDisk has performed.

Batch control window

The Batch control window is an easily accessible interface to create, delete and manipulate disk batches.

Advanced tool tabs

These tabs allow for navigation between the different advanced tool windows.

Advanced tool window

This window shows the data for the Advanced tool selected. The window can be moved, popped out and re-sized. To browse through each of these views, click on the appropriate tab. You may also open a view from the **View** menu. To close the current view at any time, press **CTRL+F4**. To open any closed view, select it from the **View** menu. The status bar, at the bottom of the workspace shows the current status of the application or status of the activity in progress.

Disk Bay Layout Overview

The purpose of Disk Bay Layouts is to match KillDisk's graphical representation of your disk configuration to your physical hardware configuration, making it easy to manage your disks for Erasure, Examination, Cloning and more. To illustrate this, let's look at an example, using the hardware below:



Figure 15: Example of a generic disk array

In the above example, we have a generic disk array consisting of 16 disks, arranged in a 4x4 grid. The machine using these disks would see the disks similarly to KillDisk's Local Disks view, as depicted in the Figure below:

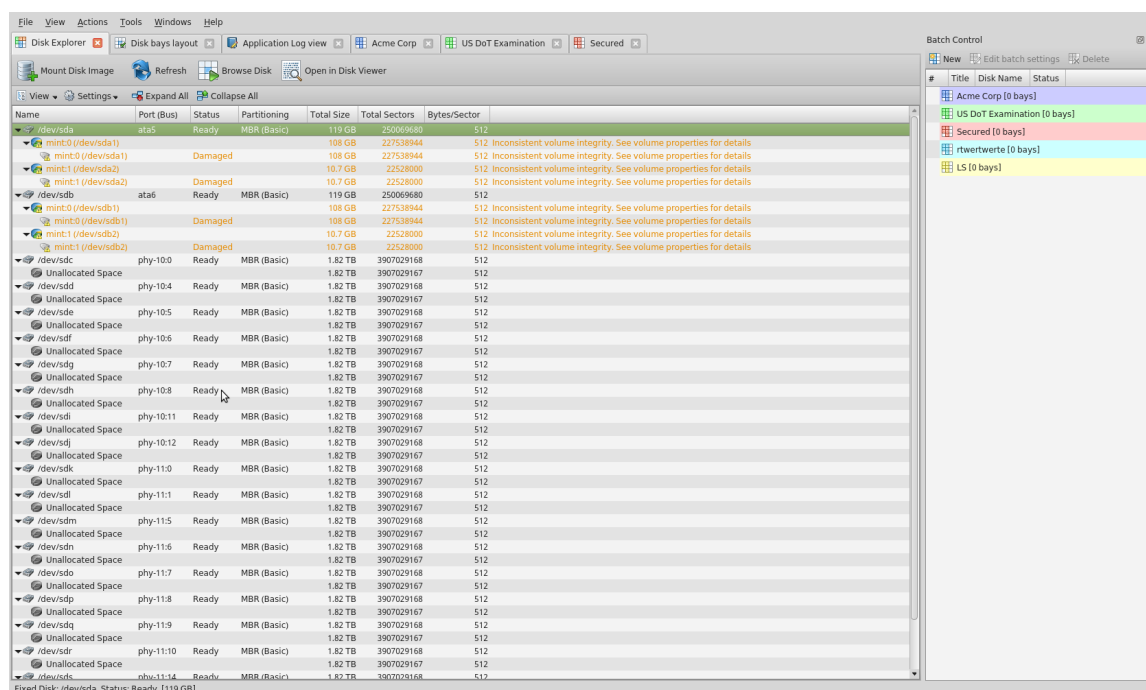


Figure 16: Local Disks view in KillDisk

Now imagine inserting a Hard Drive into the bottom-leftmost bay of the disk array and wanting to perform an operation on it. Even finding the device in a list of 15 other disks would be tedious and not very intuitive. This is

where creating a Disk Bay Layout is extremely useful. By creating a 4x4 Disk Bay Layout, we can map the physical ports to their corresponding Bay in KillDisk and visually see our disk array like this:

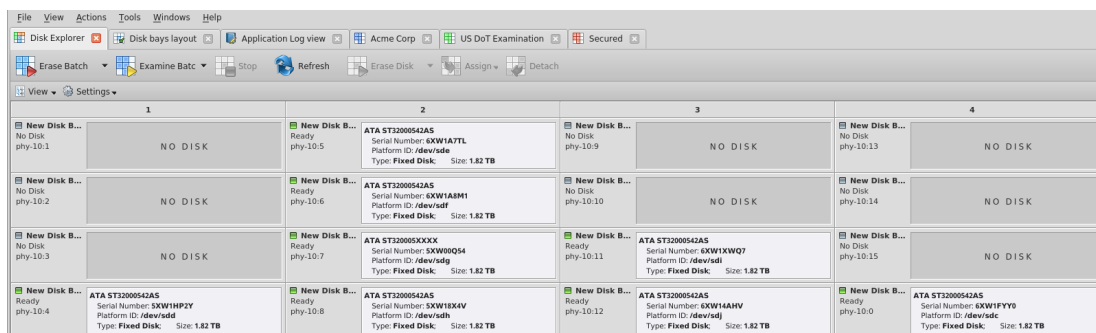


Figure 17: KillDisk's "Disk Bays" view

Assuming that the bays were mapped correctly, finding the correct disk to manipulate now much easier in the "Disk Bays" view than it would have been in a list view. You can now select the bottom-leftmost disk in the Disk Bays view and perform any necessary actions on it.

Create a new Disk bay layout

In the KillDisk toolbar, select **Tools > Disk layout editor**, or shortcut **CTRL + M**.

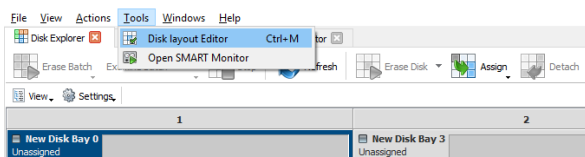


Figure 18: Opening the Disk bays layout tab

This will bring you to the Disk bays layout tab, where you can manipulate, save, import and create Disk Bay Layouts.

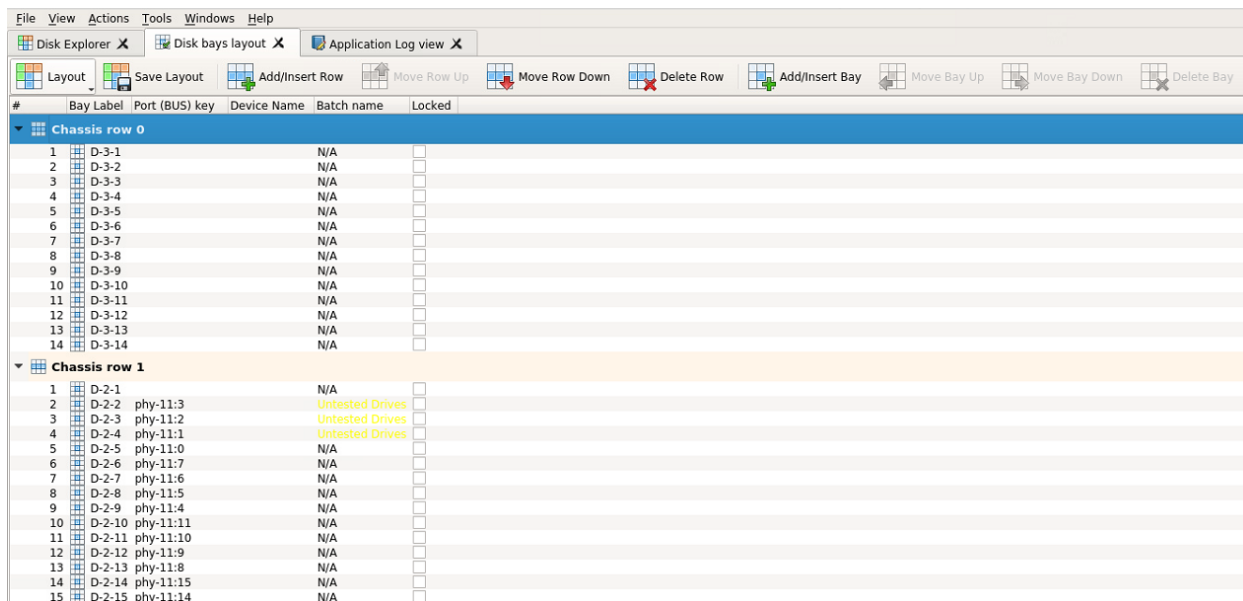


Figure 19: Opening the Disk bays layout tab

Here we are looking to create a new layout, so get rid of the current layout shown by clicking **Layout > New Layout**.

Warning: Make sure to save the old layout by selecting **Layout > Save layout as..** before creating the new layout, or your old layout WILL be lost.

Use the **Save Layout** button to commit any changes to the layout to the application views.

Note: **Save Layout** will apply current change to the KillDisk session so the changes will be seen in the Disk bay explorer views and even be loaded in upon future application launch. These changes will not affect the .dbl file, however, so be sure to commit any important changes using the **Save Layout as... command**.

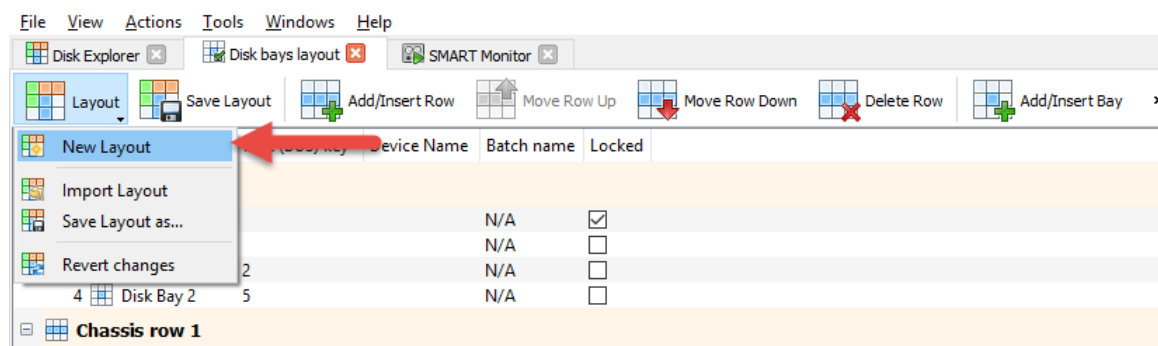


Figure 20: Creating a new layout

With the old layout cleared out, you now have a new layout ready to be configured to your machine.

Adding and Deleting Rows and/or Bays

Disk bay layout consist of disk bays grouped by row to maximize mocking effect of an actual disk bay mounted in hardware unit. To design bay layout, simply use the **Add Row** or **Add Bay** buttons to create additional rows/bays to work with. When a bay is selected, the **Delete Bay** button can be used to delete the individual bay. When a row is selected, the **Delete Row** button will delete the row and all the bays contained within it.

Map disk bays to physical drives

In Disk bay layout you can map actual physical bay to its GUI representation (disk bay widgets) in two ways:

- Assign *platform name* to disk bay widget;
- Assign *disk port* of physical disk controller to disk bay widget

Important: Due to different hard disk controller manufacture standards and platform limitations, physical disk port address format may vary.

Note: If both, platform name and disk port, are assigned to disk bay widget then platform name is used for disk bay mapping.

To make an assignment, double click in either Platform Name or **Port (BUS) key** column in correspondent disk bay line to initiate editing. Enter platform name as text or disk port as masked text. You can use drop down list of all detected physical disk controller ports for immediate port assignment.

You can also edit disk port in disk bay widget from *main view* by using context menu of disk bay widget.

Save and Import Disk bay layout

Once a disk bay layout is configured, it can be saved and later used with other KillDisk configurations. This is done with the Save and Import features.

Saving a Disk bay layout

Layouts are saved using the disk bay layout command tool bar's commands. Select Layout, then **Save Layout as...** in the drop down list of commands. This will open a dialogue where the layout can be configured by setting the Title,

description, file name and path to save the layout to. Once these settings are configured, click **Save** and the layout will be saved as a .dbl file in the specified location.

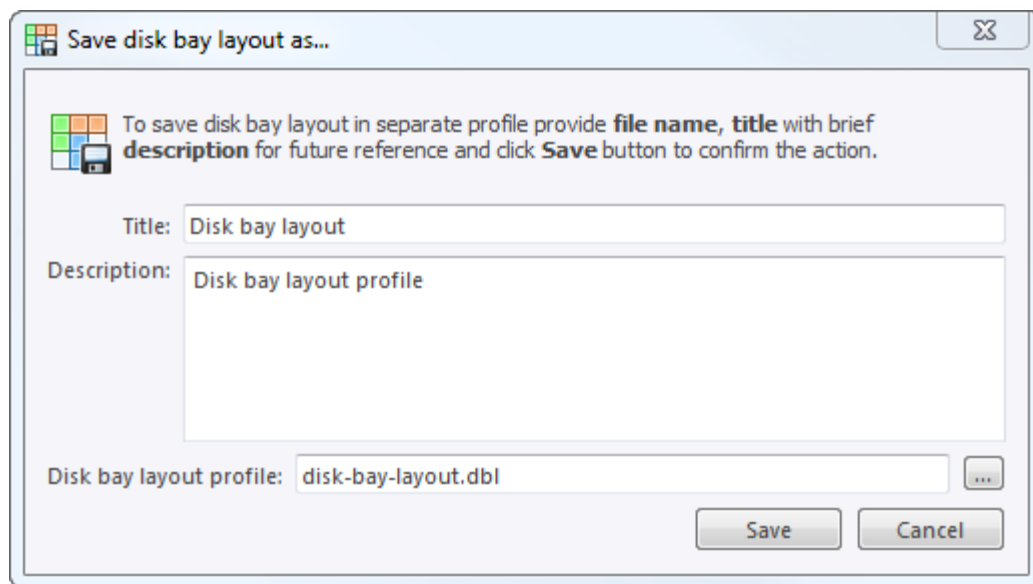


Figure 21: Export disk bay layout dialog

Title

Enter any label to distinguish newly created disk bay layout to differentiate it among other disk bay layouts.

Description

Describe any specifications, features or particularities of the new disk bay layout.

Layout profile name

Select the name of the file that the disk bay layout will be saved as. Extension should remain as '.dbl'.

Import disk bay layout from file

Saved disk bay layouts are imported into separate KillDisk sessions using the import feature. In the command tool bar, select Layout and Import Layout. Select the desired disk bay layout in the file explorer window and click **Open**. This will import the disk bay layout into the current KillDisk session. Finally, click **Save layout** to update the disks in the Disk Explorer and the import should be complete.

Formatting disk bay layout

Once a disk bay layout is created, there are a number of actions that can be performed to format or manipulate the layout and appearance of the disks in the KillDisk application.

Naming Disk Bays

To make disk bay widgets easier to navigate, they can be renamed by simply double-clicking on the existing bay label and typing in a new name, shown in the Figure below:

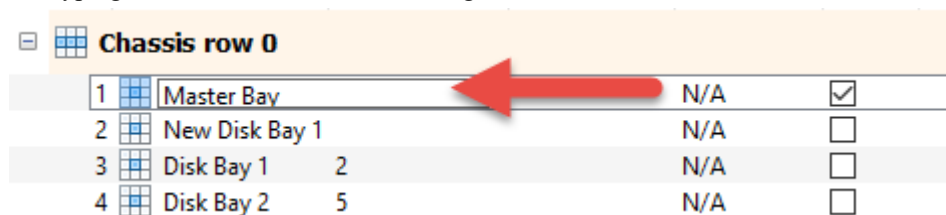


Figure 22: Renaming bays

Changing Row and Bay positioning

Configured bay widgets may be moved around to accommodate changes in physical configuration or fix mistakes in creating the layout. This is done quite simply by selecting the bay that needs to be moved, and clicking the **Move Bay Up** and **Move Bay Down** buttons. Similarly, bay rows can be manipulated by selecting the row in question and pressing the **Move Row Up** and **Move Row Down** buttons.

Advanced features

Once a disk bay layout is created, there are a number of actions that can be performed to format or manipulate the layout and appearance of the disks in the KillDisk application.

Locking Disks

In order to prevent accidental deletion of important disks, KillDisk supports locking of disks. Once a disk is locked, no write operations are allowed to be performed on the drive. To do this, simply find the disk that needs to be locked and enable the corresponding check box in the Locked column of the Disk bay layout view.

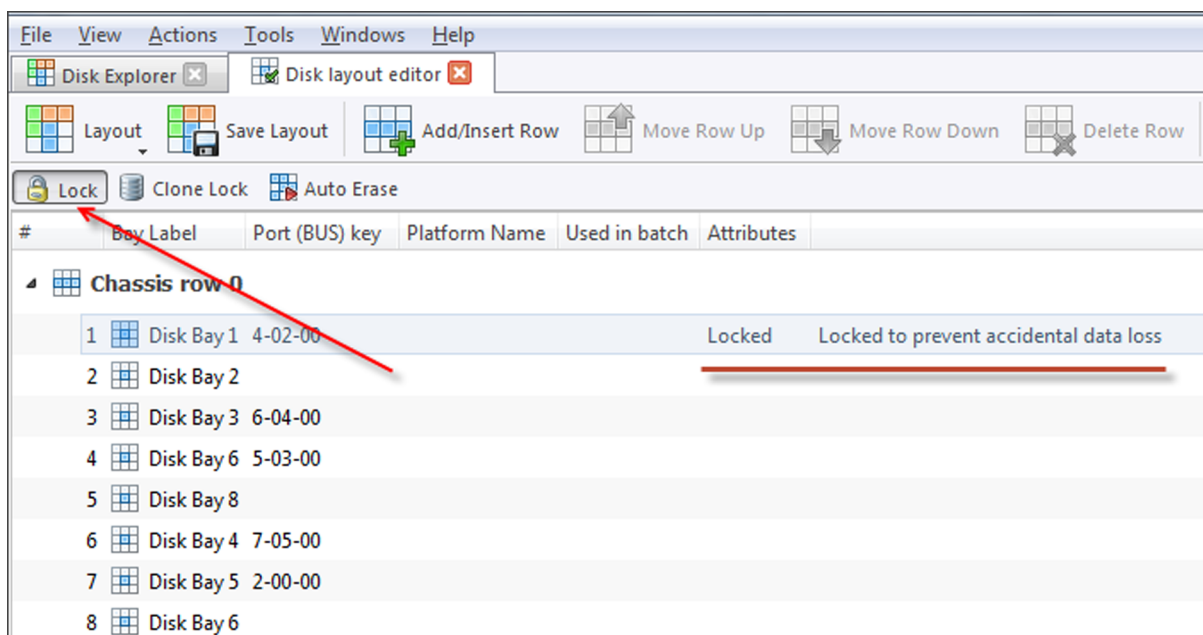


Figure 23: Locking a disk to prevent accidental destruction

Locking clone source

Disks that are planned to be used as master copy for [Disk cloning](#) on page 63 could be marked in disk bay layout by selecting disk bay and clicking **Clone Lock** in toolbar. Thus disks marked this way will be protected from accidental destruction and also will be available in list devices as source for disk cloning.

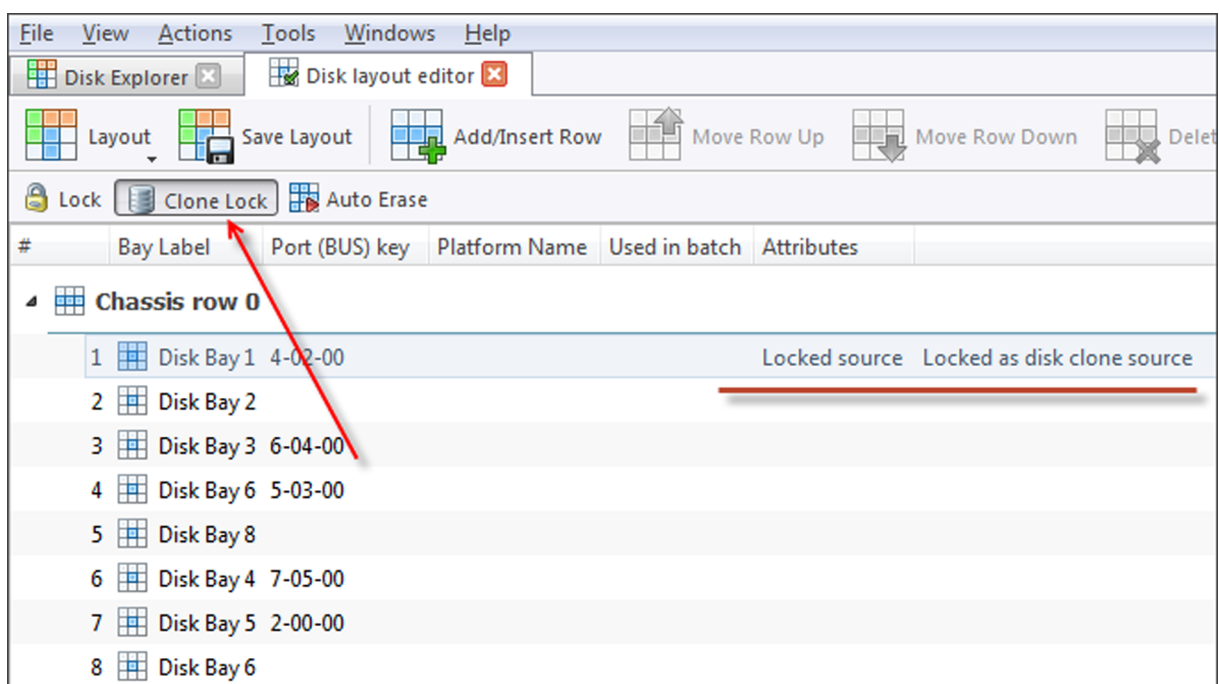


Figure 24: Locking a disk as clone source

Auto erase

Auto Erase feature designed to speed up disk wiping process in scenario when many disks must be erased with the same erase attributes with less user interaction. When disk is inserted in a bay marked as auto Erase then disk erase procedure will start without any introduction or confirmation dialogs. However you will see 30 seconds countdown started on disk bay about to be erased and may cancel this action by selecting disk bay widget and clicking **Stop** button in view's toolbar or in context menu.

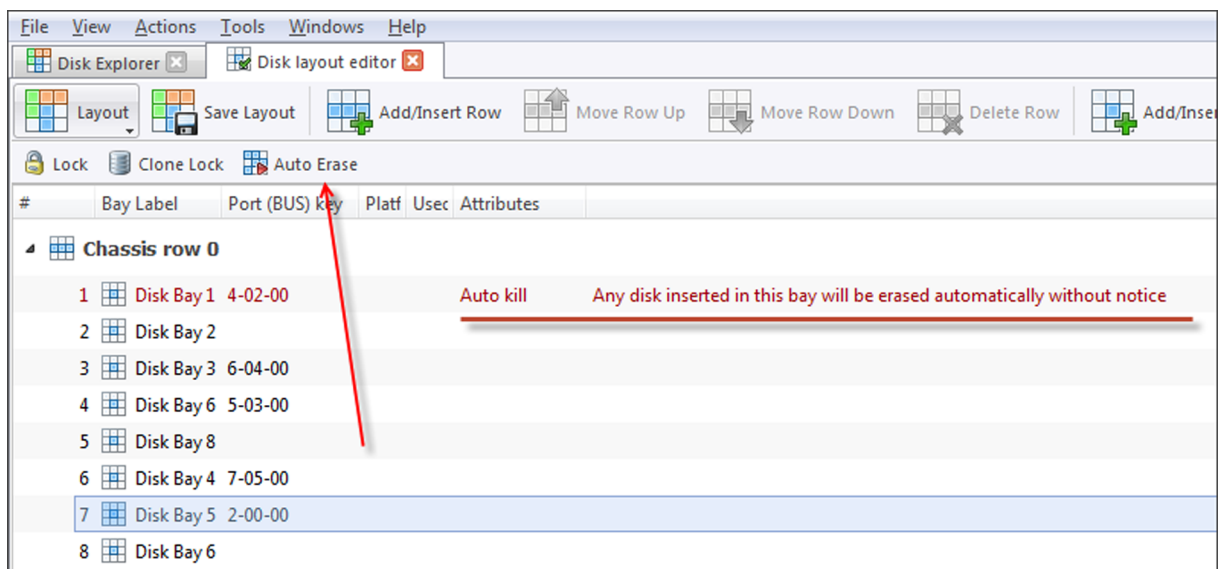


Figure 25: Locking a disk



Caution: Use this feature with extreme caution — be sure that inserted disk is intended to be erased and appeared in a right bay. You will have 30 seconds to abort disk erasure.

Disk Explorer View

The **Disk Explorer view** is the main interface for the KillDisk application. Here, disks are visualized, can be selected and manipulated. The status of any procedures performed on the disks can be seen here, new procedures like erasure can be initiated.

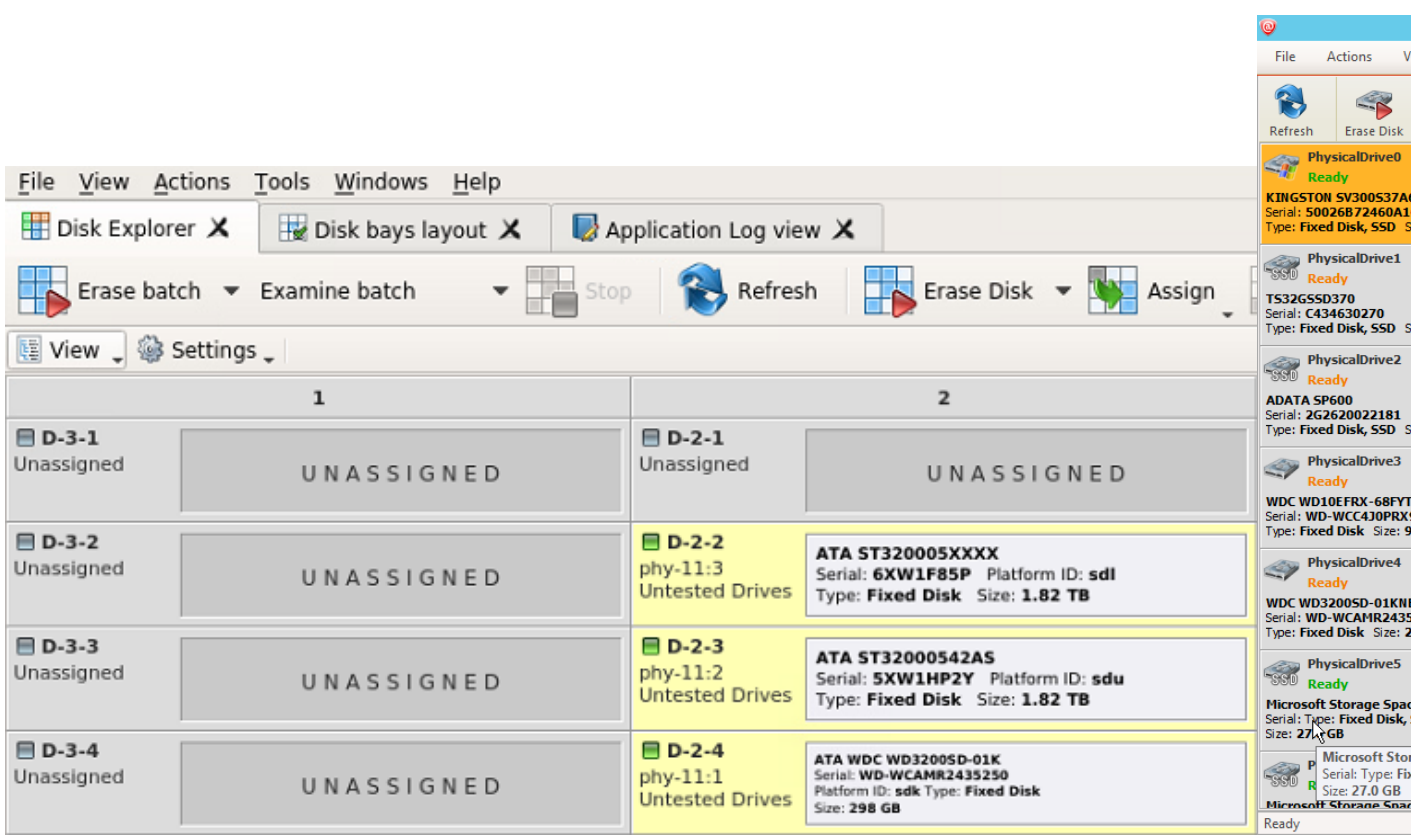


Figure 26: Disk explorer view

View

The disk explorer supports a range of different views to use when performing KillDisk's actions, each with their own customizable settings for different use cases.

Settings

View settings will let you customize appearance for better experience and specific for each view.

Disk Bays view

This view visually displays the disks configured in the disk bay layout. The bays are grouped by their row, colored by the batch color, and show the current status of the disk. If any operations are being performed on the disk, the operation and progress are displayed.

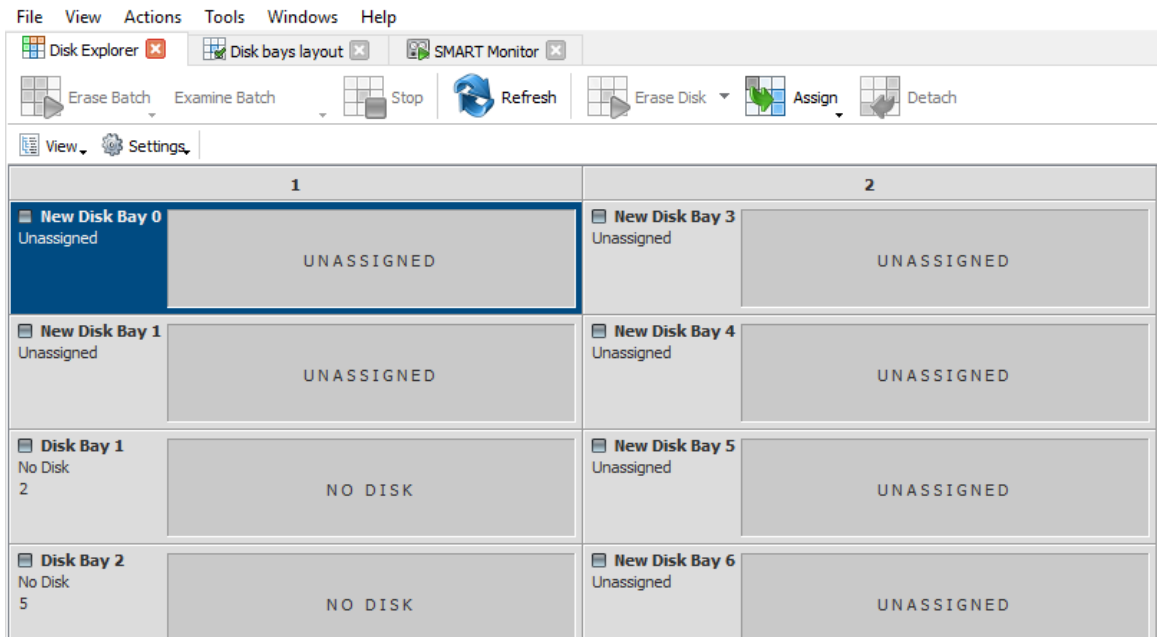


Figure 27: Disk Bays view

Settings menu

Detailed view

Toggle between detailed and simplified view of disk bay controls.

Show removable devices

Show or hide additional layout row for removable devices.

Rows as Columns

This setting can be toggled on/off to display the rows (defined by the disk bay layout) as columns in the Disk bays view.

Vertical Bays

This setting can also be toggled to change the orientation of the bays to vertical.

Disk Bays tree view

The disk bays tree view presents the disk bay layout in a standard list form, much like the disks would be shown in an explorer. Disk bays are grouped by row and colored according to their batch color. Information such as disk status, serial number, partitioning are shown in list form next to their respective disk bays.

Name	Status	Batch Name	Platform Name	Serial Number	Partitioning	First Sector	Total Sectors	Total Size
Chassis row 1								
D-3-1 [Unassigned]	Unassigned							
D-3-2 [Unassigned]	Unassigned							
D-3-3 [Unassigned]	Unassigned							
D-3-4 [Unassigned]	Unassigned							
D-3-5 [Unassigned]	Unassigned							
D-3-6 [Unassigned]	Unassigned							
D-3-7 [Unassigned]	Unassigned							
D-3-8 [Unassigned]	Unassigned							
D-3-9 [Unassigned]	Unassigned							
D-3-10 [Unassigned]	Unassigned							
D-3-11 [Unassigned]	Unassigned							
D-3-12 [Unassigned]	Unassigned							
D-3-13 [Unassigned]	Unassigned							
D-3-14 [Unassigned]	Unassigned							
Chassis row 2								
D-2-1 [Unassigned]	Unassigned							
D-2-2 [Ready]	Ready	Untested D...	/dev/sdl	6XW1F85P	MBR (Basic)	0	3907029168	1.82 TB
D-2-3 [Ready]	Ready	Untested D...	/dev/sdu	5XW1HP2Y	MBR (Basic)	0	3907029168	1.82 TB
D-2-4 [Ready]	Ready	Untested D...	/dev/sdk	WD-WCAMR2435250	MBR (Basic)	0	625142448	298 GB
D-2-5 [Unassigned]	No Disk							
D-2-6 [Ready]	Ready		/dev/sdq	6XW0E36K	MBR (Basic)	0	3907029168	1.82 TB
D-2-7 [Ready]	Ready		/dev/sdj	5XW1QP6N	MBR (Basic)	0	3907029168	1.82 TB
D-2-8 [Unassigned]	No Disk							
D-2-9 [Ready]	Ready		/dev/sdn	5XW0MF0B	MBR (Basic)	0	3907029168	1.82 TB
D-2-10 [Unassigned]	No Disk							
D-2-11 [Ready]	Ready		/dev/sdr	6XW1F3ZQ	MBR (Basic)	0	3907029168	1.82 TB
D-2-12 [Ready]	Ready		/dev/sdt	6XW15H3L	MBR (Basic)	0	3907029168	1.82 TB
D-2-13 [Ready]	Ready		/dev/sdf	5XW0KGP4	MBR (Basic)	0	3907029168	1.82 TB
D-2-14 [Ready]	Ready		/dev/sde	6XW1A7TL	MBR (Basic)	0	3907029168	1.82 TB
D-2-15 [Ready]	Ready		/dev/sdd	6XW14AHV	MBR (Basic)	0	3907029168	1.82 TB
Chassis row 3								
D-1-1 [Unassigned]	No Disk							
D-1-2 [Unassigned]	No Disk							
D-1-3 [Unassigned]	No Disk							
D-1-4 [Unassigned]	No Disk							
D-1-5 [Unassigned]	No Disk							
D-1-6 [Unassigned]	No Disk							

Figure 28: Disk Bays Tree view

Settings menu

Show inserted devices

Displays all devices that are detected by the system device manager.

Show partitions

Displays all partitions on the disks.

Show live volumes

Displays live volumes detected.

Group by chassis rows

Displays the groupings of the disk bays by rows, as defined in the disk bays layout.

Show unplugged bays

Displays bays that are not connected to a disk.

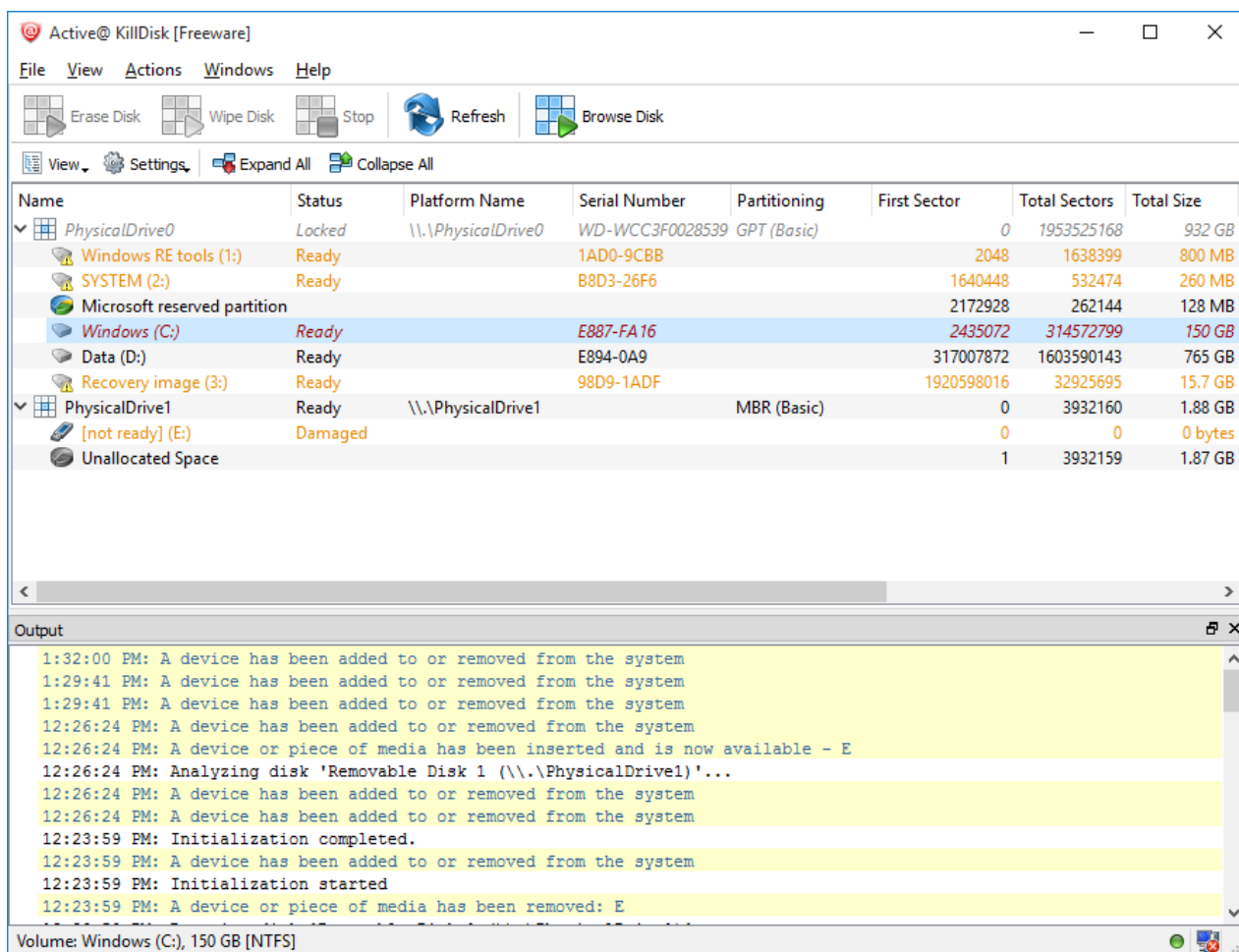


Figure 29: Disk Bays Tree view

Settings menu

Show unallocated

Displays all devices that are detected by the system device manager.

Show volumes

Displays volumes detected.

Show not ready

Displays the groupings of the disk bays by rows, as defined in the disk bays layout.

Local Disks tree view

Local Disks view shows all disks recognized by the system and available for application in hierarchical tree view:

Name	Port (Bus)	Status	Partitioning	Total Size	Total Sectors	Bytes/Sector
/dev/sdb	2	Ready	MBR (Basic)	1.82 TB	3907029168	512
Unallocated Space						
/dev/sdc	3	Ready	MBR (Basic)	149 GB	312581808	512
Unallocated Space						
/dev/sde	5	Ready	MBR (Basic)	932 GB	1953525168	512
Unallocated Space						
/dev/sdy		Ready	MBR (Basic)	1.79 GB	3751936	512
ACTIVE BOOT				1.91 GB	4015885	512
ACTIVE BOOT		Ready		1.91 GB	4015880	512
/dev/sdaa		Ready	MBR (Basic)	964 MB	1974672	512
BOOT (/dev/sdaa1)				150 MB	307204	512
BOOT (/dev/sdaa1)		Ready		150 MB	307204	512
Local Disk (/dev/sdaa2)		Damaged		467 MB	956420	512
Local Disk (/dev/sdaa3)				337 MB	690170	512
Local Disk (/dev/sdaa3)		Ready		337 MB	690170	512
Unallocated Space				7.20 MB	14742	512

Figure 30: Local disks view

Settings menu

Show partitions

Displays all partitions detected on the local disks.

Show volumes

Displays all volumes detected on the local disks.

Using KillDisk

KillDisk is a powerful industrial tool to provide disk erasure solutions for large workstations with many disks. The features in the KillDisk Industrial software are built with this goal in mind. This section outlines the key features of KillDisk and how they are used to erase single disks to large batches. Much of the software is highly customizable and this guide will help get you started with configuring KillDisk for your particular system, and using KillDisk to its' full potential.

KillDisk 11 is a powerful tool to provide disk erasure solutions for personal and corporate use. This section outlines the key features of KillDisk and how to use this software's many features. Much of the software is highly customizable and this guide will help get you started with configuring KillDisk for your particular system, and using KillDisk to its' full potential.



Note:

It is important to properly set up your KillDisk layout before using any of the features, so read and follow the steps to do this in the [Disk Bay Layout section](#), if you have not already.

Disk Erase

KillDisk is an extremely powerful tool for secure disk erasure. Individual disks or batches of disks can be erased to any desired standard with just a few clicks. The process to achieve this is outlined in this section.

1. Select a disks for erasure

Use [Disk Explorer View](#) on page 30 to select disk bays.

2. Open **Erase disks dialog** dialog using one of the following methods:

- Click the **Erase** command in the action toolbar
- Click **Actions > Disk Erase** command from main menu
- Click **Disk Erase** command from context menu
- Click **Erase Batch > Named batch** command from toolbar or from **Actions** main menu to erase disks in predefined disk batch.

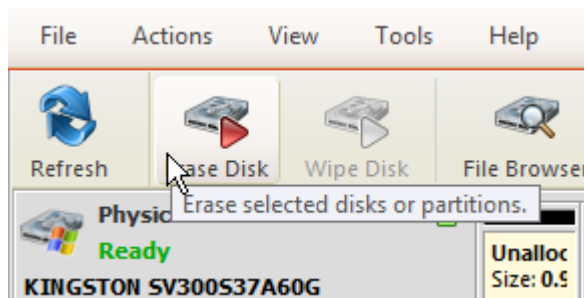


Figure 31: Initiating the Erase operation

3. Confirm erasure options

Use tabbed views to adjust disk erasure options if necessary. Available options:

- [Disk examination options](#) on page 48 [optional in Industrial & Desktop only]
- [Disk Erase Options](#) on page 50
- [Error Handling](#) on page 60
- [Certificate Options](#) on page 54
- [Report Options](#) on page 56
- [Disk copy options](#) on page 62

Use [Disk examination preferences](#) on page 53 page in application preferences to specify disk grading attributes if necessary.



Note:

If only one disk was selected for erasure than you can specify boundaries of erased area for selected disk by clicking **Select exact disk area**. Here you may select sector ranges, or select individual partitions.

Click **OK** button to begin disk erase process.

4. Observe erase process

If [Disk examination options](#) on page 48 was selected then disk examination will started first. Depending on examination outcome at second stage - disk erase begins.

Once the Erase procedure begins, you will see the disk bay represented as a progress bar and it will show the erase method and progress of that disk operation. The progress bar represents the percentage of data left to erase on the drive, with the corresponding percentage shown. As the procedure progresses, the percentage will decrease, and the red bar will get smaller.

The remaining time will also be seen and progress in the operation will be displayed, as shown below:

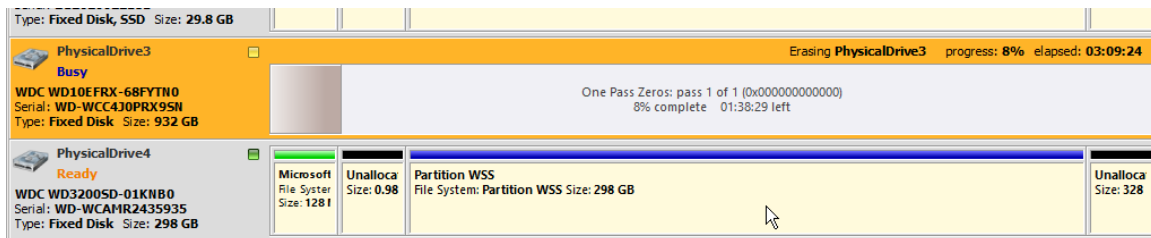


Figure 32: Disk Erase progressing

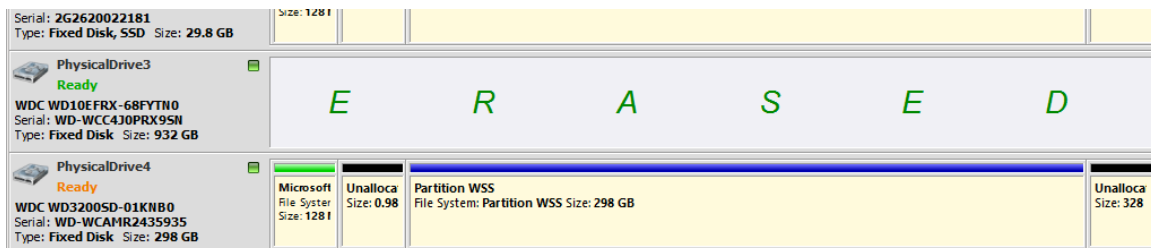


Figure 33: Disk Erase completed

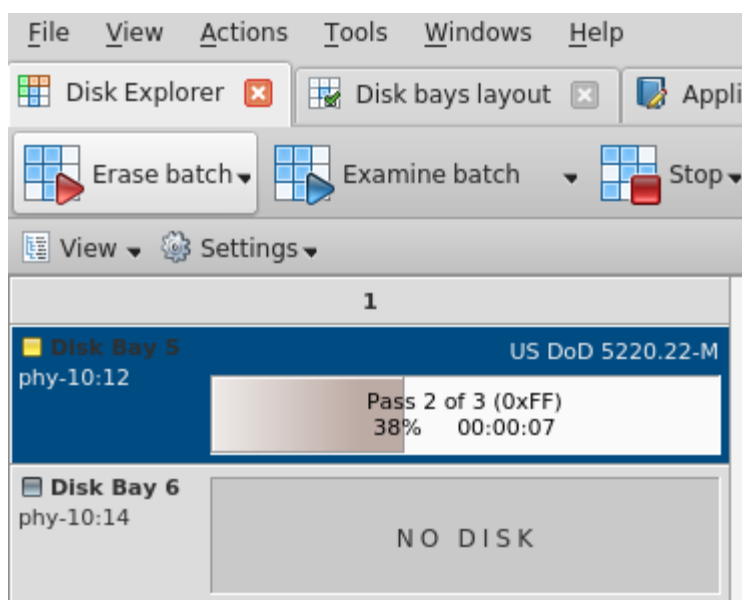


Figure 34: Disk erasure

If [Disk copy options](#) on page 62 was selected then after erase the final stage of this task begins - clone data from source to all successfully erased disks.

When erasing completes you can review results and print an [Erase Certificate](#) on page 66 [Erase labels \(KillDisk Desktop & Industrial only\)](#) on page 68 for processed disks.

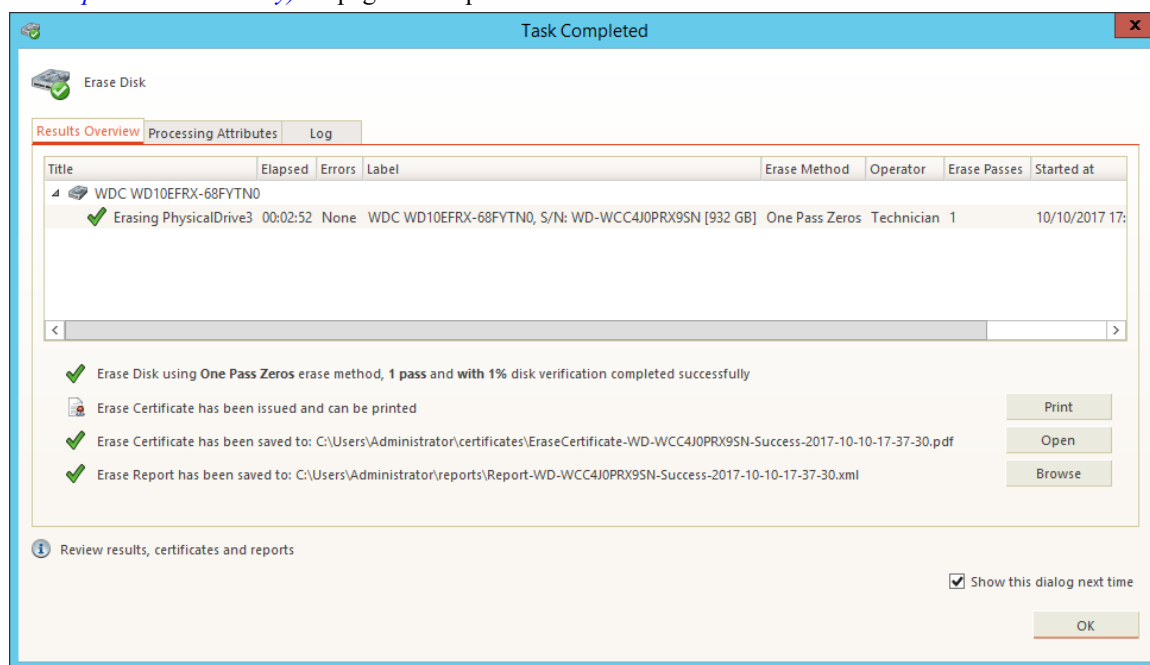


Figure 35: Disk Erase Summary

Selecting Disk Area for Erasure & Erasing Partitions

When selecting a single disk to erase in **KillDisk**, you will be given the option to specify the area on the disk to erase. The default option is **Select entire disk**, which will apply the selected operation on the entire disk selected.

If you're interested in specific areas of the disk (specific partitions, for example), you may use the **Select exact disk area** option. This will allow you to use the sliders on the visualization of your disk to select a particular range of sectors. You may also click on individual partitions and the individual partitions will be selected for erasure.

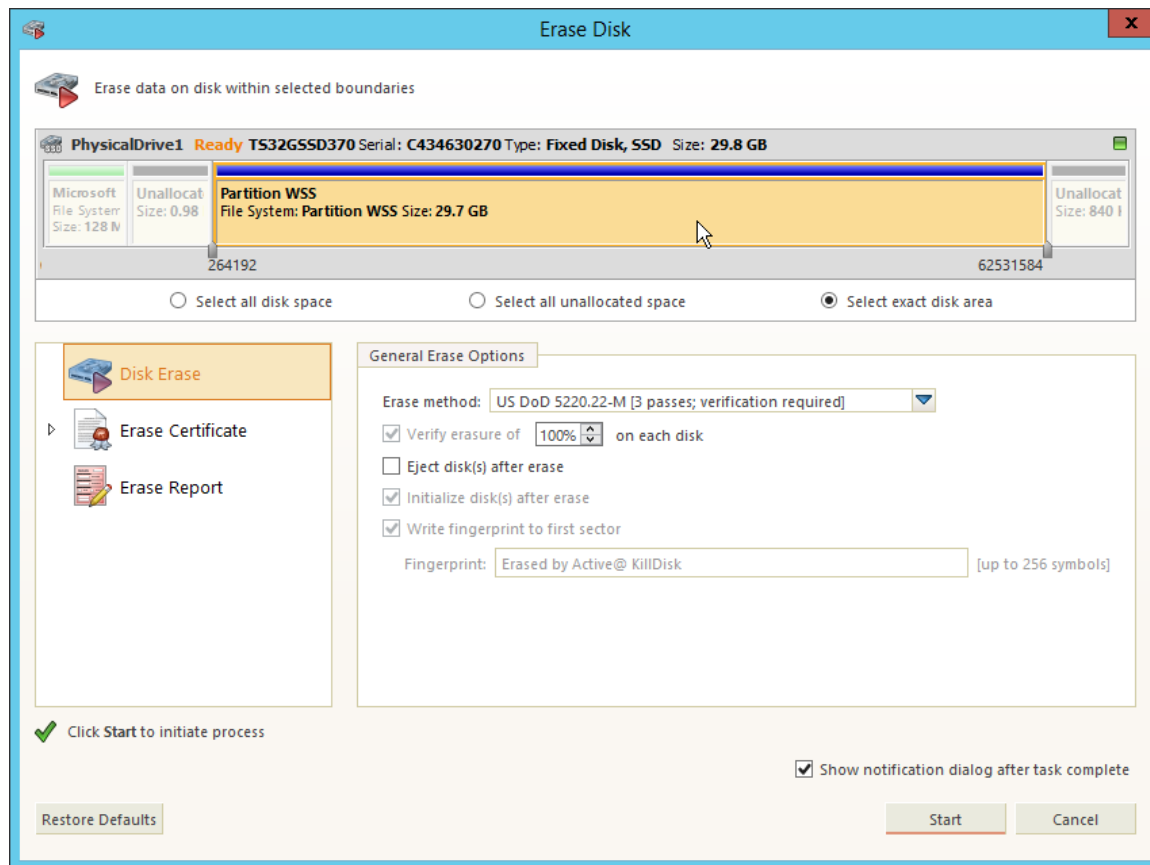


Figure 36: Erasing a specific partition

Disk Wipe

When you select a physical device such as Fixed Disk0, the wipe command processes all logical drives consecutively, deleting data in unoccupied areas. Unallocated space (where no partition exists) has been erased as well. If KillDisk detects that a partition has been damaged or that it is not safe to proceed, KillDisk does not wipe data in that area. The reason it does not proceed is that a damaged partition might contain important data.

There are some cases where partitions on a device cannot be wiped. Some examples are an unknown or unsupported file system, a system volume, or an application start up drive. In these cases the **Wipe** button is disabled. If you select a device and the **Wipe** button is disabled, select individual partitions (drives) and wipe them separately.

If you want to erase data from the hard drive device permanently, see [Disk Erase](#) on page 35.

1. Select the device to wipe in the disk explorer view. You may select multiple devices to be wiped out simultaneously
2. Click the **Wipe** toolbar button to wipe out all data in unoccupied sectors on the disk or one of its' partitions.

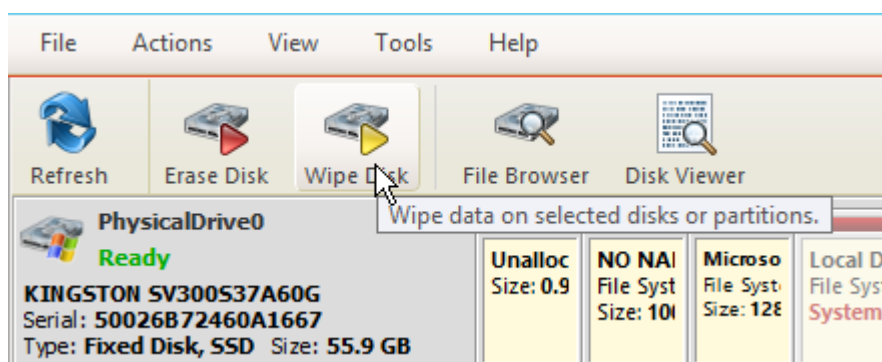


Figure 37: Initiating the Wipe operation

3. Confirm Wipe options

Use tabbed views to adjust disk wipe options if necessary. Available options:

- [Disk Wipe Options](#) on page 52
- [Certificate Options](#) on page 54
- [Report Options](#) on page 56

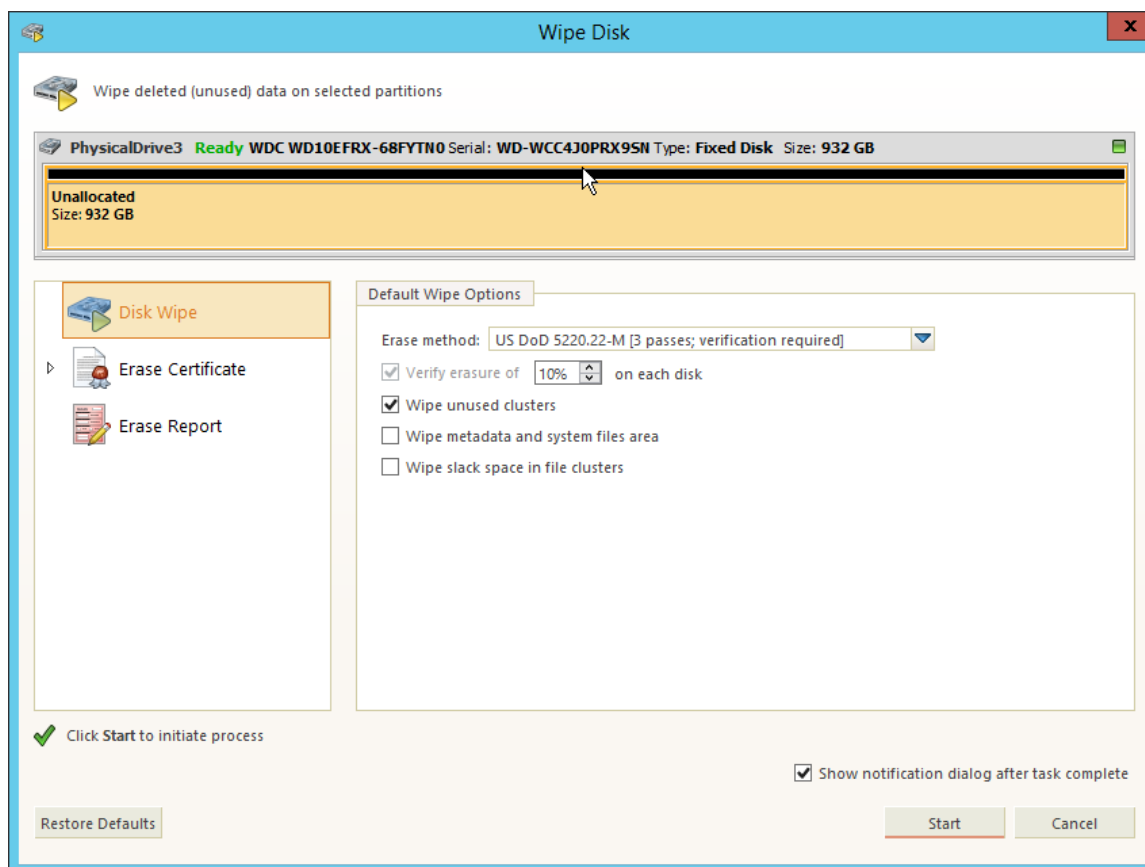


Figure 38: Selecting an an erase algorithm for the wipe

4. Select the areas of the disks to be wiped. With individual disks you may select individual partitions.
5. Click **Ok** to advance to the final step before erasing data. The progress of the wiping procedure will be monitored in the Disk Wiping screen.

To stop the process for any reason, click the stop button for a particular disk. Click the stop all button to cancel wiping for all selected disks. Note that all existing applications and data will not be touched. Data that has been wiped from unoccupied sectors is not recoverable.

6. Optional: Select the wiped partition and press **ENTER** or double-click it to inspect the work that has been done. KillDisk scans the system records or the root records of the partition. The Folders and Files tab appears. Existing file names and folder names appear with a multi-colored icon and deleted file names and folder names appear with a gray-colored icon. If the wiping process completed correctly, the data residue in these deleted file clusters and the place these files hold in the directory records or system records has been removed. You should not see any grey-colored file names or folder names in the wiped partition.

You will see a confirmation dialog when the process is complete, where you may and print an [Erase Certificate](#) on page 66



Note: If there are any errors, for example due to bad clusters, they will be reported on the Interactive screen and in the Log. If such a message appears, you may cancel the operation or continue wiping data.

Examine disks physical integrity

The disk examination feature is designed to scan the physical integrity of the disks selected for this operation.

To examine disks:

1. Select a disks for examination

Use [Disk Explorer View](#) on page 30 to select disk bays.

2. Open **Examining disks readability** dialog using one of the following:

-



Click the **Examine** command in the action toolbar

- Click **Actions > Disk Examine** command from main menu
- Click **Disk Examine** command from context menu
- Click **Examine Batch > Named batch** command from toolbar or from **Actions** main menu to examine disks in predefined disk batch.

3. Confirm examination options

Use tabbed views to adjust examination options if necessary. Available options:

- [Disk examination options](#) on page 48
- [Error Handling](#) on page 60
- [Report Options](#) on page 56

Use [Disk examination preferences](#) on page 53 in application preferences to specify disk grading attributes if necessary.



Note:

If only one disk was selected for examination than you can specify boundaries of examined area for selected disk.

Click **OK** button to begin examination process.

4. Observe examination process

In the [Disk Explorer View](#) on page 30, you will see the progress of the examination in the slot of the drive being operated on. The progress will be shown as a progress bar, seen below:

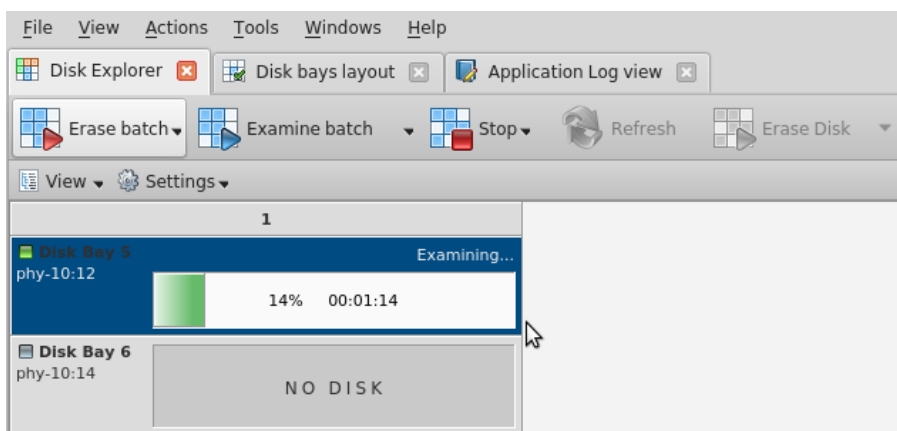


Figure 39: Disk examination progress

As seen in the image above, the green progress bar will fill the virtual drive slot in the KillDisk application. The percentage of the examination completed and the estimated completion time will also be shown in the slot. Once this process completes, the word "Examined" will flash in yellow in the slot space and the Erase procedure will begin.

When erasing completes you can review results for the processed disks.

Additional Options and Features

KillDisk also has a number of supporting features to ensure the most complete sanitation operation, flexibility to meet the most stringent requirements and compatibility with a wide range of systems. This section outlines these features.

Mapping Network Shares

Mapping Network shares is very useful, especially when booting from a boot disk and running the application in batch mode. It guarantees a specific drive letter to save logs and certificates to, as well as provides a central location for erase reports to be stored.

1. In the file menu bar, navigate to File > Map Network Share...

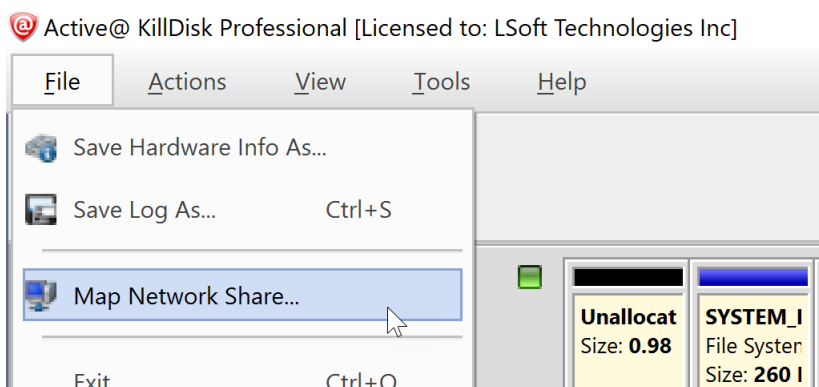


Figure 40: Accessing the network mapping menu

2. Configure your network drive and assign a letter to it, then press **OK**

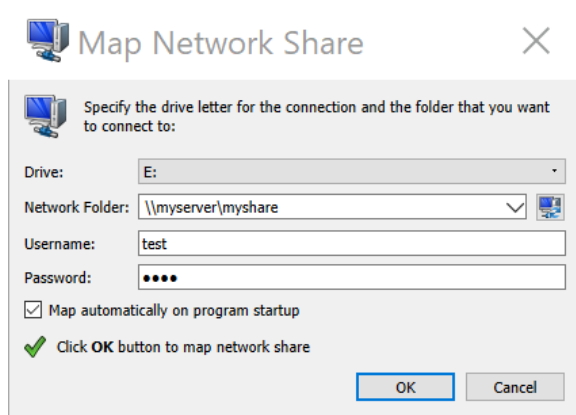


Figure 41: Mapping a network drive

Note: KillDisk will identify all connected network drives, so you may use the drop-down list to select the one you'd like to use

- Now that your network drive is configured, you may select it as a destination for certificates and reports in your [application preferences](#)

Changing Disk Serial Number

In case you notice a disk serial number does not match the number on the disk, KillDisk supports several methods of assigning disk serial numbers, where it pulls it from various sources. To access this feature, right-click the disk in question and select **Set Serial Number..** in the context menu.

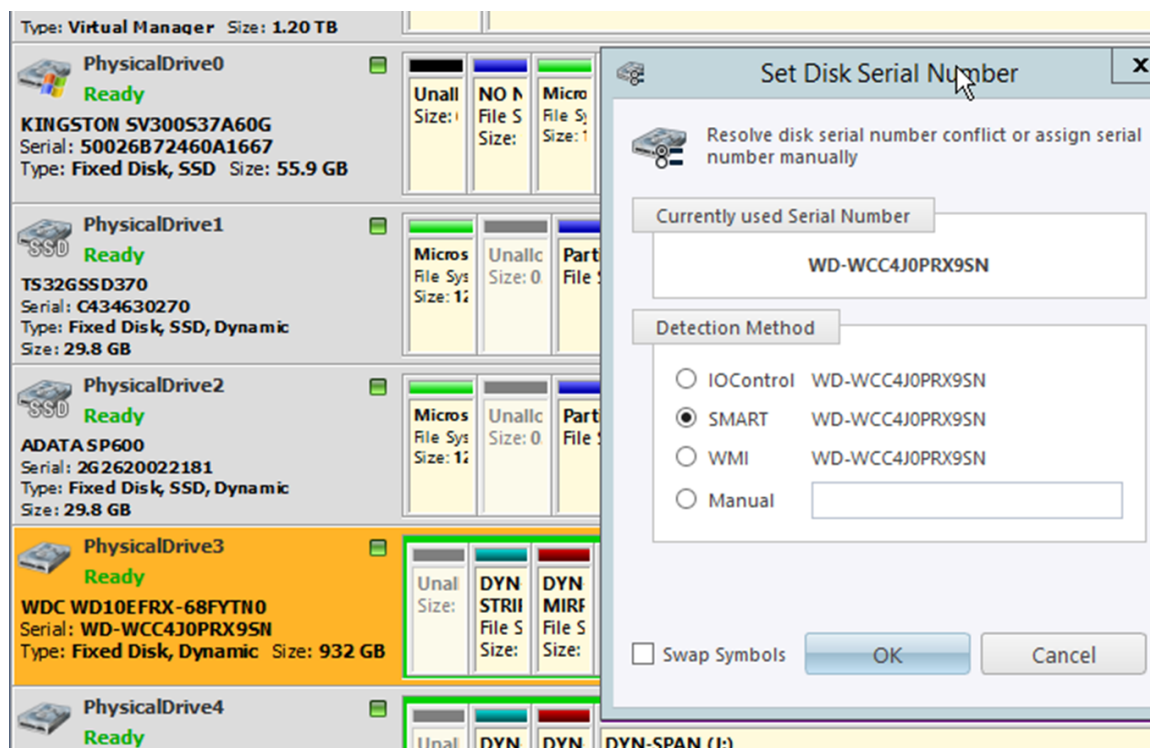


Figure 42: Setting the Disk Serial number



Note: If you don't see your serial number in any of the detection methods, try checking the **Swap Symbols** check box. If this doesn't help, input the serial number manually using the last option. The serial number you are looking for does not match the serial number stored by the disk (i.e. the sticker does not match the drive).

Reset Hidden Areas

KillDisk supports erasing hidden areas of the disk. To perform this task on its' own, right click on the disk and select **Reset Hidden Areas...**

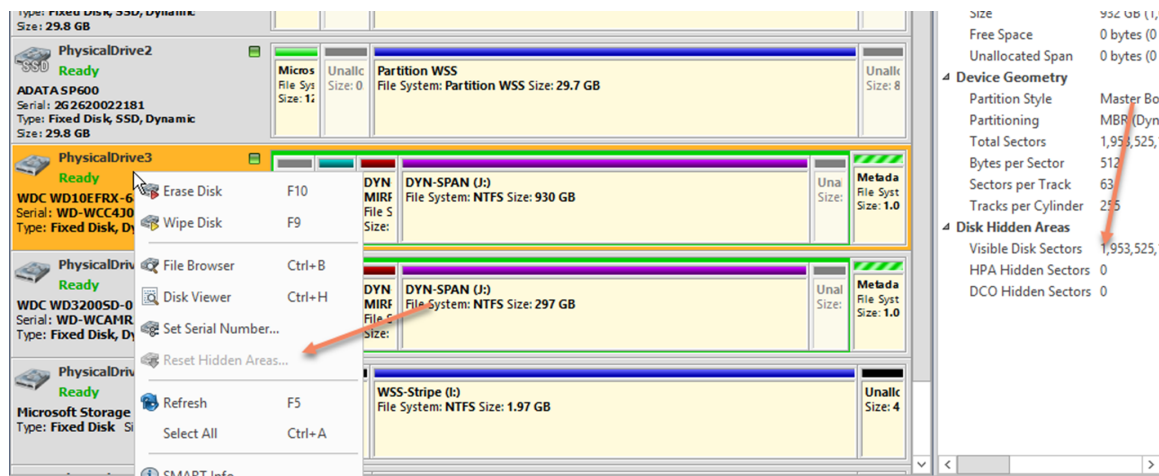


Figure 43: Resetting Hidden Areas

Property views

To show detailed information about any subject of an application, such as disk, partition, volume, file etc., KillDisk uses information views. When open, they follow selected changes and show information about the selected item automatically. Besides only displaying valuable data, they also allow you to copy that information onto a clipboard by using context menu commands.

Copy Value

Copy only value of selected field in the information view.

Copy Field

Copy formatted name and value field pair.

Copy All

Copy all information as formatted set of name and value pairs.

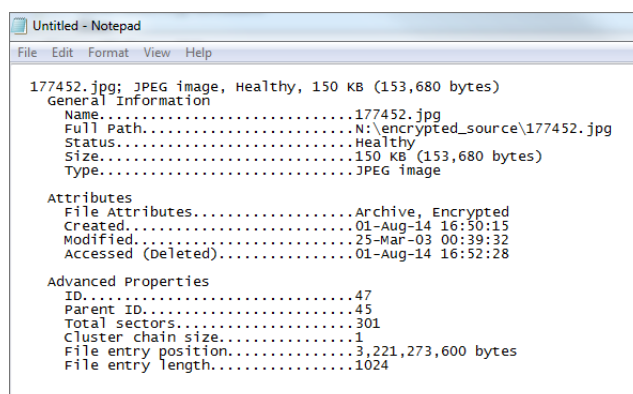


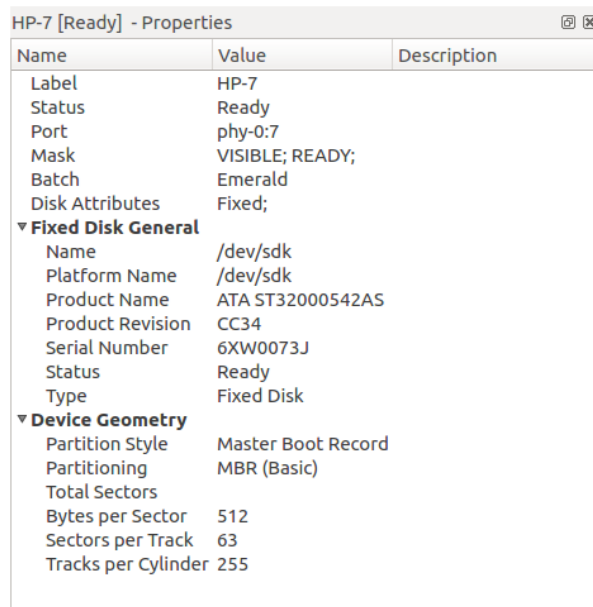
Figure 44: Example of copied information about file

Property view

To show property view for selected item do one of the following:

- Click **View > Windows > Properties**
- Click **F4** keyboard short cut or

- Use context menu command **Properties** for the same effect



The screenshot shows a window titled "HP-7 [Ready] - Properties". It contains a table with three columns: "Name", "Value", and "Description". The table lists various disk properties, including general information, fixed disk details, and device geometry.

Name	Value	Description
Label	HP-7	
Status	Ready	
Port	phy-0:7	
Mask	VISIBLE; READY;	
Batch	Emerald	
Disk Attributes	Fixed;	
▼ Fixed Disk General		
Name	/dev/sdk	
Platform Name	/dev/sdk	
Product Name	ATA ST32000542AS	
Product Revision	CC34	
Serial Number	6XW0073J	
Status	Ready	
Type	Fixed Disk	
▼ Device Geometry		
Partition Style	Master Boot Record	
Partitioning	MBR (Basic)	
Total Sectors		
Bytes per Sector	512	
Sectors per Track	63	
Tracks per Cylinder	255	

Figure 45: Property view example

S.M.A.R.T. Information

This is another information view, displaying SMART (Self-Monitoring, Analysis and Reporting Technology) data of the selected hard drive, if the device supports it. To show this view:

- Click **View > Windows > SMART Info**
- Use context menu command **SMART Info** for the same effect

Fixed Disk: /dev/sdk - S.M.A.R.T. Information	
Refresh	
Name	Value
▼ Fixed Disk General	
Device Model	ST320005XXXX
Serial Number	6XW01CTW
Firmware Version	CC34
Capacity	2000398934016
ATA Version	8
ATA Standard	Device does not report versi
SMART Support	1
Off-line data collection status	130
Self-test execution status	0
Time Off-line data collection, sec	633
Off-line data collection capabilities	123
SMART capabilities	3
Error logging capabilities	1
Short self-test time, min	1
Extended self-test time, min	255
▼ Attributes	
[001] Raw Read Error Rate	15788906
[003] Spin Up Time	0
[004] Start/Stop Count	269
[005] Reallocated Sector Count	0
[007] Seek Error Rate	9525169451
[009] Power-On Hours Count	33165
[010] Spinup Retry Count	0
[012] Power Cycle Count	267
[183] Runtime Bad Block	0
[184] End-to-End Error	0
[187] Reported Uncorrect	0
[188] Command Timeout	4295032835
[189] High Fly Writes	25
[190] Airflow Temperature Celsius	26
[194] HDA Temperature Celsius	26
[195] Hardware ECC Recovered	15788906
[197] Current Pending Sector	0
[198] Offline Uncorrectable	0
[199] UDMA CRC Error Count	0
[240] Head Flying Hours	33560
[241] Total LBAs Written	2826716440
[242] Total LBAs Read	110146536

Figure 46: SMART information for physical device example

SMART data can be used to diagnose disks by showing important information such as Power-on Hours, Reallocated Sectors and Current Pending Sectors



Note: If the Current Pending Sectors parameter is not 0, the disk has bad sectors that will cause problems in the future. Dispose of these disks as soon as possible.

Dynamic Disks, Virtual Drives and Windows Storage Spaces

Dynamic Disks (LDM), Virtual Drives and Windows Storage Spaces (WSS) are fully supported with KillDisk 11. These disks will appear in the disk view as any other disks would, along with their component disks. When you launch an erase operation on the virtual disk, you will see it reflected on the components disks as well.

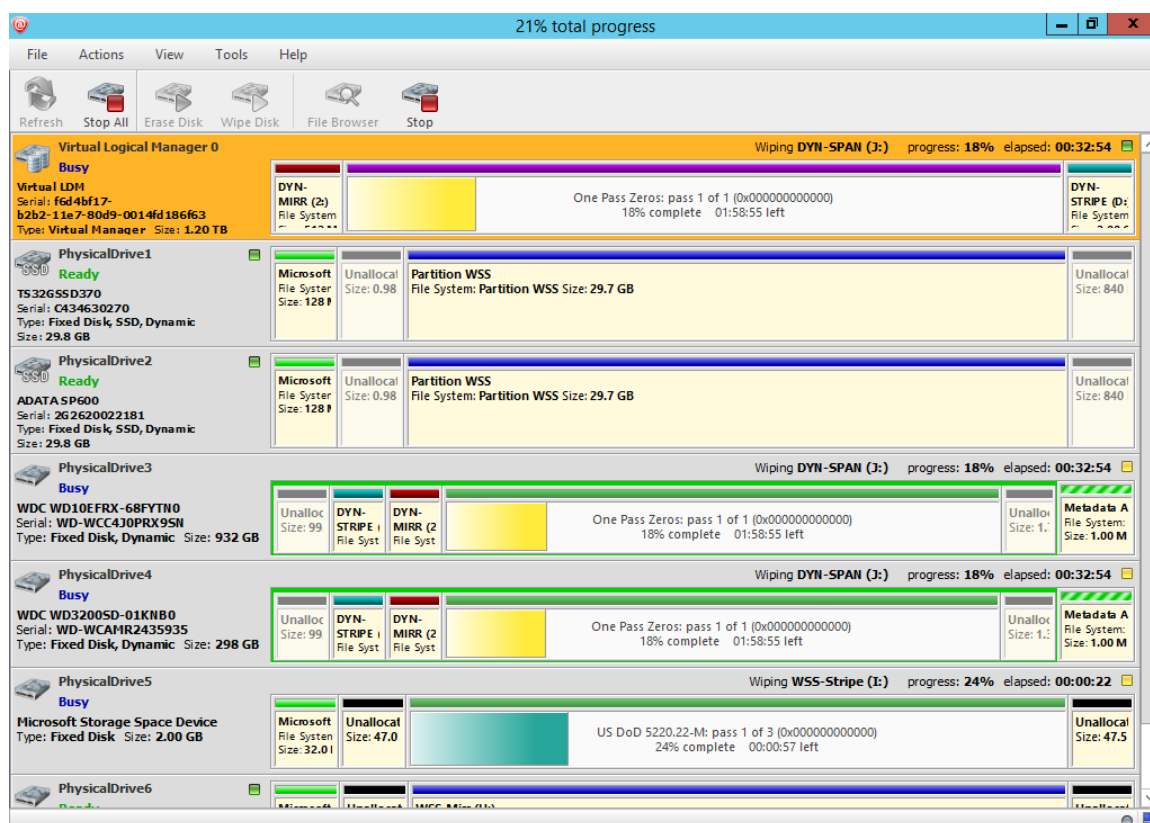


Figure 47: Virtual drive being erased in conjunction with a WSS striped array

Preferences

The **KillDisk Preferences** window is the central location where KillDisk features can be configured. These features are split up into several tabs.

To open Preferences dialog:

- From main menu choose **File > Preferences...** or
- Use **F2** keyboard shortcut at any time

Preferences dialog could be open from other task dialogs to change related settings.

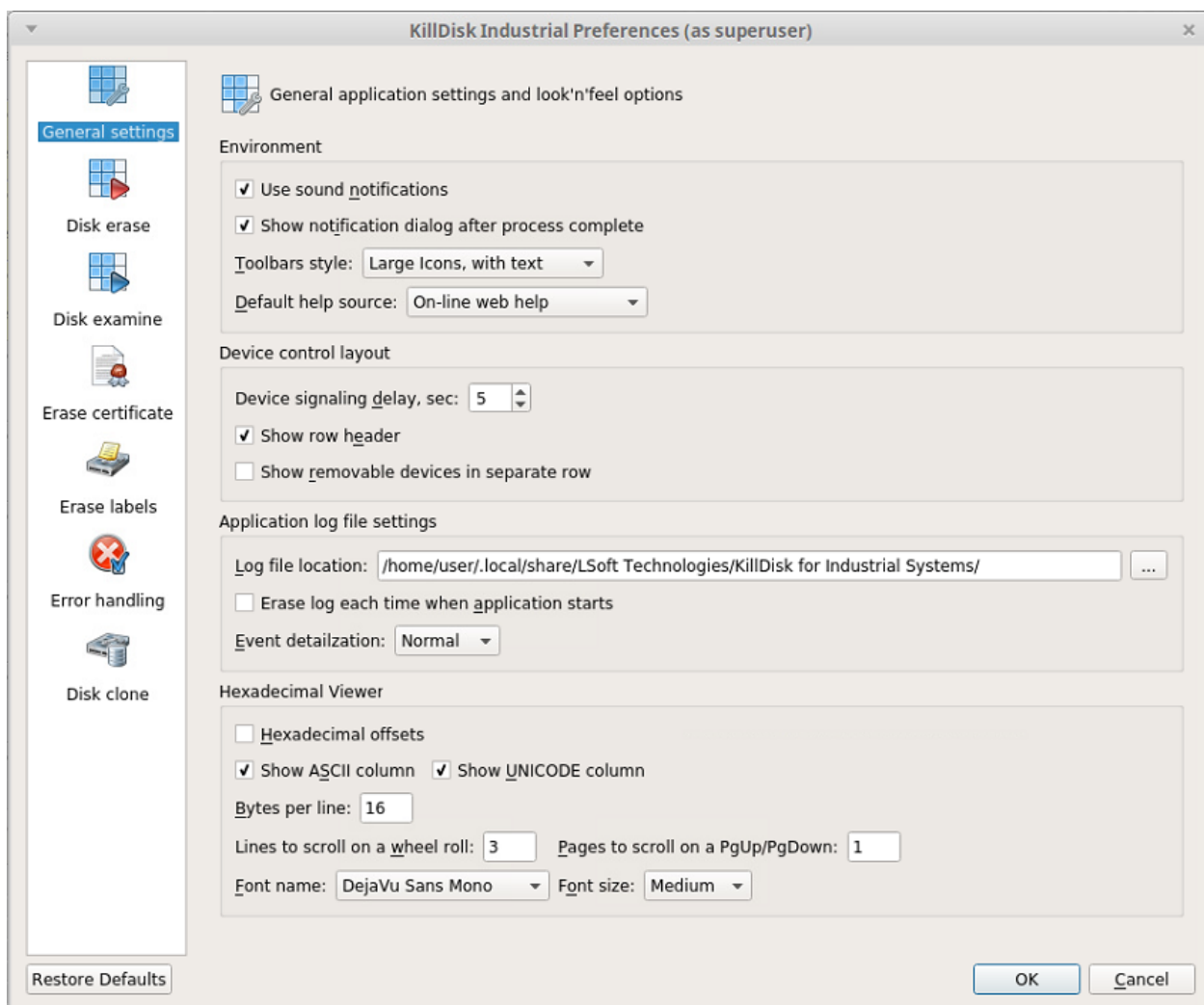


Figure 48: KillDisk Industrial Preferences dialog

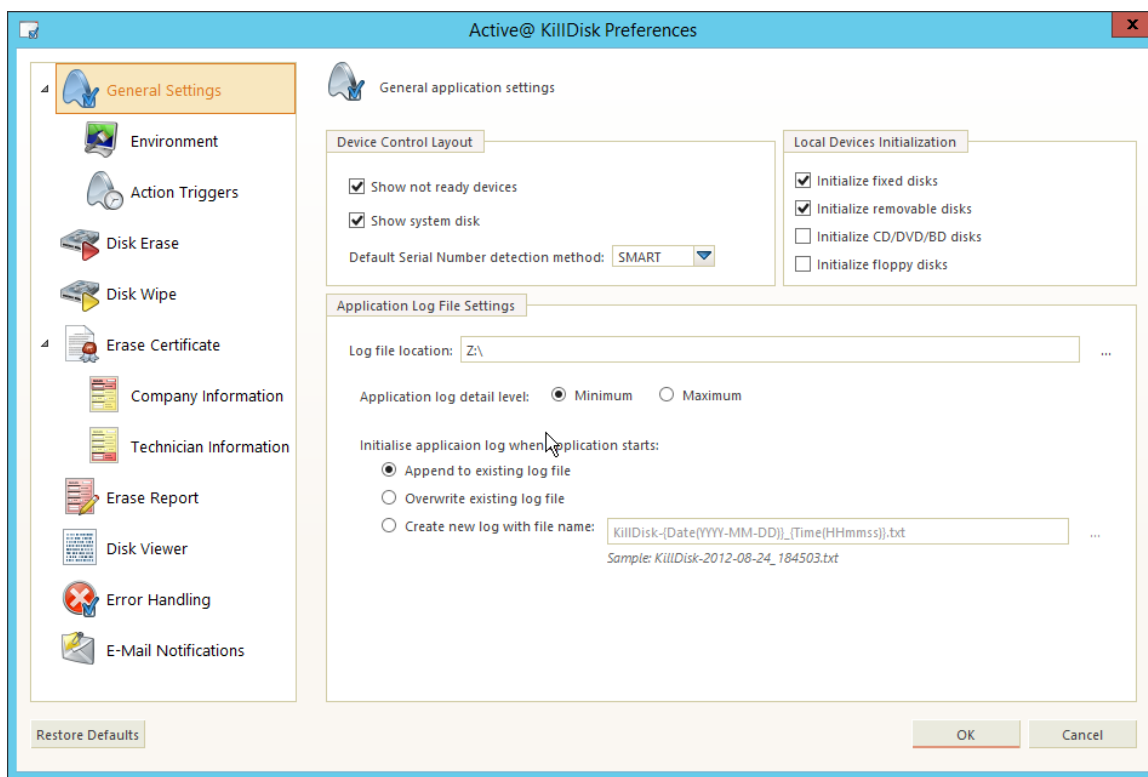


Figure 49: KillDisk 11 Preferences dialog

Accessing the **Preferences** allows users to configure all the global settings for the application.

When a KillDisk operation, such as **Wipe** or **Erase** is initiated, a smaller subset of these settings is available to modify, or the global settings may be kept, pertinent to the particular job.

The process and functionality of the **Preferences** options will be outlined in this section.

Disk examination options

KillDisk offers several different disk examination options, depending on user needs. Each examination type has its' own strengths and weaknesses, mainly tradeoffs between time and thoroughness. Any of the examination types can be performed on an entire disk, or a selected segment.

Examination options are required for disk integrity examination and optional for disk erasure but can be used to sort away faulty disk from following processing in sequence.

To examine disk integrity the following three algorithms are used:

Partial Examination

Examines a percentage of the disk, equally segmented in a selected area.

Partial Random Examination

Examines a set number of randomly distributed sections of the disk within the selected area.

Read Each Sector in Selected Area

Examines the entirety of a selected area, set for examination. Because this reads every sector in the selected area, this is the most lengthy, but thorough of the disk examination procedures.

Based on examination results disks could be "grades" depending on amount of failed sectors. Specific grade attributes can be set on [Disk examination preferences](#) on page 53 page of application preferences.

General Preferences

The General preferences options allow the user to configure general application settings, as well as the visual aspects of the application.

General Settings

These are configurable options pertaining to the applications functionality.

Device control layout

These settings controls disk bay layout behavior in main [Disk Explorer View](#) on page 30

Device signaling delay, sec

When a process finishes, KillDisk displays a message, overlaying the disk. In the disk bays view This setting configures the delay of this notification when the process finishes.

Show removable devices in separate row

All removable devices will be shown in separate row (column) regardless of disk bay mapping.

Hide system disk

Hides the disk used by the operating system from the KillDisk application.

Default Serial Number detection method

Select how KillDisk retrieves the disk serial number

Local devices initialization

Select which types of devices appear in KillDisk for examination and erasure

Application log file settings

These settings apply to the log file automatically generated by the application. Not to be confused with the erasure report or certificate. All operations performed in a KillDisk session will be saved in this log.

Log file location

Allows the user to specify where the application log file is saved. By default, this is set to KillDisk's root directory.

Initialize application log when application starts

This setting configures whether KillDisk generates a new log file for every session (erasing the log of the previous session), or appends new sessions to one log file.

Environment

These are configurable options pertaining to the applications user interface and user experience.

Use sound notifications

Toggles sound tones being used for notifying the user of the completion of a task, errors and notification during an operation.

Show notification dialog after process complete

Process complete dialog will be shown at the end of single or multiple disk processing, letting user print certificate, erase labels etc.

Application style

Configures the colour scheme used in the application

Toolbar style

Configures how icons are shown in the toolbar (shown below).

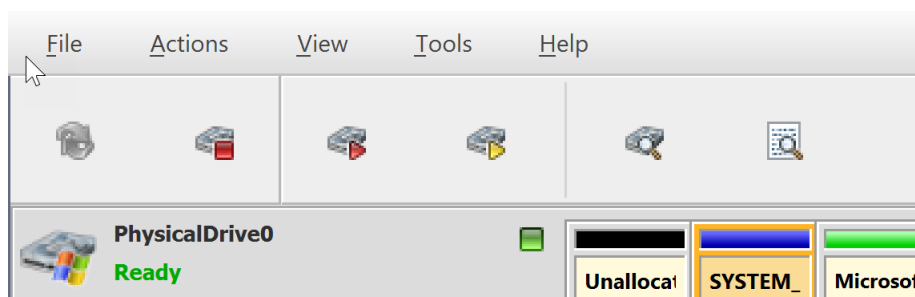


Figure 50: Small icons no text

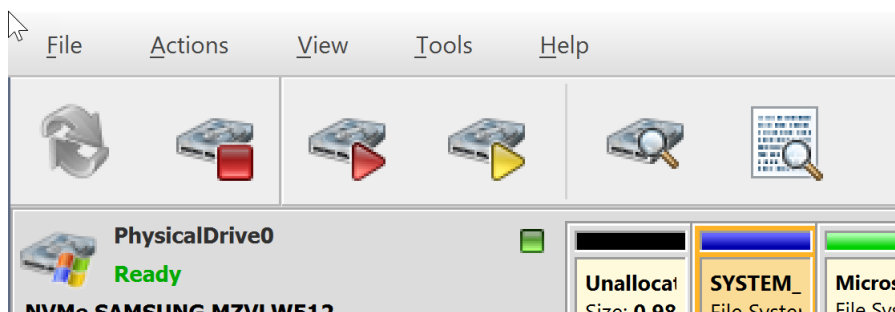


Figure 51: Large icons no text

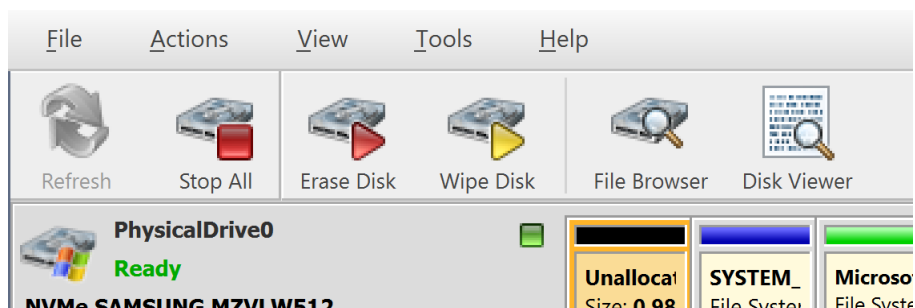


Figure 52: Large icons with text

Default help source

If available, user can select help documentation source to be addressed when requested

Run-time Actions

Configure actions performed while application is running

Automatically check for software updates

If this option set, application will check for a new updates during start.

Action after all processes complete

Select either no action or **hibernate** or **shutdown** system after all processes finished.



Caution: You will have 30 seconds to abort system hibernation or shutdown.

Disk Erase Options

The Erase Preferences tab allows for users to configure settings for the KillDisk erase procedures.

The same erase options for each batch could be set through [Edit disk batch attributes](#) on page 80 dialog

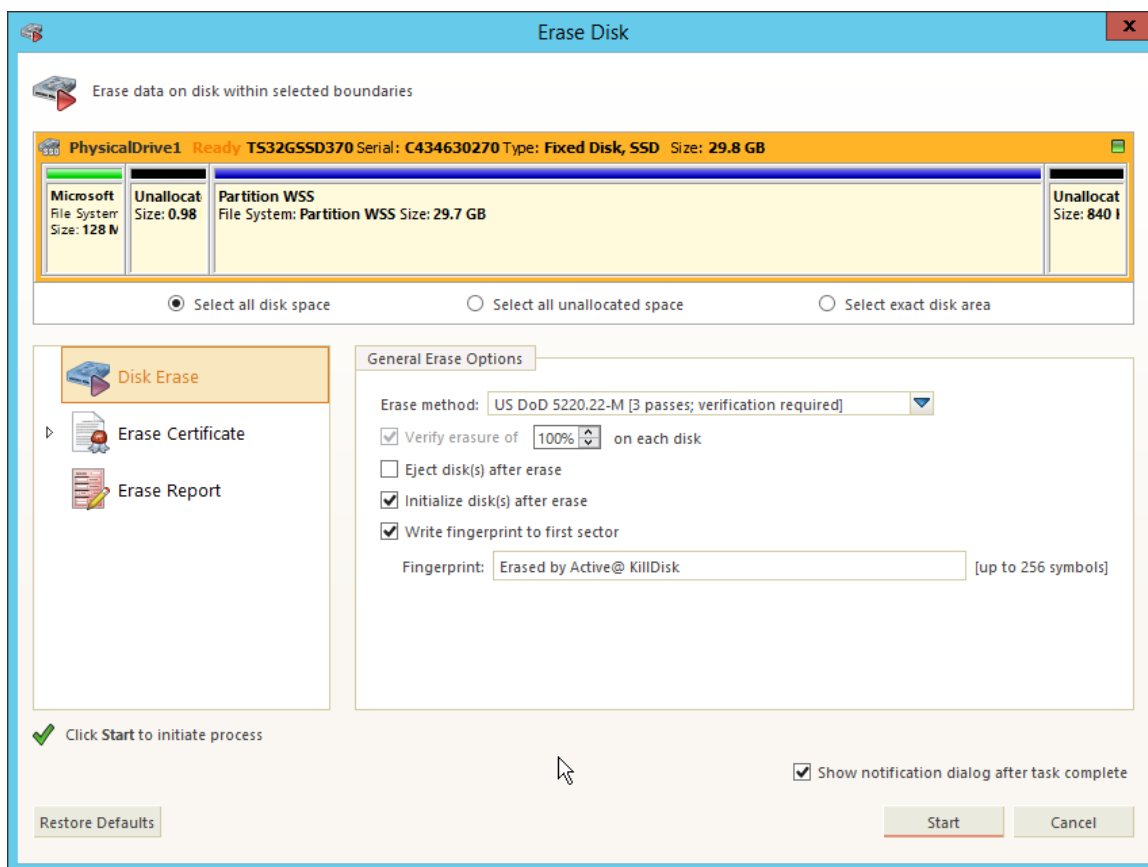


Figure 53: Erase options dialog

Select entire disk

Entire surface of the disk will be erased

Select exact area

Allows you to use the sliders on the visualization of your disk to select a particular range of sectors for erasure. You may also click on individual partitions and the selected individual partitions will be erased.

Erase method

One of many internationally recognized erase methods *supported by KillDisk*.

Erase verification

Percentage of disk to be verified after disk was erased.



Note: In some erase methods such as the US DoD 5220.22-M, this option is mandatory. After the erase operation has completed, this option will scan the entire drive evenly and verify the integrity of the erase operation. The percentage indicates the percent of the sectors that are checked, spread across the disk. Most standards specify 10% as an accurate sample size for the verification.

Initialize after erase

Formats the disk to be ready to use after erasure.

Write fingerprint

This feature will write the specified fingerprint to the first sector of the erased drive. If a machine is booted from this drive, the user will see this fingerprint as a message on the screen.

Erase confirmation

As a safety precaution to prevent accidental destruction of hard drives, KillDisk has the user type a keyphrase before the erase procedure is initiated (Figure 3.1.6). By default this precaution is set with the keyphrase

"ERASE-ALL-DATA". This keyphrase can be modified, set as a randomly generated set of characters, or disabled in these settings.

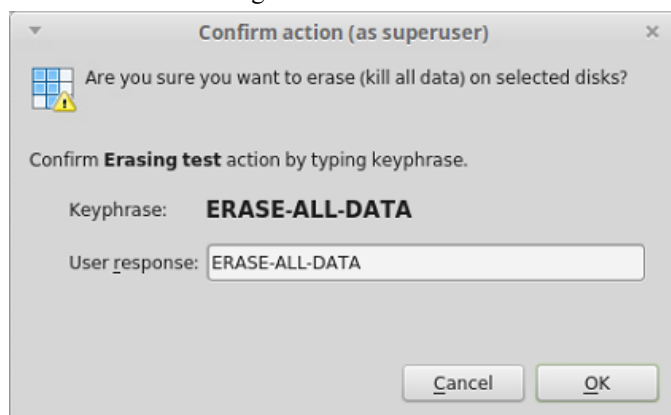


Figure 54: Sensitive action confirmation dialog

Also see [Report Options](#) on page 56 for information about erase report.

Disk Wipe Options

The disk wipe procedure, like with the erase procedure, allows you to specify the erase method used, as well as a few additional wipe-specific options.

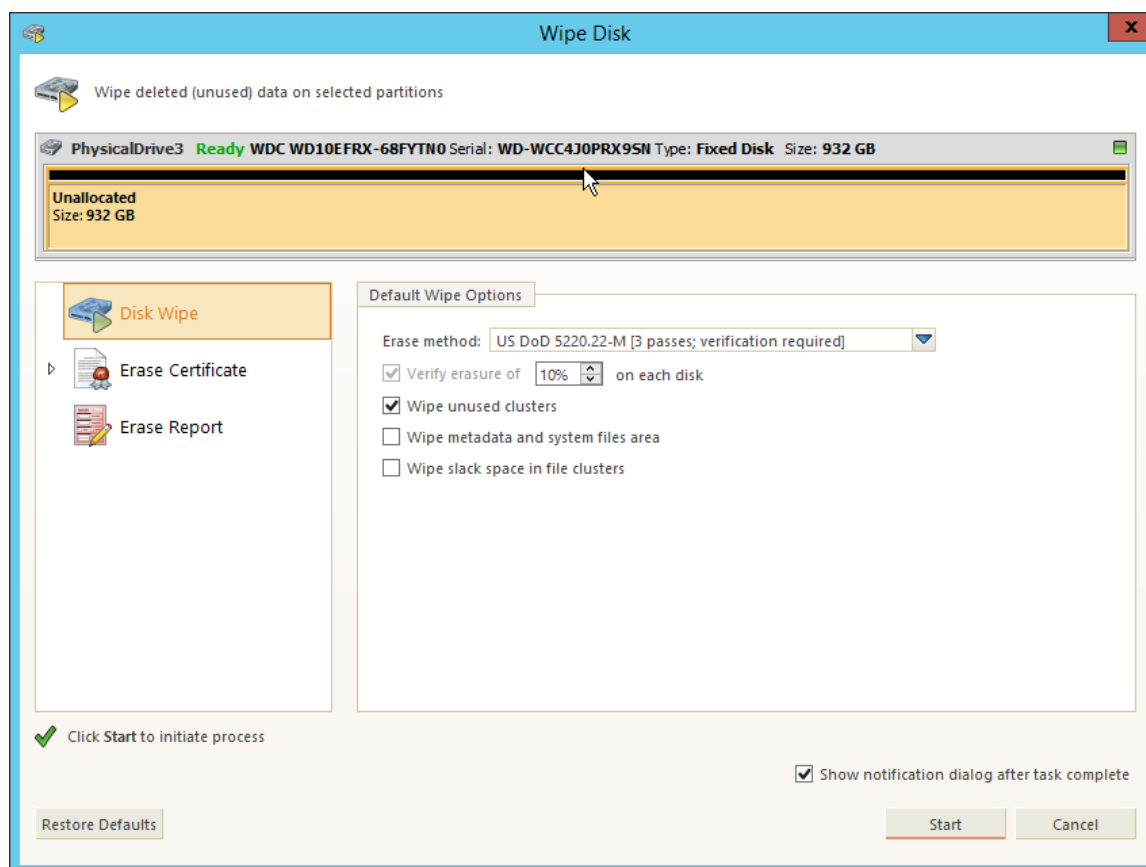


Figure 55: Wipe options dialog

Select entire disk

Entire surface of the disk will be wiped

Select all volumes

All volumes will be selected for the wipe operation

Select all unallocated space

Only unallocated space (unformatted, no drive letter) will be wiped

Select single partition

Select a specific partition to be wiped

Erase method

One of many internationally recognized erase methods *supported by KillDisk*.

Erase verification

Percentage of disk to be verified after disk was erased.

Wipe unused clusters

Erase areas of the hard drive that are not formatted and not currently used by the operating system (data has not been recently written there unless this is a recently deleted partition).

Wipe metadata and system files area

Erase areas of the disk containing information about previous files on the volume and prevents recovery of files using past records of them.

Wipe slack space in file clusters

Erase slack space within files. Files are allocated a set amount of space by the OS, in certain increments (depending on the file system). Because files are usually never *exactly* the size of the space allocated to them, there may be unused space within a file that may contain traces of data. This algorithm wipes this space to remove these data traces.

Disk examination preferences

The Disk Examination tab allows the user to configure the settings for KillDisk's examination procedure, namely the colors used to represent first, second and third grade disks and the examination XML report settings.

Disk grading**Disk grade settings**

For each grade, you may select the Green, Yellow, or Red to represent the disk grade visually. Multiple grades may share the same color.

Maximum read errors

Defined under the second grade disks section, the maximum read errors settings allows the user to define the maximum read error tolerance before a disk is categorized as a third grade disk. Third grade disks are the worst grade level, and are considered unreliable for use.

Save XML erasure reports**Report location**

User may configure where XML examination reports are saved.

File Name template

Here you may specify the name template for the XML reports. Because every erase operation will generate a separate report, KillDisk saves the date and time in the default settings to keep reports. The main tags available are:

Table 1: File name template tags:

Available file name element:	Tag:
Serial ID	{Serial ID}

Available file name element:	Tag:
Erasure Status	{Status}
Date of Erasure	{Date(YYYY-MM-DD)}
Time of Erasure	{Time(HH-mm-ss)}

To see additional file name tags available, see the [File name tags section](#) in the Appendix.

Include system and hardware info

Ensures that the system-specific information is saved in the XML report, such as:

- Operating system
- Kernel version
- Platform name
- Device attributes
- Disk geometry
- Partitioning information
- Active partitions

Include technician information

Optionally place the technician information (defined in the [Certificate Preferences](#)) into the XML erasure report

Create separate report for each disk for batch operations

By default batches are treated as one unit, so XML reports will include the report information for all the disks in a batch. This option allows for the user to create separate reports for each of the disks pertaining to a batch, so the disk records can be handled separately. This is useful when disk reports are required immediately for each disk; the batch does not need to complete before the report is issued.

Certificate Options

These preferences allow the user to customize the erasure certificates with company specific information, technician information, and additional certificate options.

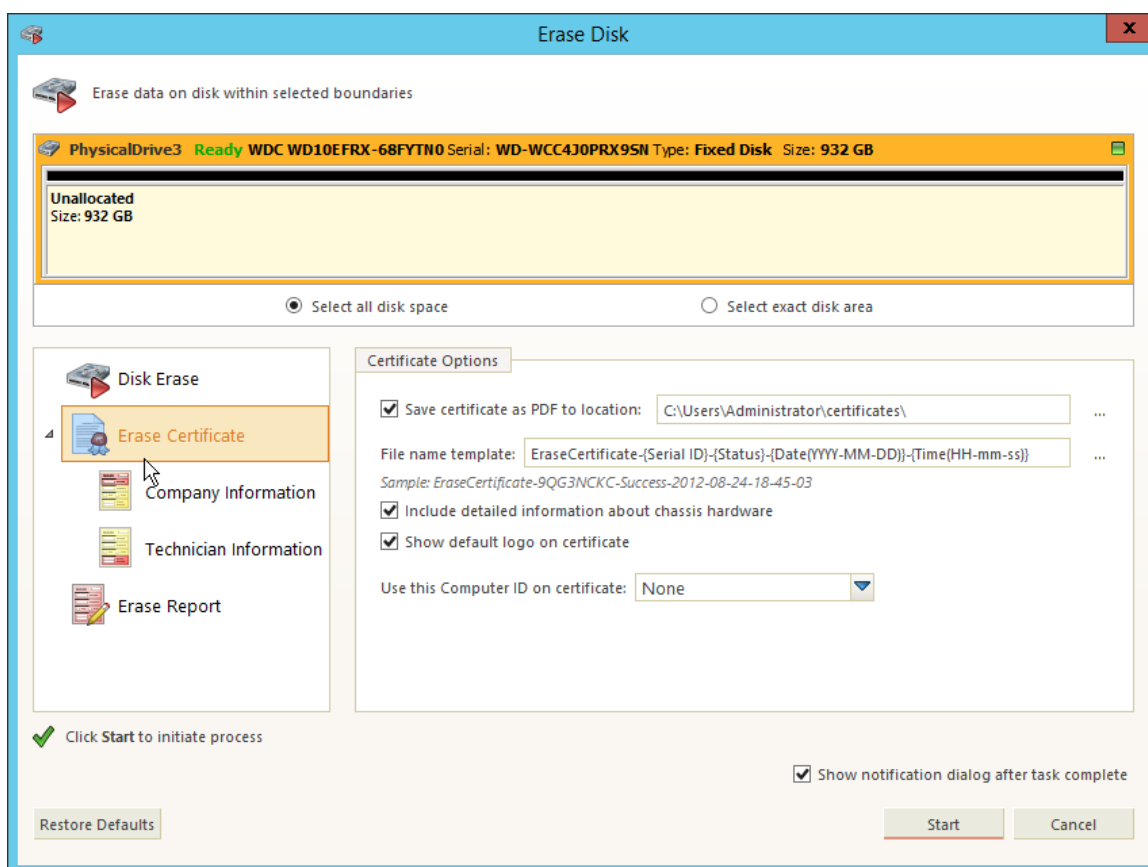


Figure 56: Certificate options window

Save PDF certificate

Use this option to save erase certificate as file in PDF format to selected **location**.

File name template

Here you may specify the name template for the erase certificate. To see additional file name tags available, see the [File name tags section](#) in the Appendix.

Include detailed information about chassis hardware

Ensures that the system-specific information is saved in the XML report, such as:

- Operating system
- Kernel version
- Platform name
- Device attributes
- Disk geometry
- Partitioning information
- Active partitions

Show default logo on certificate

Uses the logo "Erased by Active@ KillDisk" in the certificate

Use Computer ID on certificate

This option includes the Hardware ID of the machine being erased on the certificate. It may be taken from the BIOS or the Motherboard (these values may differ from each other).

Create separate certificate for each disk for batch operations


By default batches are treated as one unit, so XML reports will include the report information for all the disks in a batch. This option allows for the user to create separate reports for each of the disks pertaining to a batch, so the disk records can be handled separately. This is useful when disk reports are required immediately for each disk; the batch does not need to complete before the report is issued.

Company information

This section allows for the user to customize company features like:

- Licensed name
- Business name
- Location
- Phone
- Disclaimer
- Signature field for a company supervisor (optional)

Additionally, custom logos can be added by clicking **Set** and selecting an logo through the file explorer. The logo will be previewed in the Company logo space above.

 **Tip:** It is recommended for better results to use company logo with resolution suitable for printing (300dpi) with a side not exceeding 300px.

Technician Information

This section allows for the user to customize company features like:

- Licensed name
- Business name
- Location
- Phone
- Disclaimer
- Signature field for a company supervisor (optional)

Report Options

These settings allow you to configure the XML reports generated by KillDisk operations

Report Location

User may configure where XML erasure reports are saved.

File Name template

Here you may specify the name template for the XML reports. Because every erase operation will generate a separate report, KillDisk saves the date and time in the default settings to keep reports. The main tags available are:

Table 2: Default file name template tags:

Available file name element:	Tag:
Serial ID	{Serial ID}
Erasure Status	{Status}
Date of Erasure	{Date(YYYY-MM-DD)}
Time of Erasure	{Time(HH-mm-ss)}

To see additional file name tags available, see the [File name tags section](#) in the Appendix.

Include system and hardware info

Ensures that the system-specific information is saved in the XML report, such as:

- Operating system
- Kernel version
- Platform name
- Device attributes
- Disk geometry
- Partitioning information
- Active partitions

Include technician information

Optionally place the technician information (defined in the [Certificate Preferences](#)) into the XML erasure report

Create separate report for each disk for batch operations

By default batches are treated as one unit, so XML reports will include the report information for all the disks in a batch. This option allows for the user to create separate reports for each of the disks pertaining to a batch, so the disk records can be handled separately. This is useful when disk reports are required immediately for each disk; the batch does not need to complete before the report is issued.

The KillDisk XML report contains the following parameters:

Table 3: XML Report Parameters

Type of Information	Specific data
Company Information	<i>Name</i>
	<i>License</i>
	<i>Location</i>
	<i>Phone</i>
	<i>Disclaimer</i>
System Information	<i>OS version</i>
	<i>Platform</i>
	<i>Kernel</i>
Erase Attributes	<i>Erase Verify</i>
	<i>Passes</i>
	<i>Method</i>
	<i>Verification passes</i>
Error Handling Attributes	<i>Errors terminate</i>
	<i>Skip interval</i>
	<i>Number of Retries</i>
	<i>Lock</i>
	<i>Source?</i>
	<i>Ignore Write?</i>

Type of Information	Specific data
	<i>Read?</i>
	<i>Lock?</i>
Disks	<i>Device Size</i>
	<i>Device Type</i>
	<i>Serial Number</i>
	<i>Revision</i>
	<i>Product Number</i>
	<i>Name</i>
	<i>Geometric Information</i>
	<i>Partitioning Scheme</i>
Additional Report Attributes	<i>Fingerprint Information</i>
	<i>Initialize disk?</i>
Result	<i>Bay</i>
	<i>Time and Date Started</i>
	<i>Disk Information</i>
	<i>Status</i>
	<i>Result</i>
	<i>Time Elapsed</i>
	<i>Errors</i>
	<i>Name of operation</i>

Erase labels preferences



These preferences help you globally adjust label settings for the KillDisk system. These labels may be configured to any printer, page or label type using KillDisk's highly customizable labels features.


Label preview

Displays a preview of one label, given the current inputted settings. Refreshes as adjustments are made to the settings.


Page template

The print label dialog gives you access to a number of predefined standard templates and any custom templates you may create. These template may be easily selected without opening any additional dialogs and the details of the selected template will be displayed below the selection box. If your specific labels differ from any of the templates

available, the  button allows you to create a custom template with your own specifications. Additionally, the 

button allows you to modify an existing template and the  button deletes the selected template.

Creating a new template

Upon clicking the  button, the following template editor window will appear. Descriptions of the template editor options are listed below.

Template Title

Here you may create a custom title for your template. This is the name that will reference this template when selecting it in the Print Label dialog.

Page

Here you may specify the dimensions of the page used to print the labels. This may be selected from the list of standard sizes, or defined using exact measurements.

Page margins

Here, page margins are defined for the top, bottom, left and right sides of the page.

Label Layout

These settings define how the labels appear on the page. You may define the spacing in between labels on the page and the dimensions of the label grid. Once you've put in the proper measurements, KillDisk will take care of the formatting.

Unit size

The units of measurement may be manipulated between millimeters, inches, pixels and points. If a value is entered in one measurement and the unit size is changed, the appropriate conversion will take place.

Print Start Position

The print start position section of the dialogue allows you to select what label on the page the labels start printing from. As you use labels, the labels won't always start from the 1x1 position, so you can adjust this setting accordingly.

Label Style and options

These options allow you to change the styling on the labels with the following options:

Label Title

Allows you to set a title to be printed in bold at the top of the labels. This can be company name, batch name or any other descriptors you may consider useful to identify the operation.

Add signature line

Toggling this on places a line at the bottom of the label for the technician to sign off on upon completion of the wipe.

Add certificate logo

Includes the logo used in the certificate as a watermark background of the label.

Print options

Define options for erase label printing, including special label printers like Brother QL-570 and others

Default printer

Select printer to be used exclusively to print erase labels.

Always print labels

Use this option to automatically print erase labels right after erasure completed.

Skip print preview

Disable in-build system print preview dialog and print labels immediately when requested.

Print output adjustments

The print output adjustments section of the dialogue allows you to **vertically** or **horizontally** displace the position measured in specific **units** of the print to adjust to different printers.

Print test label command will let you print erase label sample to verify your settings and selected layout attributes.

Disk Viewer Settings

Allows user to set hexadecimal view settings, font and interaction.

Hexadecimal offset

Toggles offset format between decimal and hexadecimal.

Show ASCII column

Toggles display content in ASCII format

Show UNICODE column

Toggles display content in UNICODE format

Bytes per line

Defines amount of bytes per line in binary display

Lines to scroll

Number of lines to scroll for a single mouse wheel sweep

Pages to scroll

Number of pages to skip for a single **PageUp** or **PageDown** click

Font name

Select any monospace font available for better experience

Font size

Font size to be used in binary view

Error Handling

KillDisk has a broad capabilities to handle errors encountered during continuous disk processing. This is an advanced preference that allows for the configuration of KillDisk's error handling of continuous processes.

Error handling attributes

KillDisk allows you to select one of three ways to handle Read/Write Errors:

Abort entire disk group processing

This means that if you're running a batch erase and one of the disks has errors, the erase process for ALL the disks in the batch will be terminated.

Abort only failed disk from group processing

This is the suggested setting. Failed disks will return an error and terminate the erase process, but other disks in the batch will not be interrupted from completing the erase operation.

Ignore error for disk grouping

Ignores the read/write error and continues erasing wherever is possible on the disk. No active or forth going operations are terminated.

Additional settings:

Terminate process after number of errors

Sets the error threshold to a certain amount before the disk operation is terminated and deemed unsuccessful.

Number of Read/Write attempts

Sets the number of attempts KillDisk make to perform an operation when an error is encountered.

Sectors to skip after detection of a bad sector

Sets the number of sectors ignored by the software when bad sectors are found.

Do not show Read/Write error messages

Toggle whether or not read/write errors trigger messages to the user.

Use disk lock

Locks disks from being used by any other applications.

Ignore disk lock errors

Errors encountered with KillDisk not being able to access locked disks are ignored.

Ignore read/write errors

Toggle whether errors should appear for read and/or write errors.

Clone preferences

This preferences tab allows you to select a master-copy disk to use for cloning on other disks after they have been erased.

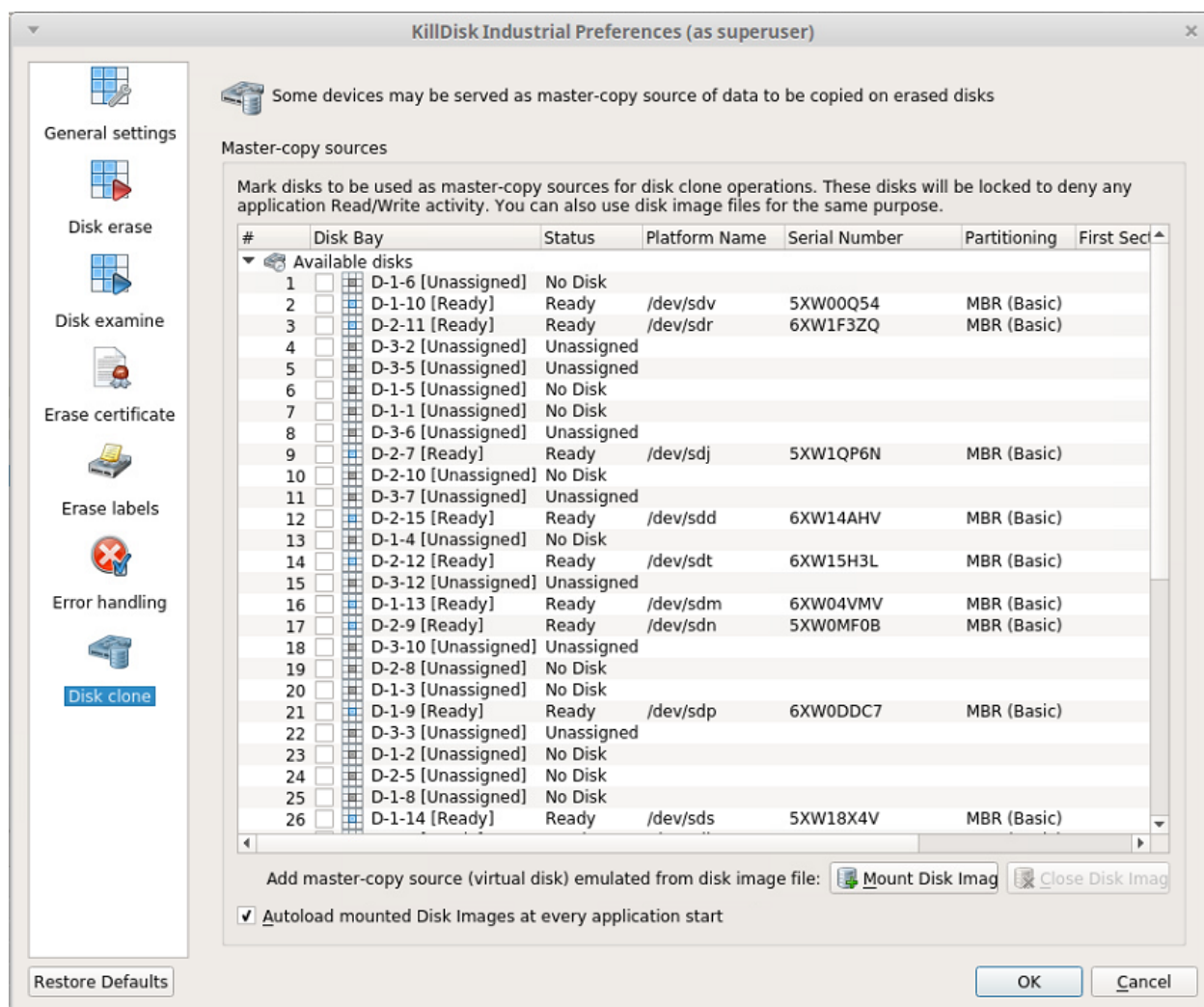


Figure 57: Disk Cloning Preferences

Selecting a Disk for cloning

Any disk recognized by KillDisk may be used as a master-copy for Cloning. Simply find the disk under the "Available Disks" column and check the box next to the desired Disk Bay. This disk will be locked and read/write operations will be restricted from the disk until the cloning operation is complete.

Selecting a Disk Image for cloning

Additionally to cloning from a disk, cloning can be done from a mounted disk image. This is done using the following procedure in the Disk Clone preferences tab:

1. At the bottom of the dialog, click **Mount Disk Image**
2. To the right of the "Disk Image file name field" click the ... button
3. Find the desired disk image in the file explorer and click **Open**
4. Fill in the "Display name" text box with a desired name for the image and click **OK**
5. The mounted disk image should appear under "Disk Images" in the Master-copy sources window. Check the box next to it and



Note: To avoid repeating steps 1-4 above every time the application is launched, check the "Autoload mounted Disk Images at every application start" box. This will complete the mounting process automatically in the future.



Note: Cloning is only available as an operation when working with a Batch of disks, as an option after erasure.

Disk copy options



Note: This feature is only available when working with a Disk Batch, after an erase. Operations on single disks will not be able to use these option.

Copy disk image

When selected, this enables the copy feature. This will copy a disk image from a selected source to all disks that were erased in the batch.

Use file image

Allows you to specify a disk image file to write to the other disks.

Use physical disk

Allows you to specify one disk from the batch to act as the "master disk". This disk will not be erased, but rather be cloned to the other disks in the batch after they are erased.

Start copy to sector

You can specify which sector the copy starts from on the source disks. If you don't know what this is for, leave as 0.

Email Notifications

These settings allow configuring mailer settings for delivering erasing/wiping reports to your mailbox. Simple Mail Transport Protocol (SMTP) is responsible for transmitting e-mail messages and needs to be configured properly.

These options can be configured in the Free version, but are useable only in the Professional version.

Account Type

KillDisk offers you a free SMTP account located on www.smtp-server.com that can be used for sending out reports. By default all required parameters are pre-filled and configured properly. The only field you need to type in is the e-mail address where reports will be sent to. If your corporate policy does not allow using services other than its own, you need to switch this option to Custom Account and configure all settings manually. Ask your system/network administrator to get these parameters.

To

Type the e-mail address where erasing/wiping reports will be sent to.

From

Type the e-mail address which you expect these reports to come from.

SMTP Server

KillDisk offers you the use of smtp-server.com for a free SMTP account. This account is pre-configured for KillDisk users. Ask your system/network administrator to get the SMTP server name to be used in the Custom Account.

SMTP Port

For the free SMTP account, KillDisk allows you to use smtp-server.com on port 80. This is a standard WWW port being used by all web browsers to access the internet. This port most likely will be kept open on a corporate or home network. Other ports can be filtered by and closed on a network firewall. Ask your system/network administrator to set proper SMTP port for the related SMTP server.

SMTP Server requests authorization

To avoid spam and other security issues, some SMTP servers require each user to be authorized before allow sending e-mails. In this case a proper user name and password are required. Ask your system/network administrator to get proper configuration settings.

Disk cloning

In addition to securely erasing hard drives, KillDisk also allows you to write an image or copy a Master Disk to newly erased hard drives with its' cloning feature.

To clone a disk or image to a disk after the erase procedure is completed, navigate to the Disk Copy Options tab in the erase menu, and check the Copy disk image box, as shown below.

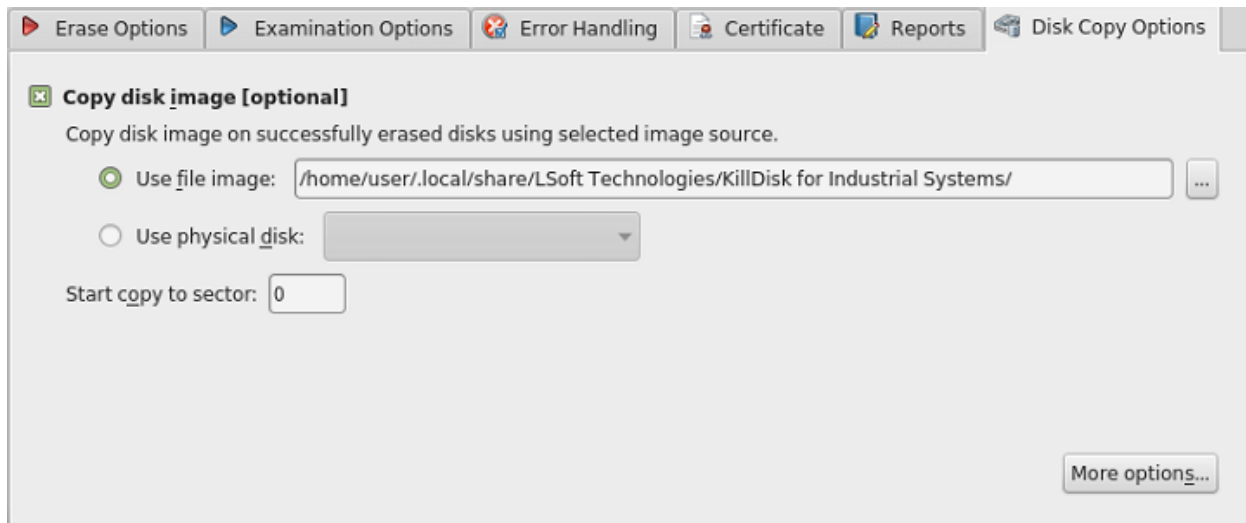


Figure 58: Disk Copy Options Tab

An existing disk image, or physical hard drive can be used as the "Master Copy" to be cloned to the newly erased drive. For additional preferences and configuration of Cloning settings, see [Clone Preferences](#).

1. Navigate to the Disk Copy Options tab in the Erase preferences menu, and check the Copy disk image checkbox.

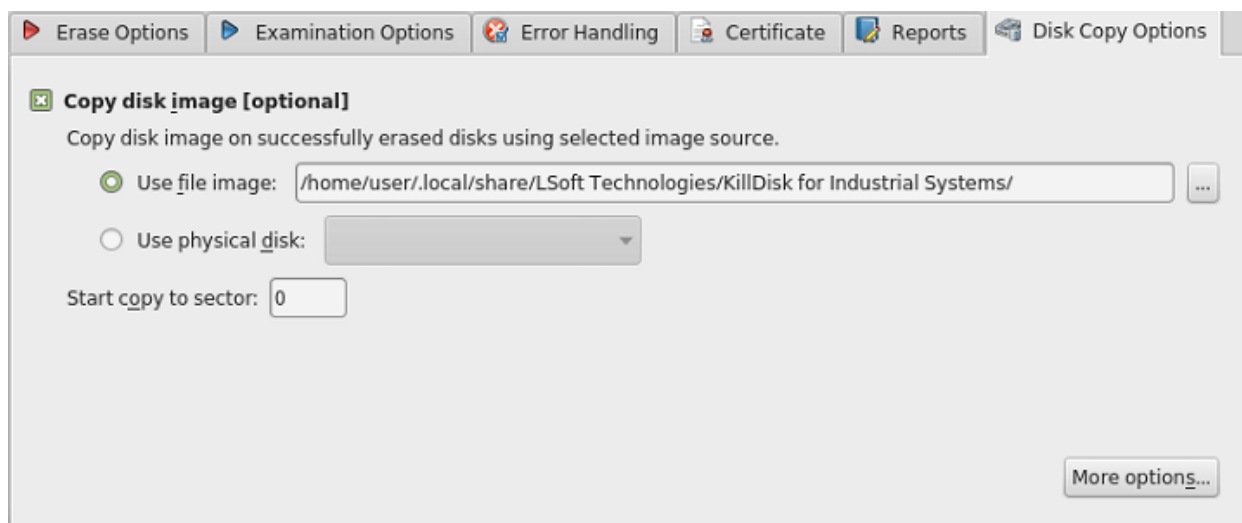


Figure 59: Disk Copy Options Tab

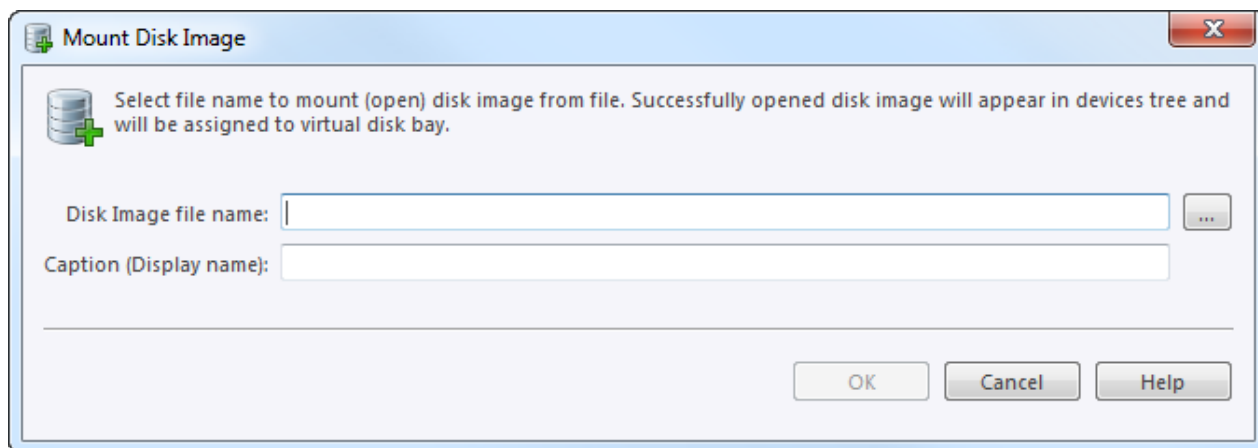
2. Select the disk image source from either an image file or a physical master disk.
3. Specify which sector to start the copy to. If unsure, leave as '0'.

Disk cloning is now configured so that when an Erase operation has completed, the source image/disk will be cloned to the newly erased drive.

Mount Disk Image

To use file as a source of write a physical copy of file contents to one or several disks

1. To open the Open Disk Image dialog, do one of the following:



File name

Disk image file name

Caption

Enter any label to distinguish newly opened (mounted) disk image among other devices and disks.

Figure 60: Mount disk image dialog

2. Confirm and open disk image
Click **OK** to mount Disk Image.

If disk image opens successfully then disk image node appears in **Disk Explorer view** and will be available as clone source in [Clone preferences](#) on page 61 tab and in drop-down list of clone sources in task dialog.

Processing Summary

Once KillDisk's finishes processing any task, such as disk erasure or disk examination, a task complete dialog will appear with a summary of the task, containing all of the information pertaining to the operation. For example, this includes information like disks operated on, status of erasure and all associated certificates and reports.

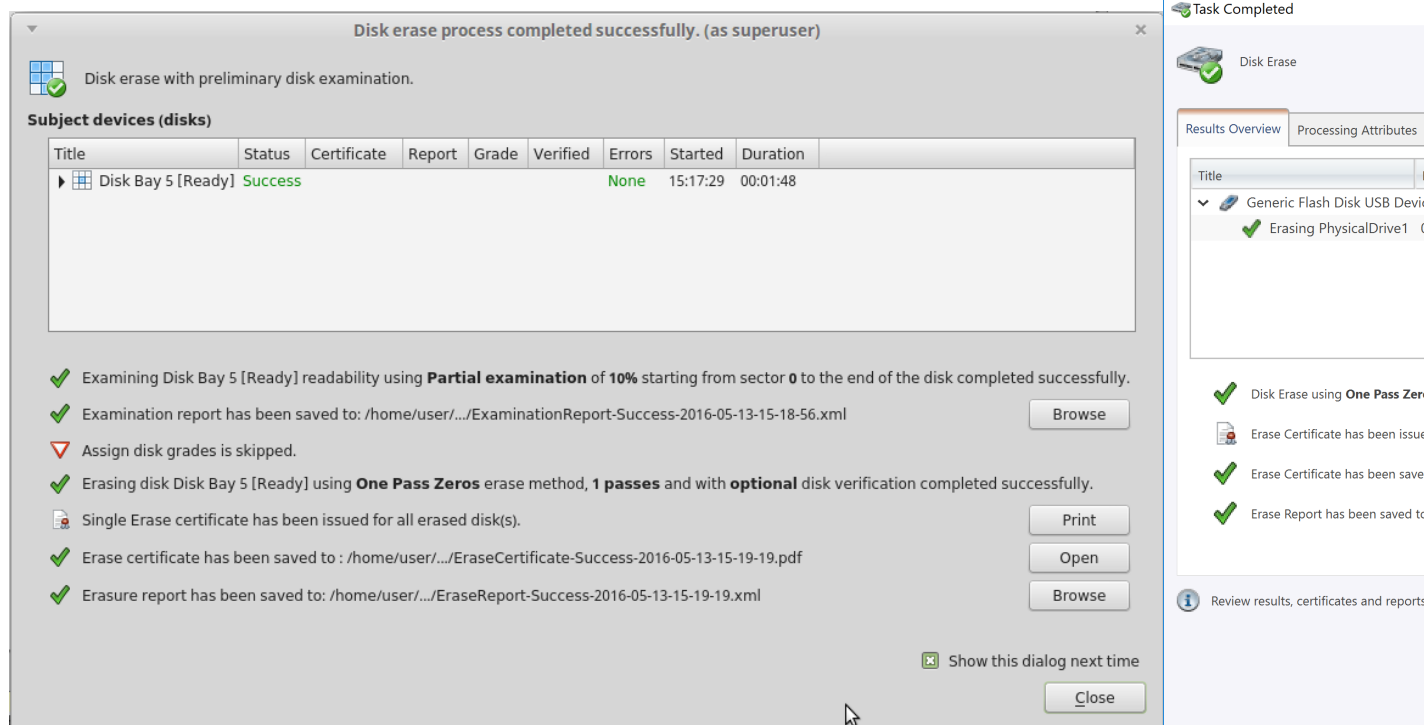


Figure 61: Example of task complete dialog after disk erasure

The successful erasure window contains the features of the successful erasure, discussed further in this section.

Devices

All devices erased are displayed with their erasure status in list format at the top of the notification.

Disk Examination Status

Specifications of the examination procedure are listed and the status of the examination is reported.

Disk Examination Report

Verifies that the examination report has been saved and specifies the path to the saved report. Allows user to examine the .xml examination report by pressing the **Browse** button.

Disk Grade Assignment Status

Confirms the inclusion of the disk grade assignment operation, based on disk integrity examination results.

Erasure Status

Details the status of the disk erase operation showing the erasure specifications and status with which the erasure was completed.

Disk Erasure Certificate

Verifies that the erasure PDF certificate has been saved and specifies the path to the saved report. Allows user to examine the certificate by pressing the **Open** button.

Disk Erasure Report

Verifies that the erasure report has been saved and specifies the path to the saved report. Allows user to examine the .xml erasure report by pressing the **Browse** button.



Note: The Wipe operation will produce a similar processing summary for the disk wipe

Reports and Certificates

KillDisk maintains the highest standards in disk erasure, and with that, provides extensive documentation options for its' operations through [Reports](#) and [Certificates](#). This section will discuss these features in length.

Erase Certificate

Overview

KillDisk provides PDF certificates of erasure upon the completion of data erase operations. These certificates may be customized to include company-specific information and notes specific to the particular procedure. Configuring these custom settings is outlined in the [Certificate Preferences](#) section of this guide. A sample of the certificate is shown below:

KillDisk for Industrial Systems

ERASE CERTIFICATE

Company information
Business name: **KillDisk for Industrial Systems**

Technician information
Name: **Software user** Date: **April 22, 2016**
Time: **16:21**

Erasure results information
Erase Method: **One Pass Zeros, 1 passes**
Verification: **100%**
Started: **22/04/2016 16:20:47** Duration: **00:00:30**
Status: **Erasing 4 disk(s) process completed successfully.**

Disk
Name: **ATA ST32000542AS** Sectors: **3907029168**
Serial: **5XW1HP2Y** Size: **1.82 TB**
Partitioning: **MBR (Basic)** (2,000,398,934,016 bytes)
Status: **Success** Started: **22/04/2016 16:20:47** Duration: **00:00:30**

System information
OS: **Ubuntu 14.04.2 LTS 3.16.0-38-generic 64-bit**

I hereby state that the data erasure has been carried out in accordance with the instructions given by software provider.

TECHNICIAN

Active@ KillDisk Professional

File Actions View Tools Help

Refresh Erase Disk Wipe Disk File Browser Disk Viewer

PhysicalDrive1
Ready
TS32GSSD370
Serial: C434630270
Type: Fixed Disk, SSD Size: 29.8 GB

PhysicalDrive2
Ready
ADATA SP600
Serial: 2G2620022181
Type: Fixed Disk, SSD Size: 29.8 GB

PhysicalDrive3
Ready
ST3320310CS
Serial: 9TX0887C
Type: Fixed Disk Size: 298 GB

PhysicalDrive4
Ready
WDC WD3200SD-01KNB0
Serial: WD-WCAMR2435935
Type: Fixed Disk Size: 298 GB

ERASE CERTIFICATE

Erasure results information
Device Name: **PhysicalDrive1**
Product Name: **TS32GSSD370**
Serial Number: **C434630270**
Erase Method: **US DoD 5220.22-M, 3**
Verification: **100%**
Erase Range: **Whole disk**
Pass 1 (0x000000000000) - **OK**
Pass 2 (0xFFFFFFFFFFFF) - **OK**
Pass 3 (Random) - **OK**
Verification - **passed OK**

Started: **24/10/2017 11:13:08**
Status: **Disk Erase completed**

Output
11:53:49 AM: Valid
11:39:47 AM: Valid
11:26:29 AM: Valid
11:13:10 AM: Valid
11:13:07 AM: Disk

Figure 62: Disk Erase Certificate.

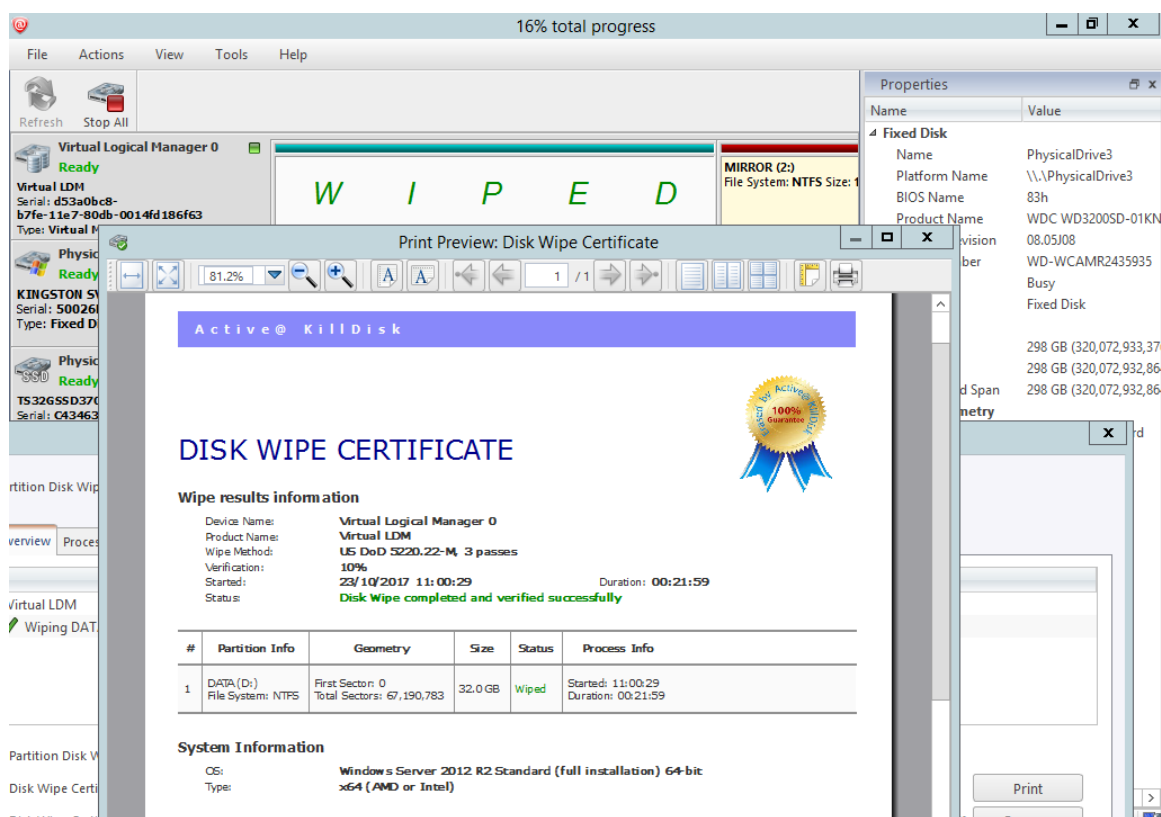


Figure 63: Disk Wipe Certificate

Certificate Elements

Company Information

Displays all company information provided in the preferences. The user in the above example only provided their business name, but other company information may also be included in the certificate.

Technician Information

Displays the technician information provided in the preferences. Namely, this section is for the name of the operator and any notes they may want to include in the certificate report.

Erasure Results Information

Displays information pertaining to the erasure procedure conducted on the hard drive(s). Type of erasure algorithm, custom settings, date and time started and duration of the erasure are all listed here.

Disk

Uniquely identifies the disk that was operated on by the KillDisk application. Includes information like Name, Serial Number, Size and Partitioning Scheme.

System Information

Provides details on the system used to run KillDisk, such as the Operating System and architecture.



Note: The system information here only applies to the system running KillDisk, not the system that was erased by the application! Provided KillDisk remains on one workstation, this information will stay consistent with all systems that the workstation erases.

Reports

KillDisk gives you the option to save XML reports for any major operation it performs on a disk, such as **Examination** and **Erasure**. These reports contain all the information pertaining to the KillDisk procedure. The contents of the report are outlined below.

<p>Company Information</p> <ul style="list-style-type: none"> • Name • License • Location • Phone • Disclaimer <p>System Information</p> <ul style="list-style-type: none"> • OS version • Platform • Kernel <p>Erase Attributes</p> <ul style="list-style-type: none"> • Erase verify • Passes • Method • Verification passes <p>Error Handling Attributes</p> <ul style="list-style-type: none"> • Errors terminate • Skip interval • Number of Retries • Lock Source? • Ignore Write? • Read? • Lock? 	<p>Disks</p> <ul style="list-style-type: none"> • Device Size • Device Type • Serial Number • Revision • Product Number • Name • Geometric Information • Partitioning Scheme <p>Additional Report Attributes</p> <ul style="list-style-type: none"> • Fingerprint Information • Initialize disk? <p>Result</p> <ul style="list-style-type: none"> • Bay • Time and Date Started • Disk Information • Status • Result • Time Elapsed • Errors • Name of operation
---	---

Erase labels (KillDisk Desktop & Industrial only)

Along with the PDF certificate, KillDisk allows you to print labels to place on erased disks with its Print Label features. These labels may be completely customizable to print on any sized sheet with any dimension. Simply specify the parameters and KillDisk will prepare the printable labels for you. The procedure is outlined in this section.

Accessing the Print Labels Option

Upon the completion of a major KillDisk operation, you will see a report dialog. In the list of completed tasks, you will see the `Print Labels` button, depicted below. Click it to enter the Print Label dialog.

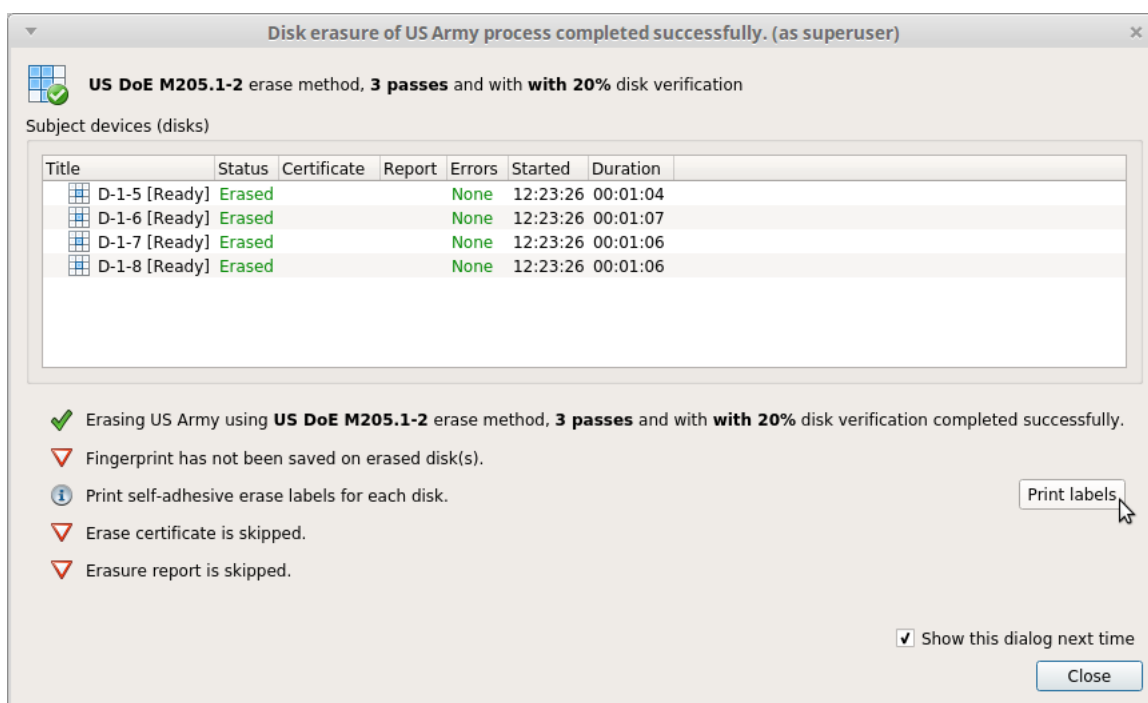


Figure 64: Opening to Print Label dialog.

Print Label dialog

This dialog will allow you to configure the labels and prepare them for printing. The top of the dialog will show you a list of the drives that will have labels generated for them. At any point in the operation, a sample of the label is shown in the Label Preview window on the left side. The right side of the dialog has the styling and template configuration options.

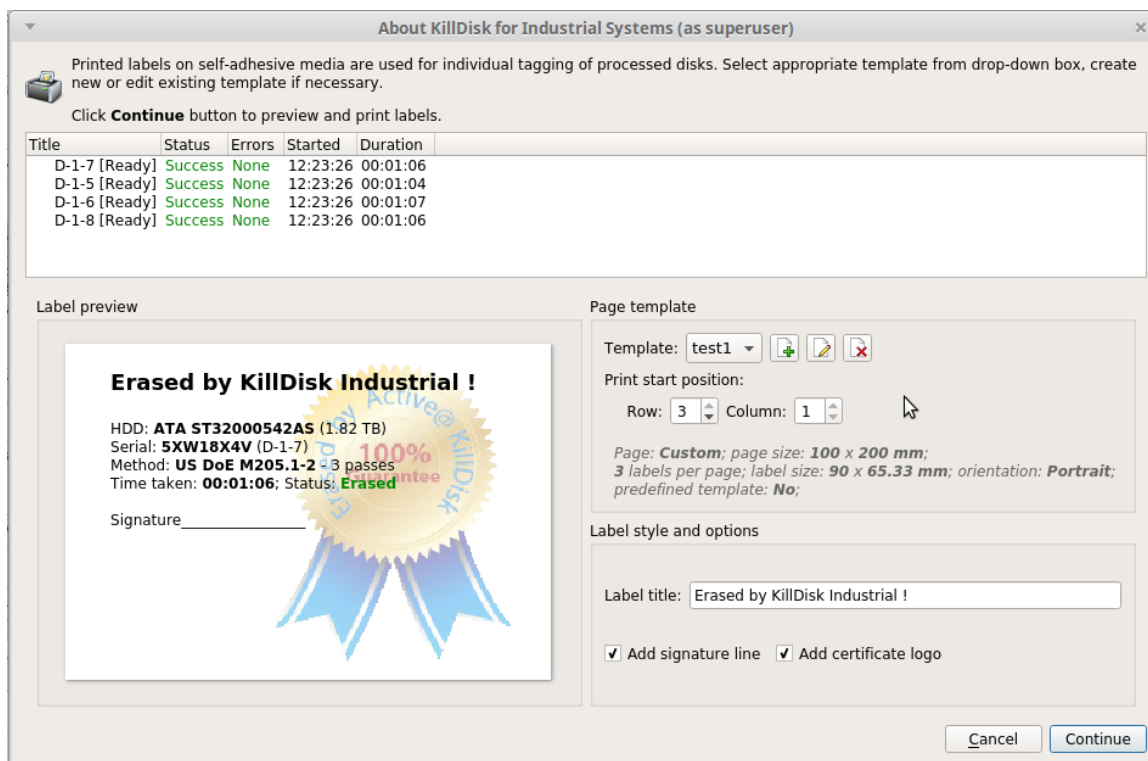






Figure 65: Print label dialog.

Page template options

The print label dialog gives you access to a number of predefined standard templates and any custom templates you may create. These template may be easily selected without opening any additional dialogs and the details of the selected template will be displayed below the selection box. If your specific labels differ from any of the templates

available, the  button allows you to create a custom template with your own specifications. Additionally, the  button allows you to modify an existing template and the  button deletes the selected template.

Creating a new template

Upon clicking the  button, the following template editor window will appear. Descriptions of the template editor options are listed below.

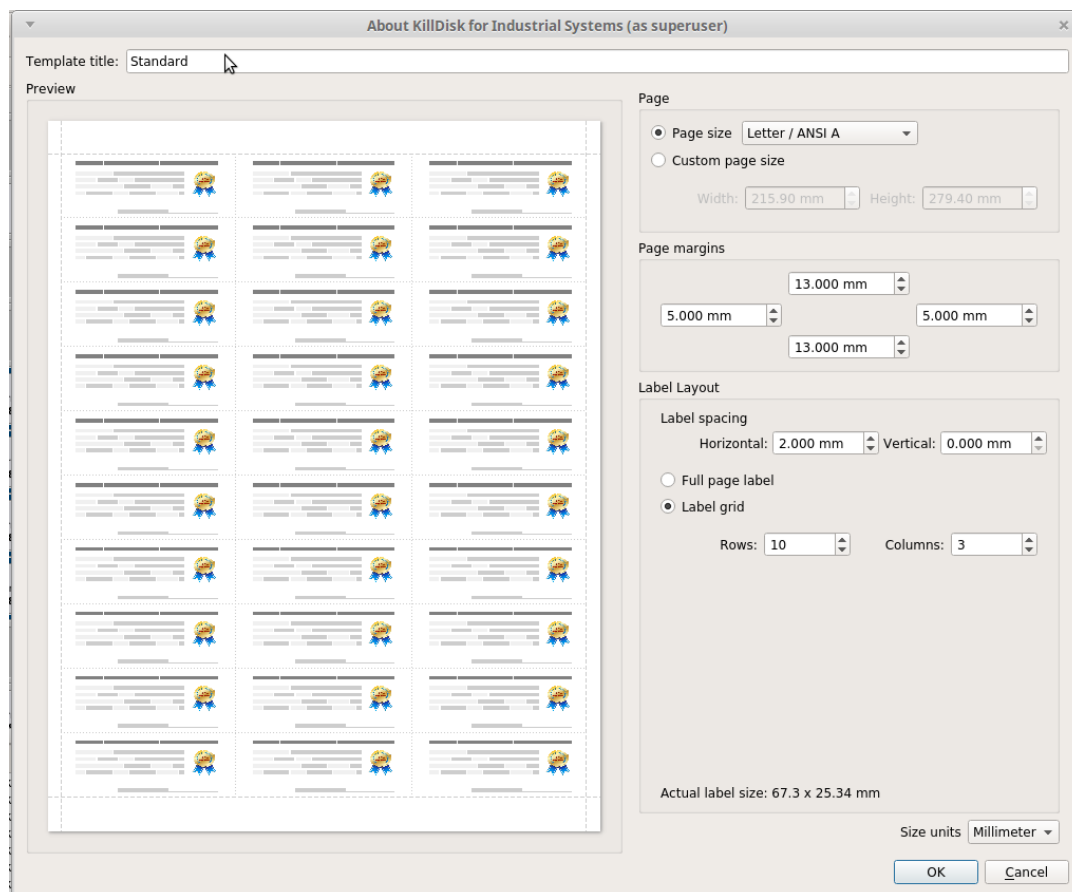


Figure 66: Template editor window.

Template Title

Here you may create a custom title for your template. This is the name that will reference this template when selecting it in the Print Label dialog.

Page

Here you may specify the dimensions of the page used to print the labels. This may be selected from the list of standard sizes, or defined using exact measurements.

Page margins

Here, page margins are defined for the top, bottom, left and right sides of the page.

Label Layout

These settings define how the labels appear on the page. You may define the spacing in between labels on the page and the dimensions of the label grid. Once you've put in the proper measurements, KillDisk will take care of the formatting.

Unit size

The units of measurement may be manipulated between millimeters, inches, pixels and points. If a value is entered in one measurement and the unit size is changed, the appropriate conversion will take place.

Print Start Position

The print start position section of the dialogue allows you to select what label on the page the labels start printing from. As you use labels, the labels won't always start from the 1x1 position, so you can adjust this setting accordingly.

Label Style and options

These options allow you to change the styling on the labels with the following options:

Label Title

Allows you to set a title to be printed in bold at the top of the labels. This can be company name, batch name or any other descriptors you may consider useful to identify the operation.

Add signature line

Toggling this on places a line at the bottom of the label for the technician to sign off on upon completion of the wipe.

Add certificate logo

Includes the logo used in the certificate as a watermark background of the label.

Print Preview and Printing

Once all the settings are configured, you may see the print preview by clicking the `Continue` button. The preview displays what the print is going to look like and from here the print job can be sent to a printer that is configured with the system.

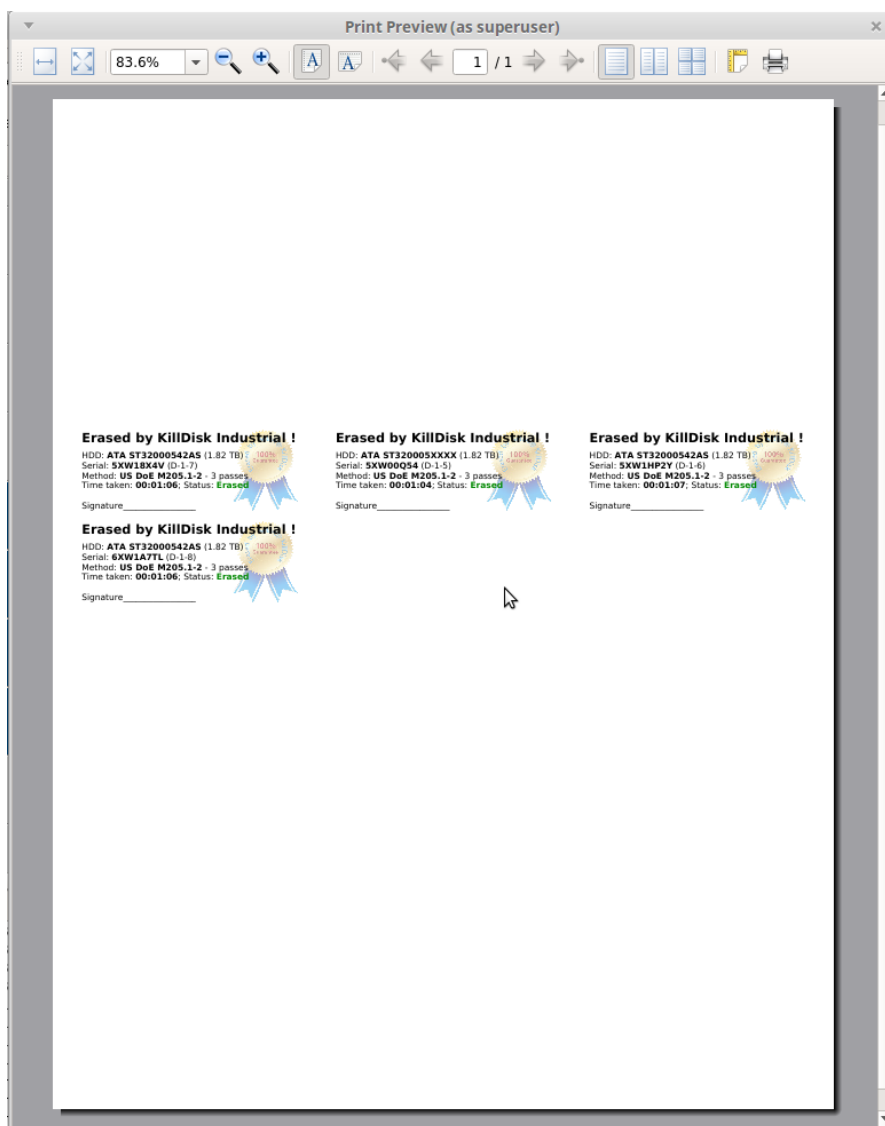


Figure 67: Example of a print preview.

Command Line and Batch Modes

KillDisk can be executed with some settings pre-defined when started from a command prompt with specific command line parameters.

KillDisk can be also launched in fully automated mode (batch mode) which requires no user interaction.

KillDisk execution behavior depends on either command line parameters (highest priority), settings configured in interactive mode and stored in the KILLDISK.INI file (lower priority), or default values (lowest priority).

Command Line Mode

To run Active@ KillDisk in command line mode, open a command prompt screen.

At the command prompt, start Active@ KillDisk for Windows by typing:

```
KILLDISK.EXE -?
```

In Linux environment, type:

```
KillDisk -?
```

A list of parameters appears. You can find explanations of them in the table below.

Table 4: Command Line Parameters

Parameter	Short	Default	Options
no parameter			With no parameter, the Interactive screens
-erasemethod=[0-23]	-em=	2	0 - One pass zeros (quick, low security)
			1 - One pass random (quick, low security)
			2 - US DoD 5220.22-M (slow, high security)
			3 - US DoD 5220.22-M (ECE) (slow, high security)
			4 - Canadian OPS-II (slow, high security)
			5 - British HMG IS5 Baseline (1 pass, quick)
			6 - British HMG IS5 Enhanced (slow, high security)
			7 - Russian GOST p50739-95(slow, high security)
			8 - US Army AR380-19 (slow, high security)
			9 - US Air Force 5020 (slow, high security)
			10 - Navso P-5329-26 RL (slow, high security)
			11 - Navso P-5329-26 MFM (slow, high security)
			12 - NCSC-TG-025 (slow, high security)
			13 - NSA 130-2 (slow, high security)
			14 - German VSITR (slow, high security)
			15 - Bruce Schneier (slow, high security)
			16 - Gutmann (very slow, highest security)
			17 - User Defined Method. Number of passes and Overwrite pattern supplied separately
			18 - NIST 800-88 (1 pass zeroes, quick)
			19 - NIST 800-88 (1 pass random, quick)
			20 - NIST 800-88 (3 pass zeroes, slow, high security)
			21 - Canadian CSEC ITSG-06 (3 passes, verify, slow, high security)
			22 - US DoE M205.1-2 (3 passes, verify)
			23 - Australian ISM-6.2.93 (1 pass random, quick)
-passes=[1 - 99]	-p=	3	Number of times the write heads will pass over a disk area to overwrite data with User Defined Pattern. Valid for User Defined Method only

Parameter	Short	Default	Options
-verification=[1 - 100]	-v=	10	Set the amount of area the utility reads to verify that the actions performed by the write head comply with the chosen erase method (reading 10% of the areaby default). Verification is a long process. Set the verification to the level that works best for you
-retryattempts=[1 - 99]	-ra=	2	Set the number of times that the utility will try to rewrite in the sector when the drive write head encounters an error
-erasehdd=[0,1..63]	-ch=		Number in BIOS of the disk to be erased. First physical disk has a zero number. In Linux first disk usually named /dev/sda. In Windows Disk Manager first disk is usually named Disk 0. On older systems (DOS, Windows 9x) first disk is usually named 80h (obsolete syntax is still supported in the parameter)
-eraseallhdds	-ea		Erase all detected disks
-excluderemovable	-xr		Exclude all removable disks from erasing when erase all disks selected
-exclufixed	-xf		Exclude all fixed disks from erasing when erase all disks option selected
-excludedisk=[0,1..63]	-xd=		Exclude disk from erasing when erase all disks option selected
-ignoreerrors	-ie		Do not stop erasing each time a disk error is encountered. When you use this parameter, all errors are ignored and just placed to the application log
-initdisk	-id		Initialize disk(s) after erase
-fingerprint	-fp		Initialize disk(s) and write fingerprint to the disk's first sector
-computerid	-ci		1 - Display BIOS ID on the certificate
			2 - Display Motherboard ID on the certificate
-clearlog	-cl		Use this parameter to clear the log file before recording new activity. When a drive is erased, a log file is kept. By default, new data is appended to this log for each erasing process. By default the log file is stored in the same folder where the software is located
-exportlog	-el		Export a log file as XML report
-logpath=["fullpath"]	-lp=		Path to save application log file. Can be either directory name or full file name. Use quotes if full path contains spaces
-certpath=["fullpath"]	-cp=		Path to save erase/wipe certificate. Can be either directory name or full file name. Use quotes if full path contains spaces
-inipath=["fullpath"]	-ip=		Path to the configuration file (KILLDISK.INI) for loading the advanced settings. See table below
-noconfirmation	-nc		Skip confirmation steps before erasing starts. By default, confirmation steps will appear in command line mode for each hard drive as follows: Are you sure?
-beep	-bp		Beep after erasing is complete
-wipeallhdds	-wa		Wipe out unallocated space on all recognized volumes located on all detected disks

Parameter	Short	Default	Options
-wipehdd = [0,1...63]	-wh=		Wipe out unallocated space on the disk specified by BIOS number
-test			If you are having difficulty with Active@ KillDisk, use this parameter to create a hardware information file to be sent to our technical support specialists
-batchmode	-bm		Execute in batch mode based on command line parameters and INI file settings (without user interaction, all operations being stored to log file)
-userpattern =["fullpath"]	-u		File to get user-defined pattern from. Applied to User Defined erase method. Each line in the file corresponds to the particular pass pattern
-shutdown	-sd		Save log file and shutdown PC after completion
-nostop	-ns		Prevent erase/wipe stop action
-help or -?			Display this list of parameters



Note: Parameters -test and -help must be used alone. They cannot be used with other parameters.



Note: Commands -erasehdd, -eraseallhdds, -wipehdd and -wipeallhdds cannot be combined.

Type the command and parameters into the command prompt console screen at the prompt. Here is a Windows example:

```
killdisk.exe -eh=80h -bm
```

The same in Linux:

```
KillDisk -eh=80h -bm
```

In the example above, data on device 80h will be erased using the default method (US DoD 5220.22-M) without confirmation and returning to the command prompt screen when complete.

Here is another Windows example:

```
killdisk.exe -eh=80h -nc -em=2
```

The same in Linux:

```
KillDisk -eh=80h -nc -em=2
```

In this example, all data on the device 80h will be erased using US DoD 5220.22-M method without confirmation and showing a report at the end of the process.



Note: In Linux environment, to detect and work with physical disks properly, Active@ KillDisk must be launched under SuperUser account, so, if you are not a Super User, you should type a prefix sudo, or su (for different linux versions) before each command.

After you have typed KillDisk and added command line parameters, press ENTER to complete the command and start the process.

Information on how drives have been erased is displayed on the screen when the operation has completed successfully. KillDisk execution behavior depends on either command line parameters (highest priority), settings configured in interactive mode and stored in the KILLDISK.INI file (lower priority), or default values (lowest priority).

Batch Mode



Note: This feature is intended for advanced users only

Batch mode allows KillDisk to be executed in fully automated mode without any user interaction. All events and errors (if any) will be placed in the log file. This allows system administrators and technicians to automate erase/wipe tasks by creating scripts (*.CMD, *.BAT files) for different scenarios that can be executed later on in different environments.

To start KillDisk in batch mode, add the `-bm` (or `-batchmode`) command line parameter to the other parameters and execute KillDisk either from the command prompt or by running a script.

Here is an example of batch mode execution with the wipe command:

```
KillDisk -wa -bm -em=16
```

This will, using Gutman's method and returning to the command prompt when complete, wipe all deleted data and unused clusters on all attached physical disks without any confirmations

If `-ns` (`-nostop`) command line parameter is specified, no user interaction is possible after erase/wipe action started, so user cannot cancel the command being executed.

After execution, application returns exit codes to the operating system environment: 0 (zero) if all disks being erased successfully, 1 (one) if errors occurred or nothing erased/wiped, and 2 (two) if minor warnings occurred.

Disk batches

Disk batches are used to organize disks into groups, depending on what the disks are being used for, type of disk, or the desired operation to be performed on them. The user has complete freedom to use disk batches however is most convenient for their particular use case. Disks can be added or removed from a particular batch at any time.

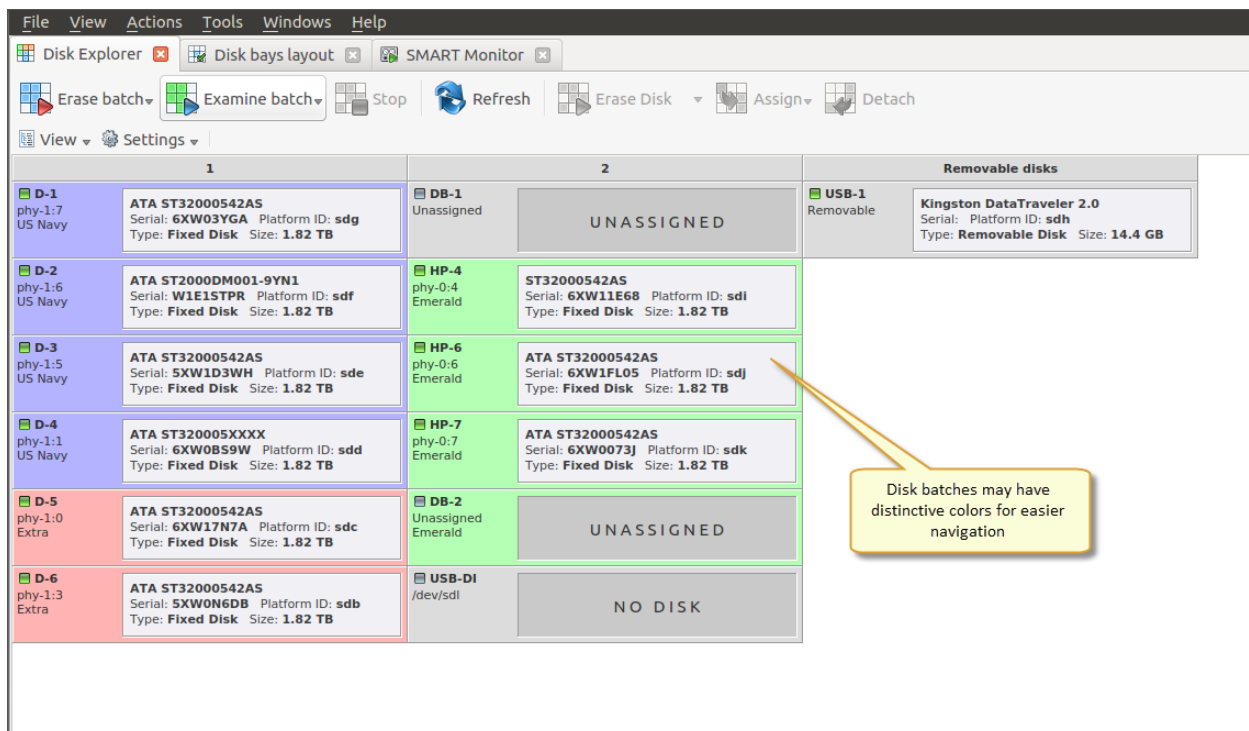


Figure 68: Batch control toolbar

Once disks are batched together, they may be treated as a group and similar settings may be set for this batch. Likewise, operations may be performed on these batches — initiating the operation on a batch will perform the operation on all the disks belonging to the batch.

Using disk batches

Create a disk batch

Disk batches are created using the **Batch Control tool**.



Note:

If you can't find the Batch Control toolbox when you run KillDisk, make sure that you have the view activated. To do this, navigate to the file menu bar, click **View > Batch Control**. There should be a check mark next to the Batch Control view.

In the Batch Control toolbar, click **New**. This will open the batch settings window. After [configuring the batch settings](#), click **OK** in the bottom of the edit window and the new batch will appear in the batch control window.

Adding disks to a disk batch

Available disk bays can be added to existing disk batches in [several ways](#).

Removing disks from a disk batch

Disks are removed from a batch in a very similar way to the way they are attached. Follow the same steps as with Adding disks, only select bays that are attached to batches and select the **Detach** command.

Deleting batches

Batches can be deleted by selecting the batch in the Batch control toolbar and selecting the **Delete** command.

Edit batch attributes

Batch attributes can be edited at any time after batch created. See: [Edit disk batch attributes](#) on page 80



Note:

Disk batch attributes changed every time if altered in confirmation dialog before executed.

Add disk bays to disk batch

Disk bays can be assigned to existing disk batches in order to apply same batch attributes for selected tasks (disk examination, erasure, etc).



Note:

Single disk bay can belong only to one disk batch at the same time.

Once a new batch is created, a new message will appear at the top of the Disk Bays view of the Disk Explorer window, prompting you to add disks to the new batch.

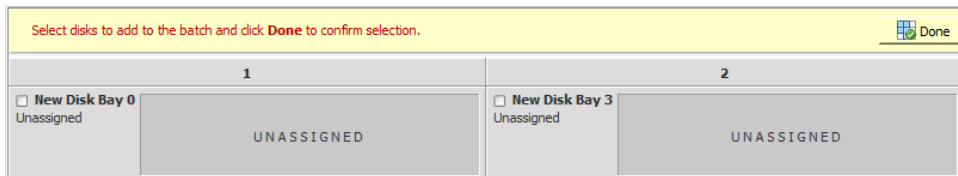


Figure 69: Adding disks to a batch in the disk bays view

Click on disks to select them and/or click on selected disk to remove them from the batch disk selection. Once the desired disks are selected, click **Done** in the message toolbar and the selected disks will be added to the new batch.

Alternatively, disks can be added to a batches in one of several ways:

From Batch control toolbar

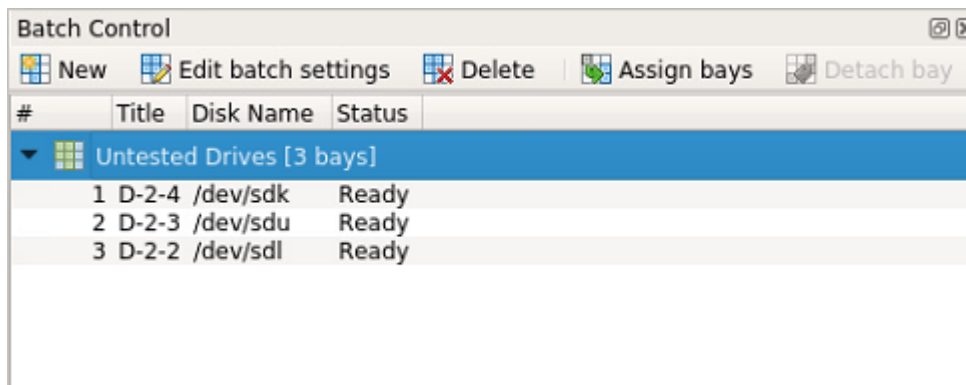


Figure 70: Batch control toolbar

1. Navigate to the Batch control toolbar

2. Click the **Assign** button at the top of the toolbar
3. Select the bays in the Disk Bays view and click **Done**.

In Disk Bays view

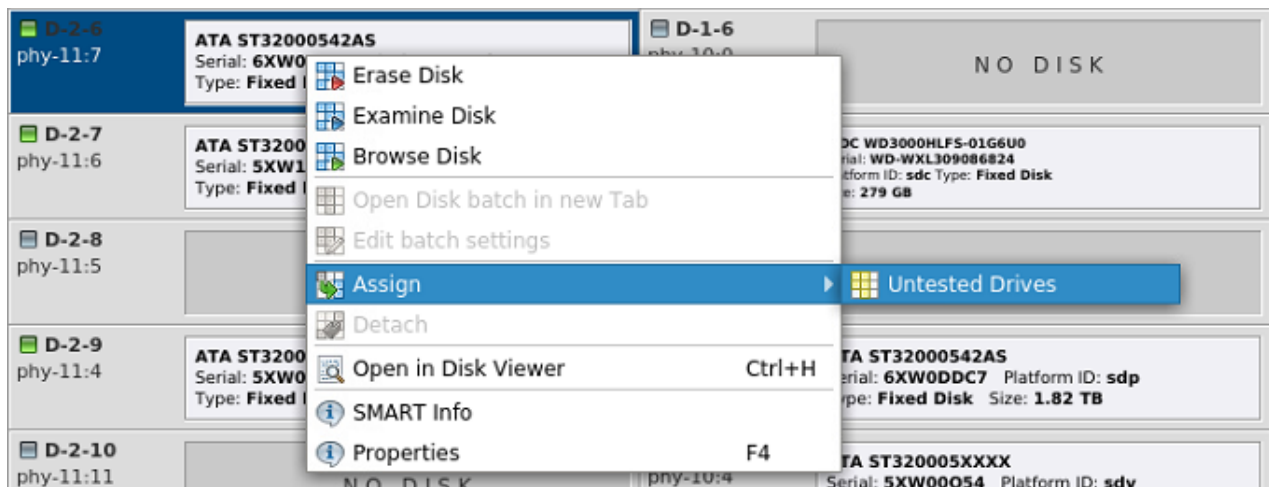


Figure 71: Batch control through the disk bays view

1. In the disk bays view, select the disk(s) that you'd like to place in a batch.
2. Right-click on the disk.
3. Hover over the **Assign** option to see a list of available batches.
4. Select the desired batch from the list to place the selected disk into.

From main file menu bar

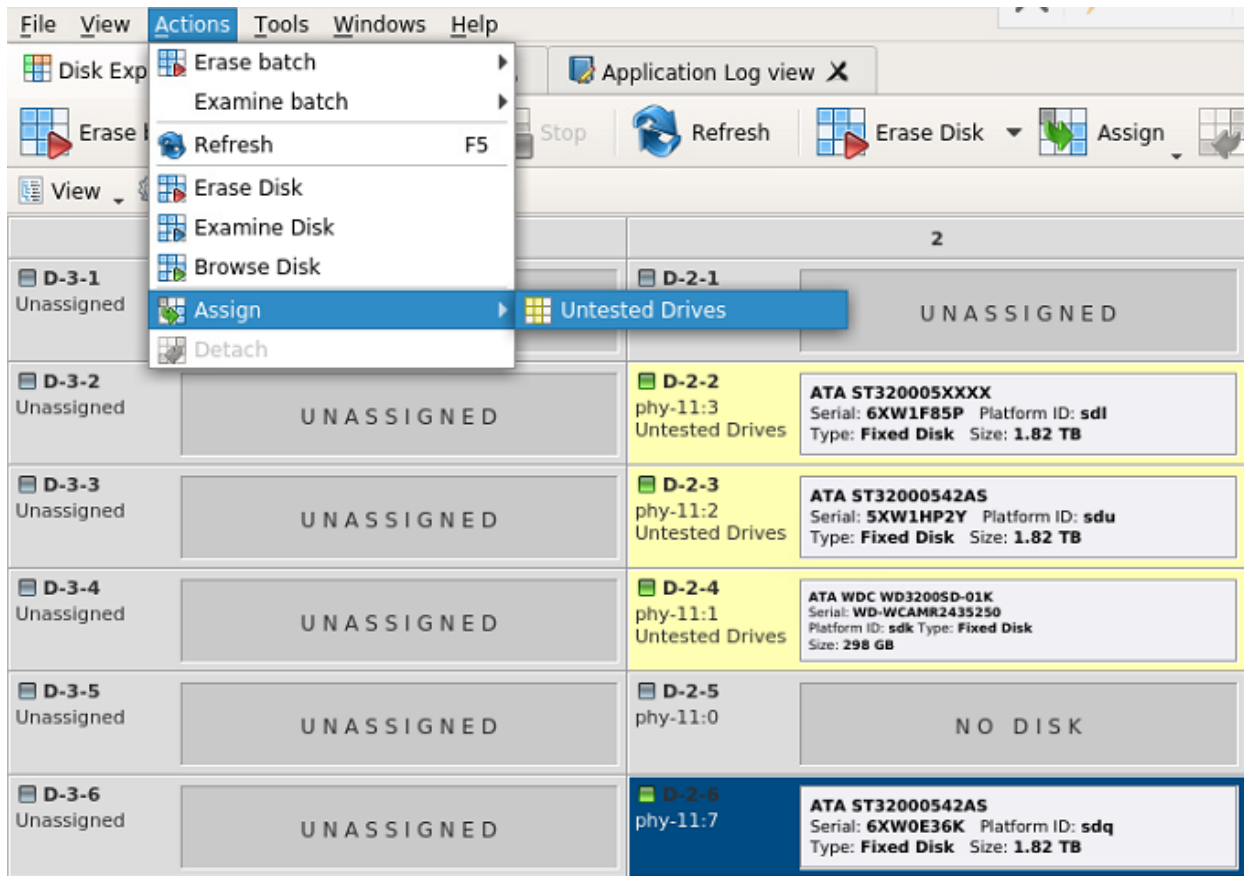


Figure 72: Batch control through the file menu bar

1. In any view of the Disk Explorer, select the disk bay(s) that needs to be assigned
2. In the File menu bar, select the **Action**.
3. Hover over the **Assign** action to see a complete list of available batches.
4. Click on the desired batch. The selected bay(s) will be assigned to that batch.

Edit disk batch attributes

When you create a new disk batch, you will encounter the Edit disk batch window, where disk batch settings may be set. For existing disk batches, you may access this window by selecting the desired batch in the Batch control tool and clicking **Edit batch settings**.

General attributes

These are general settings for the batch, such as Name, color, how the batch is displayed, and more.

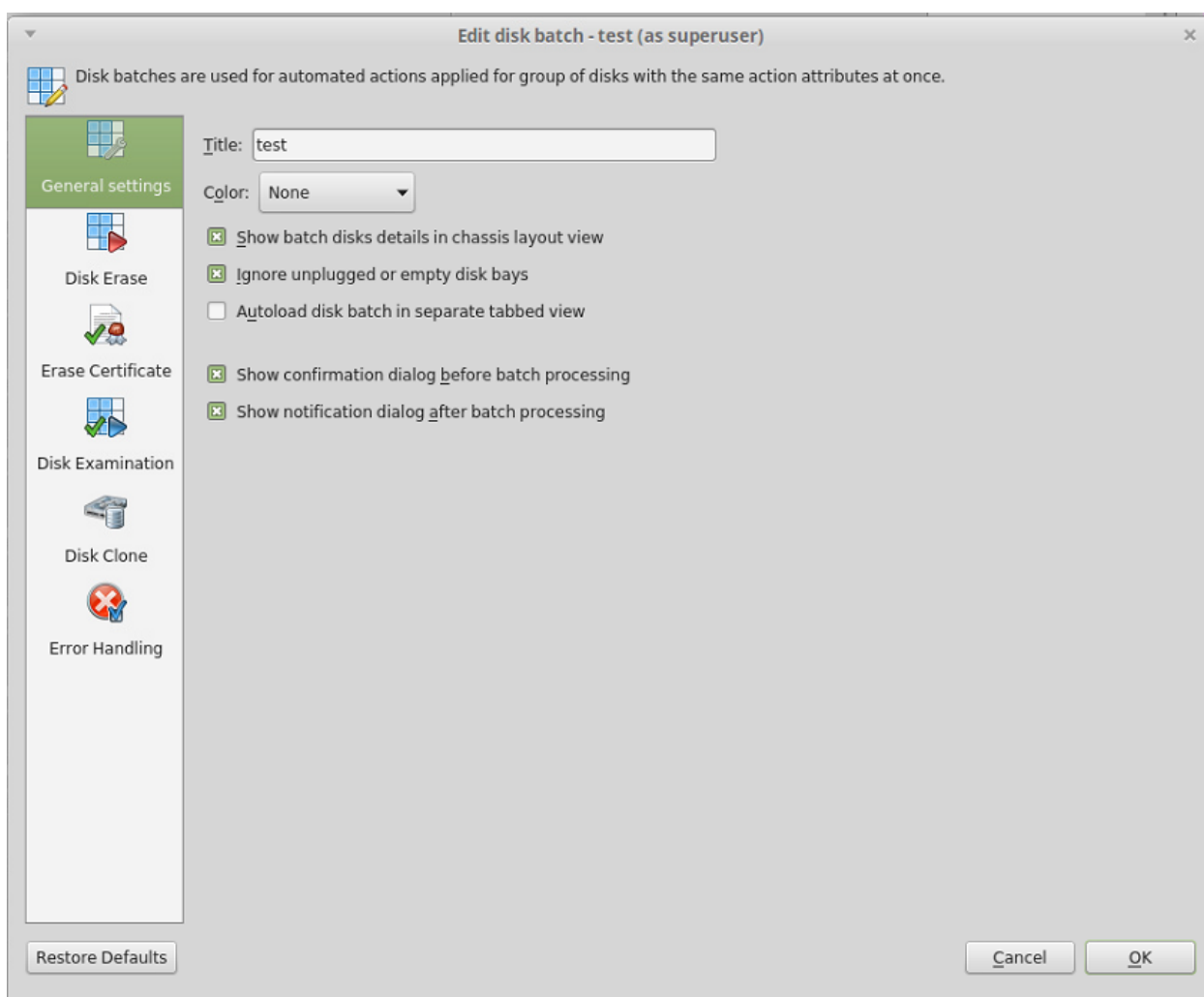


Figure 73: Batch editor 'General' tab

Disk Erase

These settings configure the disk erase settings for the batch. Erase methods, verification, and report settings can be changed here. Additionally, [KillDisk Preferences](#) can be individually configured here by selecting **More options....**

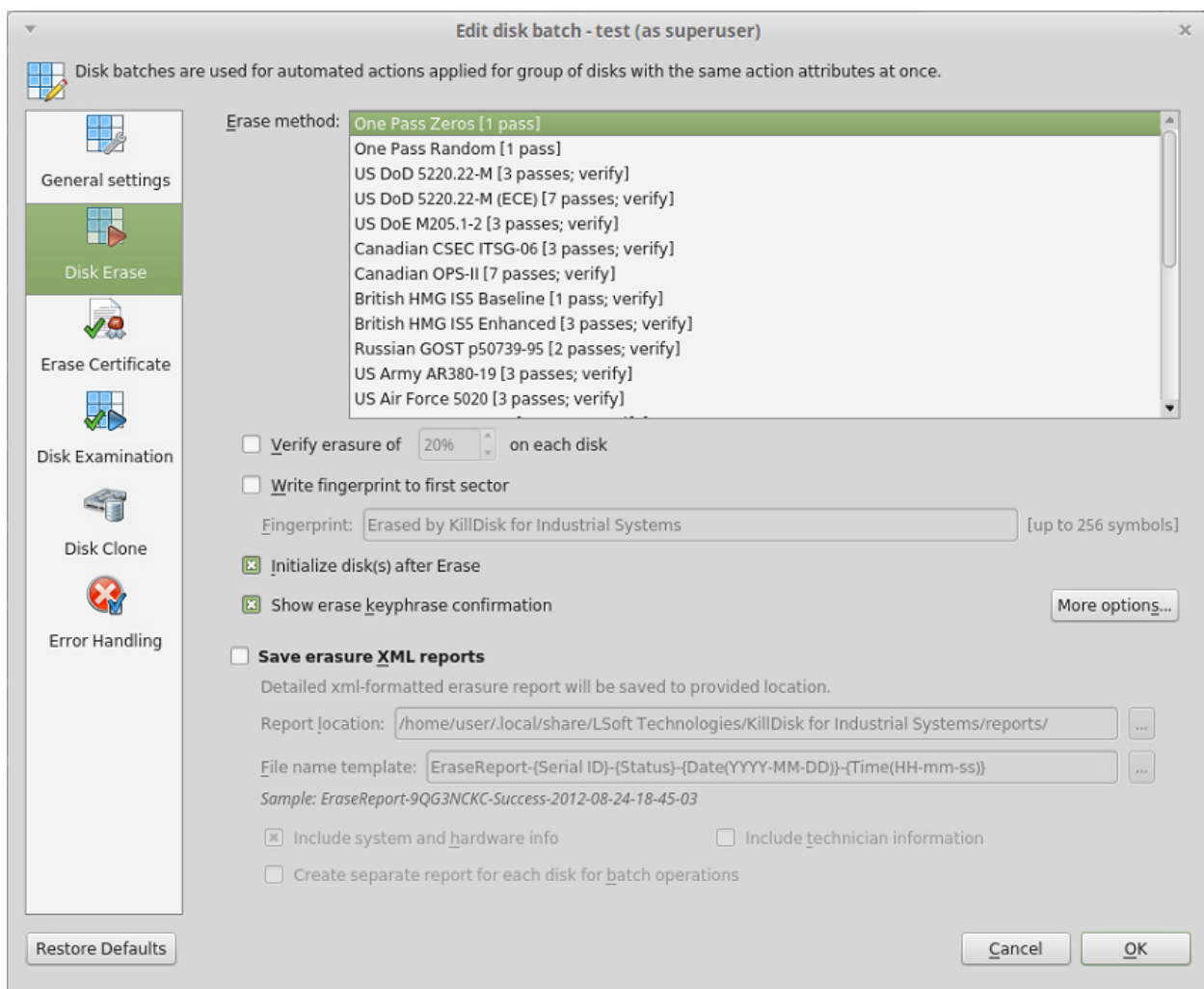


Figure 74: Batch editor 'General' tab

Erase Certificate

These settings give you the option to toggle whether or not to issue an erasure certificate upon erase and configure the settings for this, like name, destination, details and comments. Additional configurations can be made to the certificate through the [Certificate preferences](#).

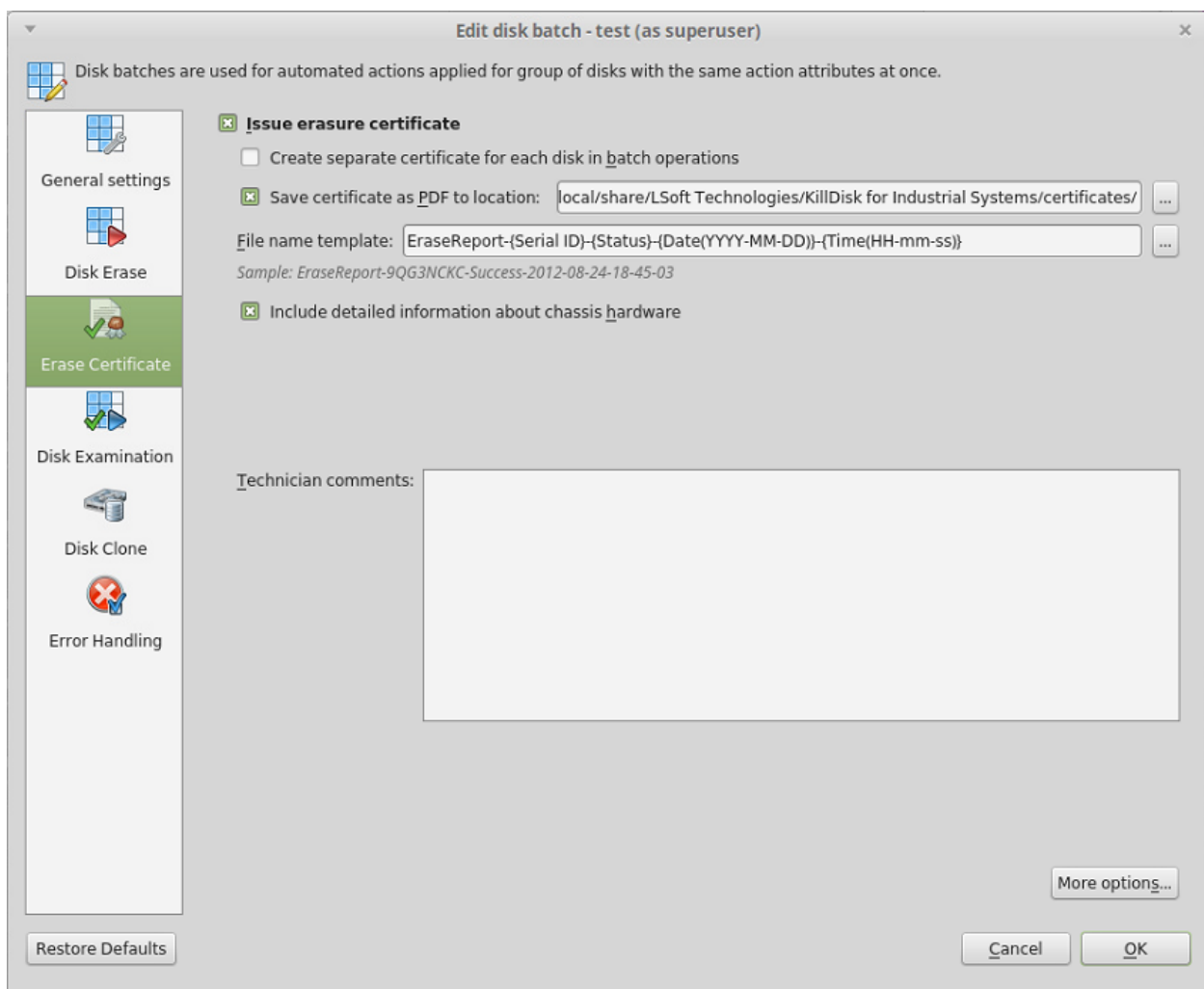


Figure 75: Batch editor 'General' tab

Disk Examination

These settings allow you to configure the optional Disk Examination feature, toggling it on/off, method of examination, setting disk integrity thresholds and how these reports are saved.

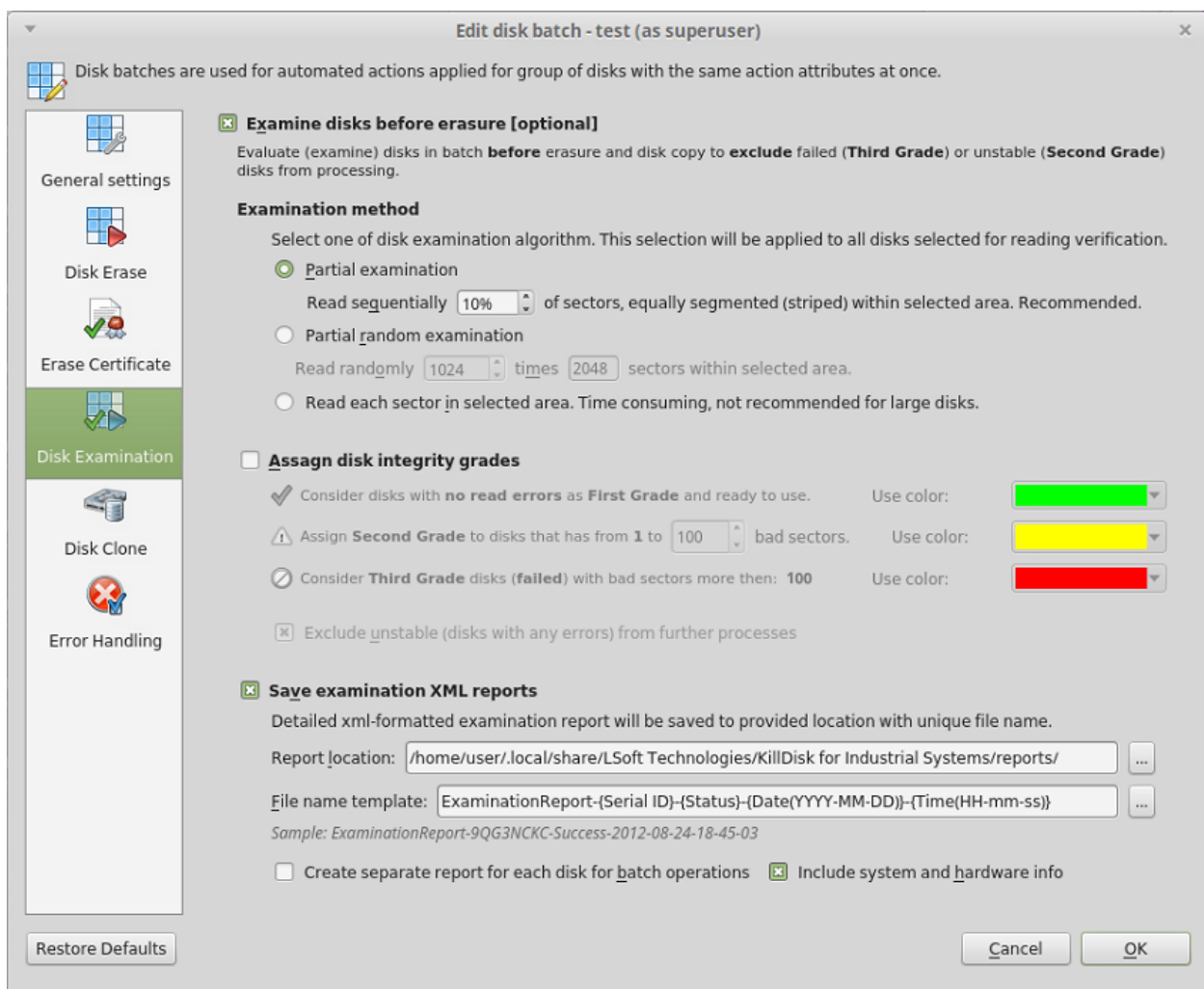


Figure 76: Batch editor 'General' tab

Disk Clone

This feature allows the user to configure either a disk or disk image to write to all the disks in the batch.

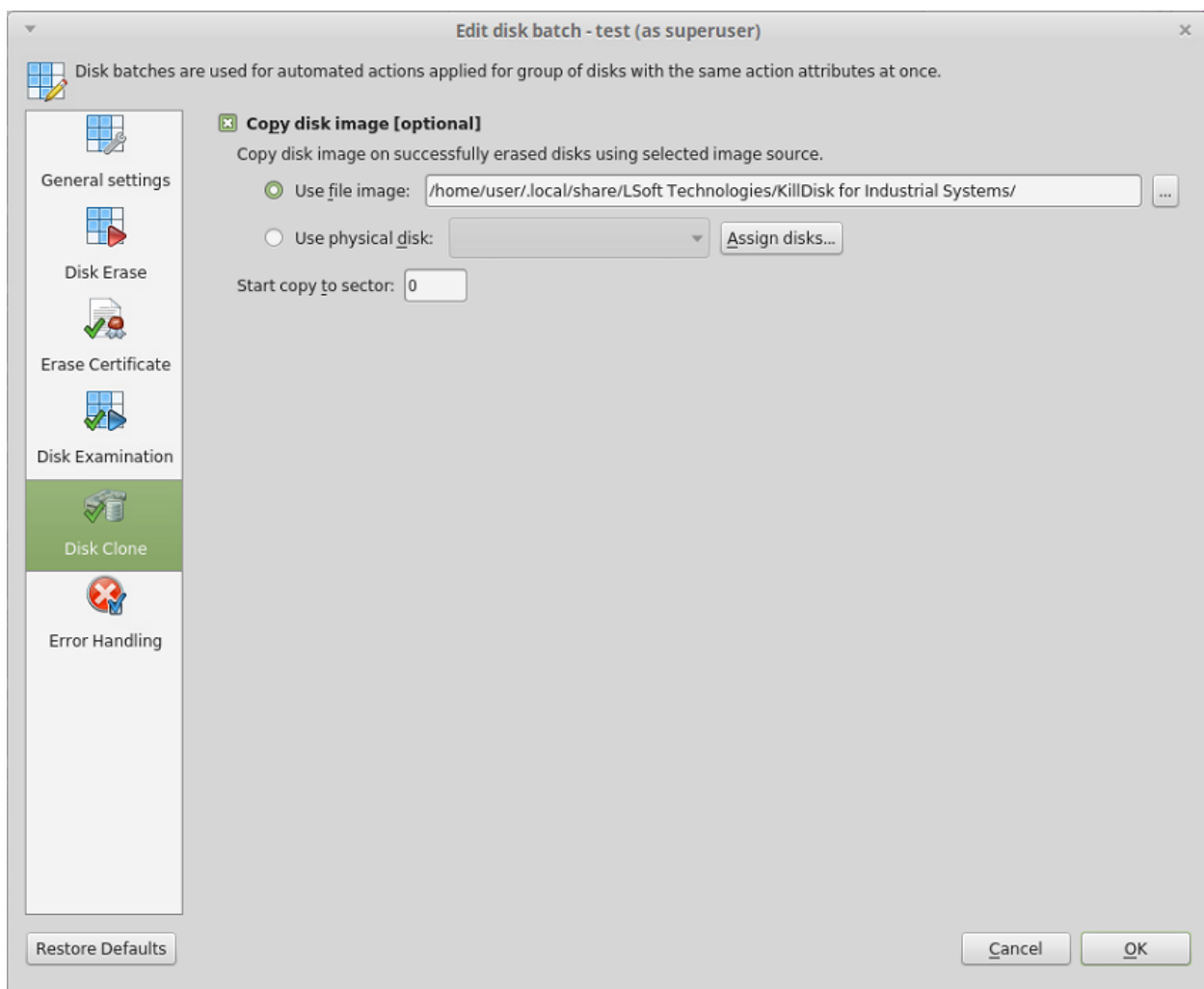


Figure 77: Batch editor 'General' tab

Error Handling

For each batch error handling attributes can be set individually.

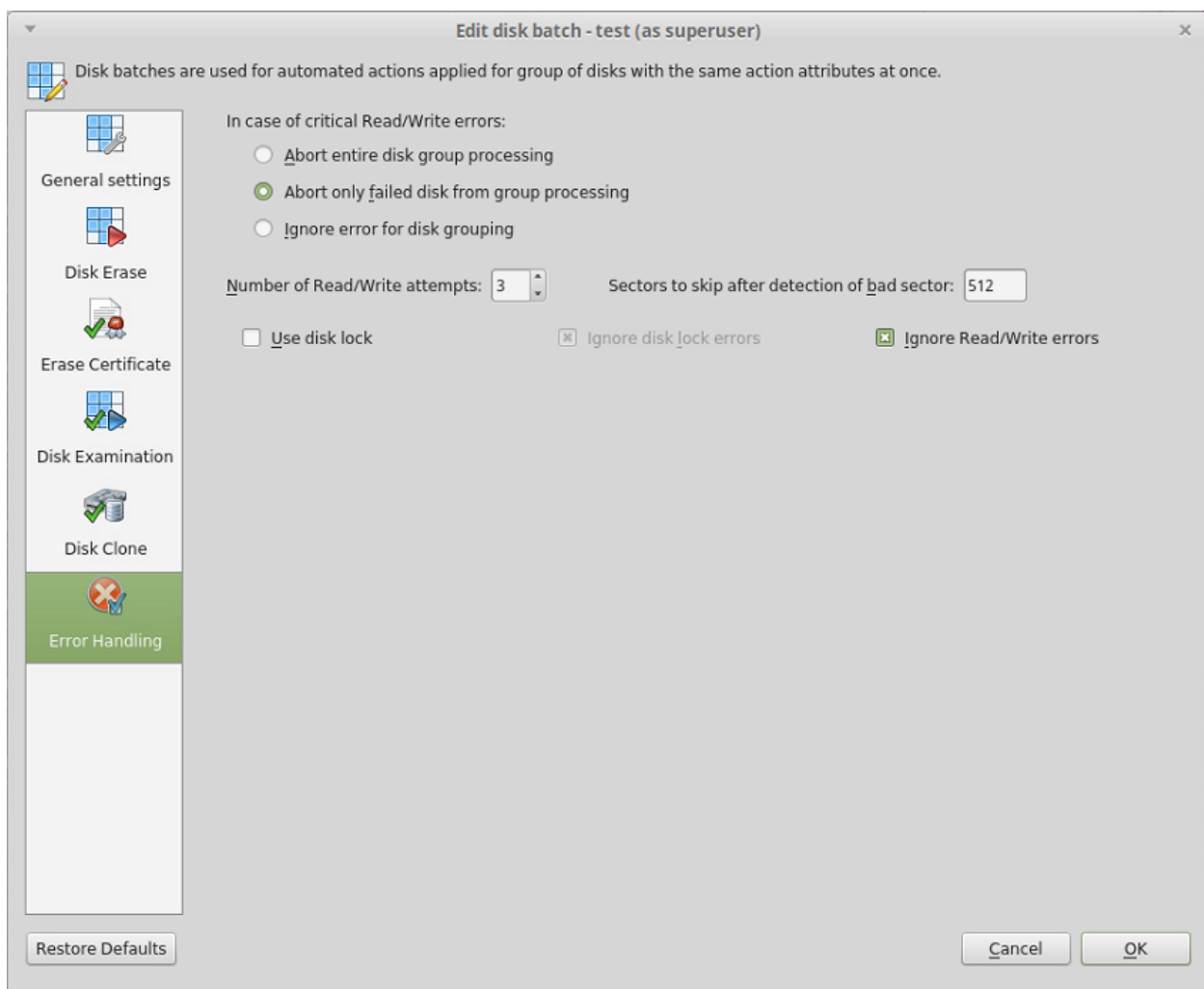


Figure 78: Batch editor 'Error handling' tab

Read [Error Handling](#) on page 60 for description of each attribute.

Advanced Tools

KillDisk offers a number of advanced tools to work in conjunction with the software to make operations easier to perform and the disks easier to navigate. KillDisk give you the power to browse through disks on both a file level and a low, HEX level, as well as analyze disk health with its' SMART monitor. This section describes each of these features at length:

- [File Browser](#)
- [Hexadecimal Viewer](#)
- [SMART monitor \(Industrial only\)](#)

File Browser

KillDisk also includes a built-in file browser for examining the contents of disks for verification purposes of the procedure and that correct hard drives are being selected, and validation that erased files have been overwritten after erase and wipe. Details on using this feature will be discussed in this section.



Note: KillDisk **will** detect files that have been deleted, but not sanitized. They will appear grey and indicate deleted files with a high probability of being recovered with file recovery tools.

Opening the browse view

To browse the contents of a specific disk from the Disk Bay layout view, simply select the desired disk and click **Browse Disk** in the action toolbar. This action can be found in the disk action list shown below.

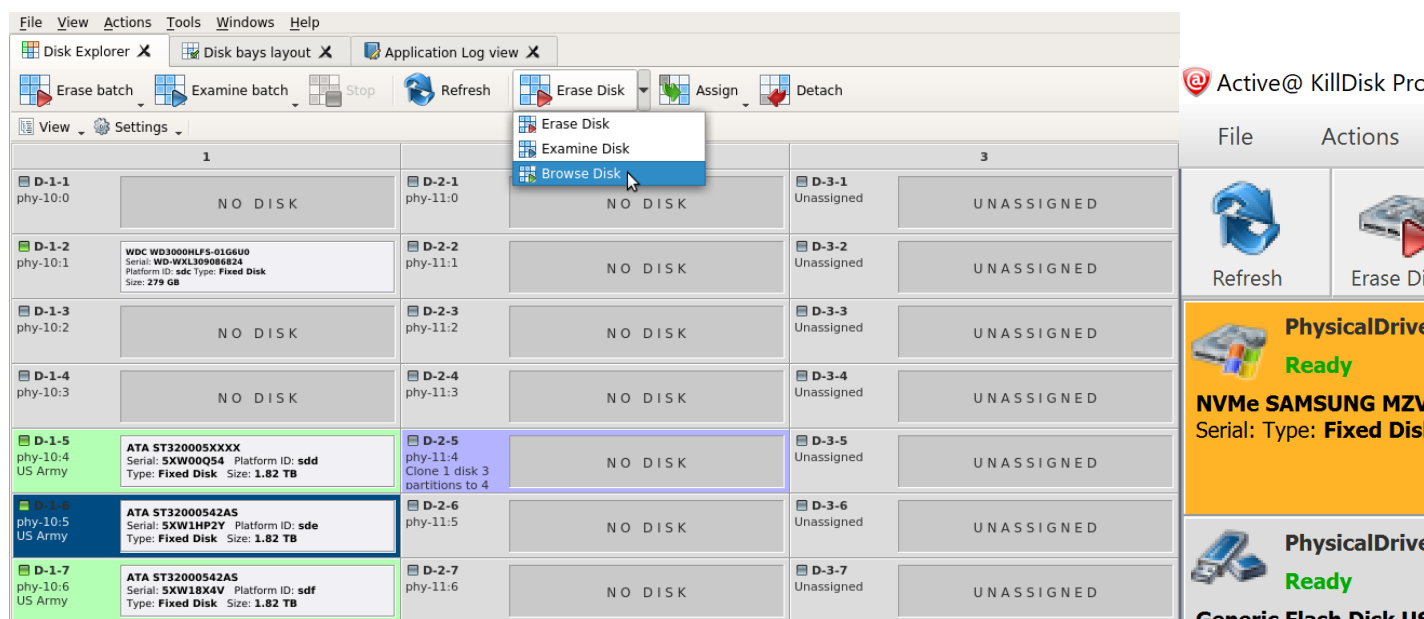


Figure 79: Launching the file browser

This will launch the file browser window, seen below.

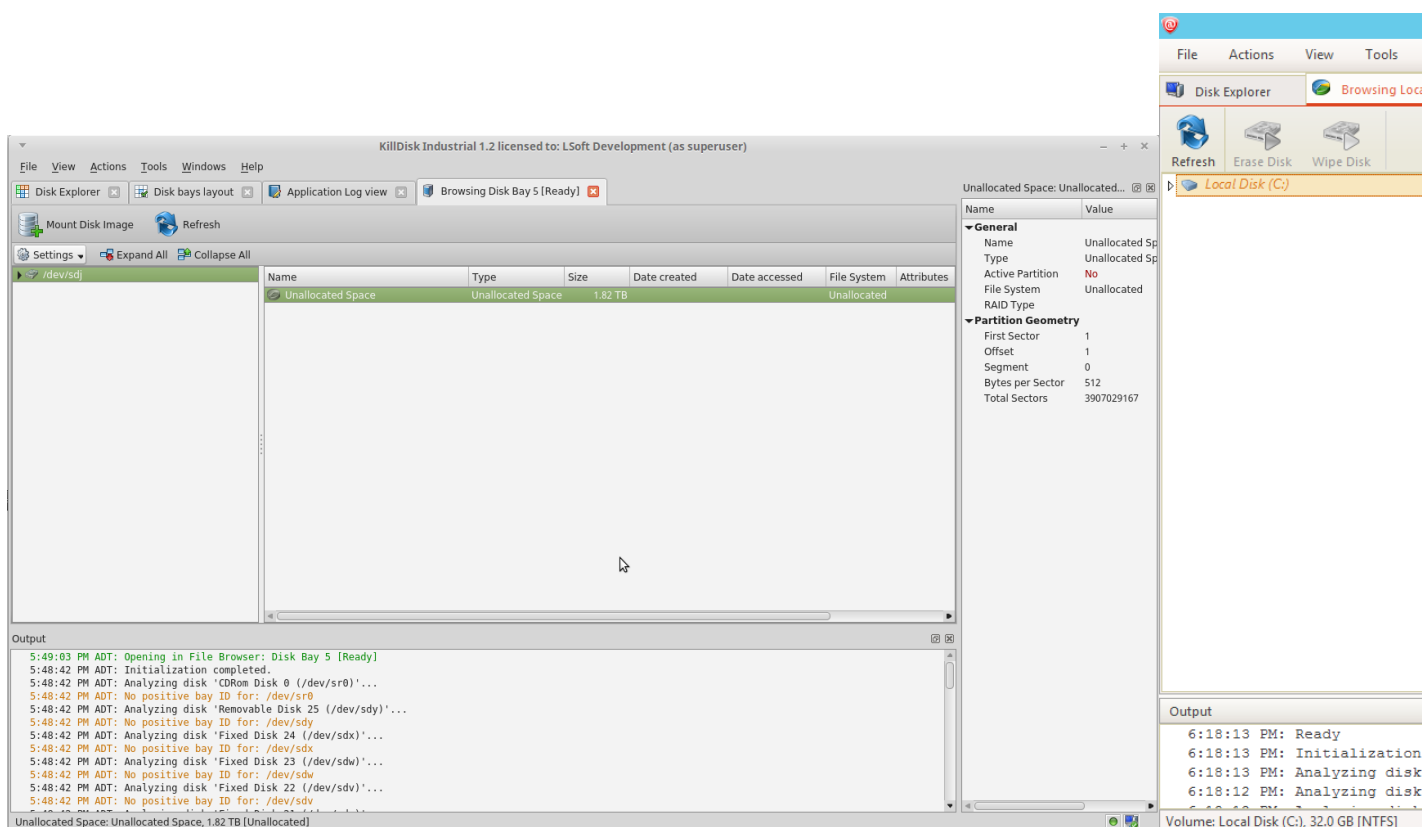


Figure 80: File Browser window

The file browser window displays the disk selected. The **Expand All** button at the top left expands all the partitions on the disk in the Navigator Pane, while the **Collapse All** button hides them. The file explorer windowed view may also be manipulated by navigating to the **Settings** button at the top. Here, you can have options to manipulate the elements below.

Advanced

Toggles advanced disk information being shown.

Show Partitions

Toggles the disk partitions being shown.

Navigator Pane

Toggles the Navigator Pane view on and off.

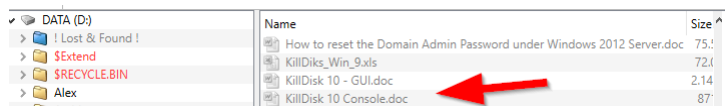


Figure 81: Deleted files in the Disk Explorer

Grey files indicate deleted files that have not been sanitized. These files are recoverable. Running KillDisk's *Wipe* operation will ensure these files are unrecoverable and make these grey files disappear from the file browser.



Note: Found deleted files will appear in their original directory (before they were deleted). The **! Lost & Found !** folder a directory created for found deleted files where the directory information is not discovered by the application.

Disk Viewer

KillDisk's Disk Viewer allows users to view the contents of connected drives in a Hex Editor view.

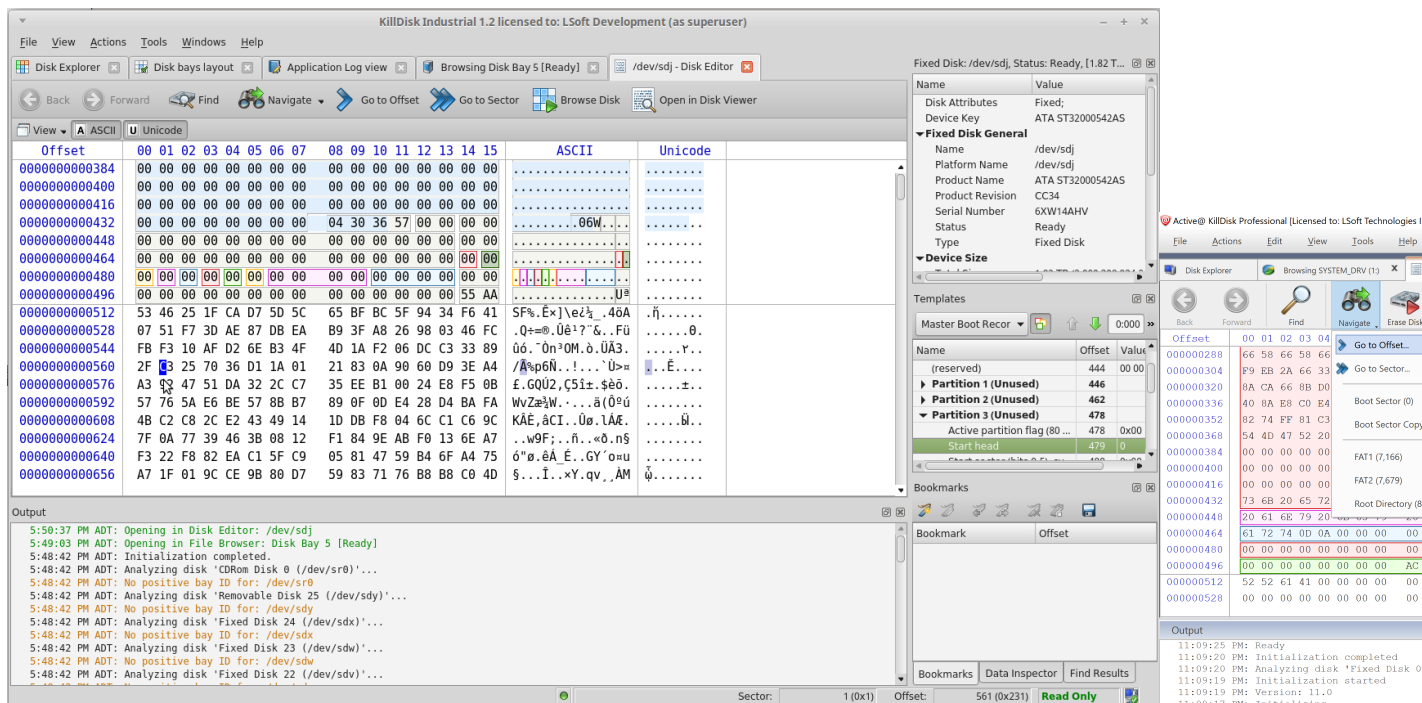


Figure 82: KillDisk's built-in disk viewer with the MBR template

To make it easier to navigate the Hex Editor view, KillDisk also offers a list of templates to help display the organization of the sectors on the disk by colored sections. The above uses the MBR template.

Templates			
NTFS Boot Sector	0:000	0:000	
Name	Offset	Value	Copy Value
JMP instruction	000	FFFFFFFFFFFF	FFFFFFFFFFFF
OEM ID	003	NTFS	NTFS
BIOS Parameter Block	008		
Bytes per sector	008	512	512
Sectors per cluster	00D	8	8
Reserved sectors	00E	0	0
(always zero)	010	000	000
(unused)	013	00	00
Media descriptor	015	248	248
(unused)	016	00	00
Sectors per track	018	63	63
Number of heads	01A	255	255
Hidden sectors	01C	567,296	567,296
(unused)	020	0000	0000
Signature	024	FFFFFFFFFFFF	FFFFFFFFFFFF
Total sectors	028	272,629,759	272,629,759
\$MFT cluster number	030	725,343	725,343
\$MFTMirr cluster number	038	2	2
Clusters per File Record Se...	040	246	246
Clusters per Index Block	044	1	1
Volume serial number	048	6B6FFFFFFFFF	6B6FFFFFFFFF
Checksum	050	0	0
Bootstrap code	054	FFFFFFFFFFFF	FFFFFFFFFFFF
Signature (\$S AA)	1FE	55FFFFFFFF	55FFFFFFFF

Figure 83: NTFS boot sector template values

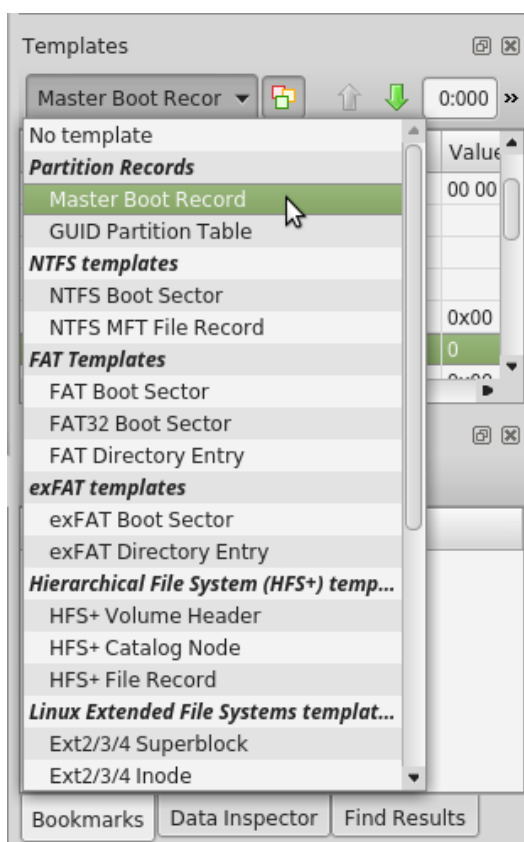


Figure 84: KillDisk's disk viewer templates

The Disk Viewer also includes a Find feature, for locating specific data in the low-level disk view

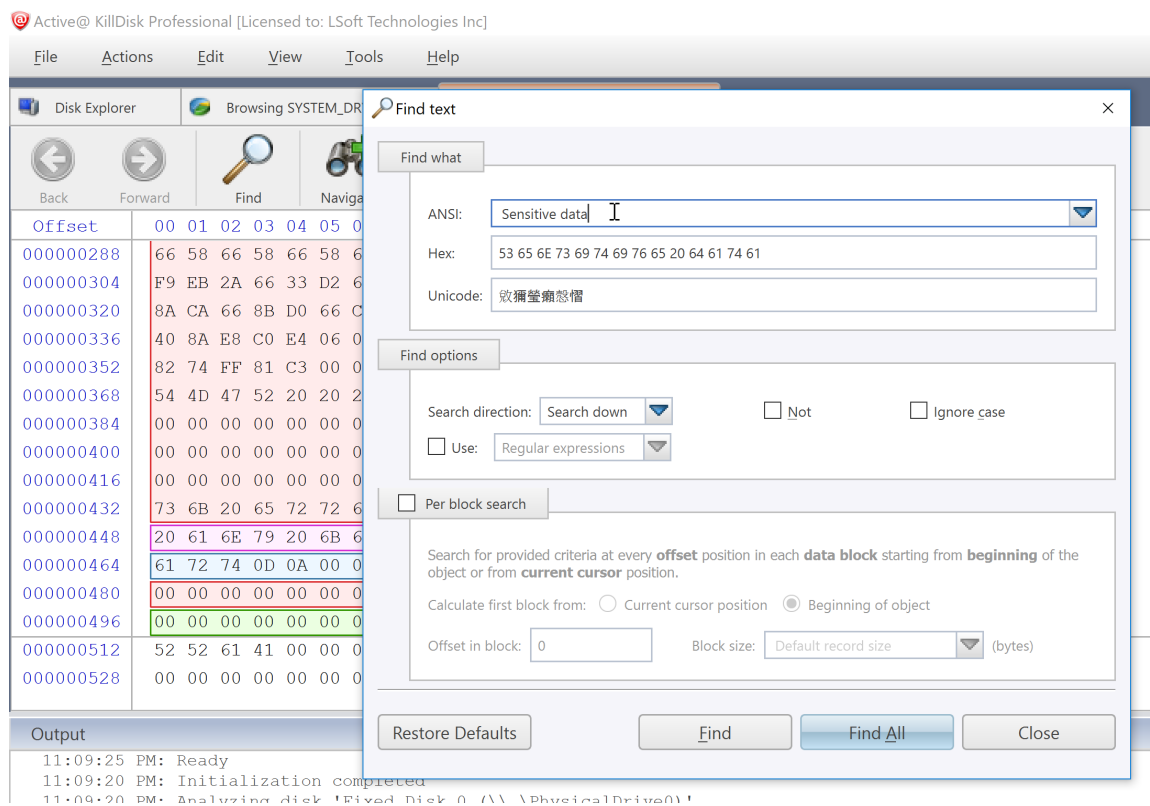


Figure 85: Finding data in the disk viewer

Find what

Input the characters you are searching for in ANSI, Hex or Unicode

Search Direction

If you have an idea of where the data may be located, specify where to search

Not

Search for characters that do not correspond to the **Find what** parameter

Ignore case

Disables case-sensitivity in the search

Use

Select between regular expressions and wildcards

Per block search

To speed up the search process, if you are familiar with the position of the data in the data block, you may specify a search with an offset or beginning of the object

SMART Monitor

KillDisk also supports displaying SMART information pertaining to the disks it sees. This is done simply by navigating to the file menu bar and selecting **Tools > Open SMART Monitor**. This will open the SMART Monitor window shown below.

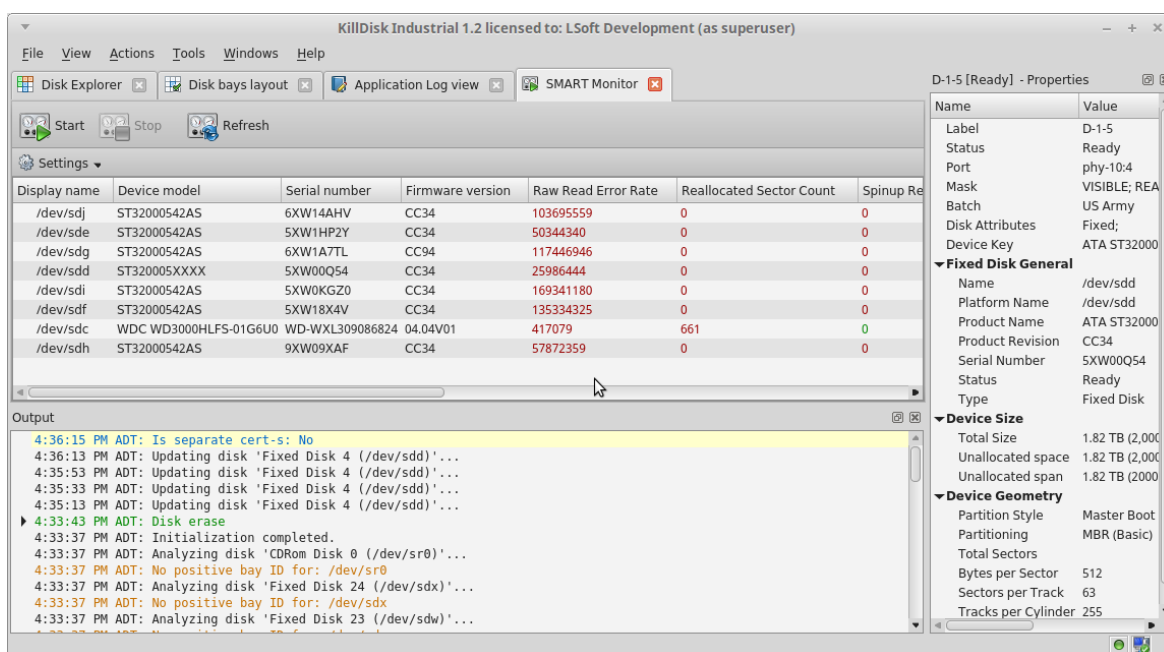


Figure 86: KillDisk's SMART monitor

SMART Information

The SMART Monitor displays a list of all discovered disks and shows the SMART information next to them in table format. The following SMART information is shown as separate columns:

- Display name
- Device model
- Serial number
- Firmware version
- Raw read error rate
- Reallocated sector count
- Spinup retry count
- Command timeout
- Reallocated Event Count
- Current Pending Sector
- Reported Uncorrect
- Soft Read Error Rate
- Read Error Retry Rate

Configurable settings

In the settings tab, these are the parameters that can be configured:

Monitored disks

Here you have the option to either display **all disks** seen by the system, or only the **active** (processing) disks.

Refresh Rate

This specifies the interval in seconds between updates to the SMART information displayed when the SMART Monitor is running.

Running the SMART monitor

The SMART monitor can either be refreshed manually or run to keep the information current. To run the SMART monitor, simply click the **Start** button in the action toolbar. To pause or stop auto-refreshing sequence click **Pause** or **Stop** buttons in view's toolbar respectively.

Application Settings

When you start `KillDisk`, change its settings (erase method, certificate options, etc...) and close the application, all current settings are saved to the **KILLDISK.INI** file in the location of the `KillDisk` executable. These settings will be used as default values the next time `KillDisk` is run.

KILLDISK.INI is a standard text file possessing sections, parameter names and values. All `KillDisk` settings are stored in the [General] section.

For parameter storage the syntax being used is:

Parameter=value

Here is an example of an INI file:

```
[General]
excludeSystemDisk=false
initHD=true
initRD=true
initCD=false
initFD=false
defaultSerialDetectionMethod=2
clearLog=false
logPath=C:\\Program Files\\LSoft Technologies\\Active@ KillDisk
Ultimate 11\\
logName=killdisk.log
logging=0
shutDown=false
saveToRemovable=false
showCert=true
killMethod=0
killVerification=false
killVerificationPercent=10
initDevice=true
fingerPrint=false
autoEject=false
skipConfirmation=false
wipeMethod=0
wipeVerification=false
wipeVerificationPercent=10
wipeUnusedCluster=true
wipeUnusedBlocks=false
```

```
wipeFileSlackSpace=false
wipeInHex=false
wipeUserPattern=Erased by Active@ KillDisk
wipeUserPasses=3
eraseInHex=false
killUserPattern=Erased by Active@ KillDisk
killUserPasses=3
accessDeniedCount=10
retryAtt=3
ignoreErrors=true
saveCert=true
certPath=C:\\Users\\Mikhail\\certificates\\
hideDefaultLogo=false
computerIDSource=0
showLogo=false
logoFile=
clientName=
companyName=
companyAddress=
companyPhone=
logComments=I hereby state that the data erasure has been
carried out in accordance with the instructions given by software
provider.
technicianName=Technician
sendSMTP=false
attachCert=true
useDefaultAccount=true
fromSMTP=
toSMTP=
nameSMTP=
portSMTP=2525
authorizeSMTP=false
usernameSMTP= password
SMTP=
mapName=
mapPath=
mapUser=
mapPass=
```

When KillDisk is running in interactive mode, all these parameters can be configured from a settings dialog accessed by clicking the “Settings” toolbar button. They also can be changed manually by editing the **KILLDISK.INI** file in any text editor such as Notepad.

Here is an explanation of all settings:

Table 5: KillDisk's Settings.ini Parameters

Parameter	Default	Options
defaultSerialDetectionMethod=	2	1 - use operating system's DeviceIOControl method
		2 - use S.M.A.R.T information, if device supports it
		3 - use Windows Management Instrumentation (WMI), if operating system supports it
showCert=	true	true/false – option of displaying the Erase/Wipe Certificate for printing after completion
saveCert=	false	true/false – option of saving the Erase/Wipe Certificate after completion
certPath=		Full path to the location where Erase/Wipe Certificate will be saved. This is a directory name
logPath=		Full path to the location where log file will be saved. This is a directory name
logName=		Name of the log file where event log will be saved to
skipConfirmation=	false	true/false – whether to display or skip Erase/Wipe confirmation dialog, or not
ignoreErrors=	false	true/false – whether to display disk writing errors (bad sectors), or ignore them (just place them to the log file)
clearLog=	false	true/false – whether to truncate log file content before writing new sessions, or not (append to existing content)
initDevice=	true	true/false – whether to initialize disks after erasing complete, or not
fingerPrint=	false	true/false – whether to initialize disk(s) and write fingerprint to the disk's first sector, or not
hideDefaultLogo	false	true/false – whether to hide default KillDisk logo at the top-left corner of the certificate, or not
computerIDSource=	0	0 - Disables showing the computer ID on the certificate
		1 - Shows BIOS ID in the certificate
		2 - Shows Motherboard ID in the certificate
shutDown=	false	true/false – whether to shutdown PC after Erase/Wipe execution complete, or not
sendSMTP=	false	true/false – to send e-mail report by email via SMTP
attachCert=	false	true/false – to attach a PDF certificate to e-mail report being sent
useDefaultAccount=	true	true/false – use pre-defined Free SMTP account for sending e-mail reports
fromSMTP=		E-mail address you'll get a report from, for example: reports@killdisk.com

Parameter	Default	Options
toSMTP=		E-mail address the report will be sent to
nameSMTP=		SMTP server (relay service) being used for sending e-mail reports, for example: www.smtp-server.com
portSMTP=	25	TCP/IP port SMTP service will be connected on. The standard SMTP port is 25, however some internet providers block it on a firewall
authorizeSMTP=	false	true/false – use SMTP authorization for sending e-mail reports (Username and Password must be defined as well)
usernameSMTP=		In case if SMTP service requires authorization, this is SMTP Username
passwordSMTP=		In case if SMTP service requires authorization, this is SMTP Password
showLogo=	false	true/false – whether to display custom Logo (image) on a Certificate, or not
logoFile=		Full path to the file location where Logo image is stored
clientName=		Client Name - custom text to be displayed on a Certificate
technicianName=		Technician Name - custom text to be displayed on a Certificate
companyName=		Company Name - custom text to be displayed on a Certificate
companyAddress=		Company Address - custom text to be displayed on a Certificate
companyPhone=		Company Phone - custom text to be displayed on a Certificate
logComments=		Any Comments - custom text to be displayed on a Certificate
killMethod=	2	[0-23] – Erase method to use for disk/volume erasing. See table of Erase Methods available. DoD 5220.22-M by default
killVerification=	true	true/false – whether to use data verification after erase, or not
killVerificationPercent=	10	[1-100] – verification percent, in case if data verification is used
killUserPattern=		ASCII text to be used for User Defined erase method as a custom pattern
killUserPasses=		[1-99] – number of overwrites to be used for User Defined erase method
wipeMethod=	2	[0-23] – Wipe method to use for volume wiping. See table of Erase Methods available. DoD 5220.22-M by default
wipeVerification=	true	true/false – whether to use data verification after wipe, or not
wipeVerificationPercent=	10	[1-100] – verification percent, in case if data verification is used
wipeUserPattern=		ASCII text to be used for User Defined wipe method as a custom pattern
wipeUserPasses=		[1-99] – number of overwrites to be used for User Defined wipe method
wipeUnusedCluster=	True	true/false – whether to wipe out all unused clusters on a volume, or not
wipeUnusedBlocks=	False	true/false – whether to wipe out all unused blocks in system records, or not
wipeFileSlackSpace=	False	true/false – whether to wipe out all file slack space (in last file cluster), or not

When you start **KillDisk** with or without command line parameters, its execution behavior depends on either command line settings (highest priority), settings configured in interactive mode and stored in the **KILLDISK.INI** file (lower priority), or default values (lowest priority).

Default value means that if the **KILLDISK.INI** file is absent, or exists but contains no required parameter, the pre-defined (default) value will be used.

Troubleshooting, Backup and System Recovery

In the event that you encounter technical difficulties with KillDisk, you may choose to either troubleshoot the system yourself with the files describe or, if you have active support and updates (you receive 1 year free with your purchase), contact our support team and attach your application log and hardware configuration file.

Common Troubleshooting Tips

Active@ Boot Disk Creator Troubleshooting:

All the OS options are greyed out

Ensure you have the Boot Disk Creator activated. You should see your registered name in the application.

Image file not found

You have activated the freeware that does not have the boot disk image you wish to create. Download your complete version using the link provided in your email and reinstall the software.

Issues formatting USB drive

This may happen occasionally when the file system causes conflicts in Windows. Launch the KillDisk application and erase the first few megabytes of the USB drive you wish to use. This will solve the problem.

Issues booting from the boot disk

Ensure the boot disk device is set at the top of your boot priority in the BIOS

Ensure your system time in the BIOS is accurate

Ensure you are not booting a 64-bit boot disk on a 32-bit system. In these cases, create a Console boot disk

Active@ KillDisk Troubleshooting:

Disk data will not erase

Ensure you are not erasing the system disk from the application. Use the boot disk to erase system disks

Data still found after a 'Wipe' operation

The Wipe operation will only sanitize data that has already been deleted in the OS. To sanitize all the data, including the operating system, use the 'Kill' operation

Erased the wrong disk

Stop the operation as soon as possible. Once data is sanitized by KillDisk, it will no longer be accessible. Use a tool like Active@ File Recovery to recover any data that has not been sanitized

Application Log

This log view monitors each action taken by the application and displays messages, notifications and other service information. Use the messages in this screen to observe and further understand the flow of the recovery process.

To open and activate Application log view do one of the following:

- From main menu choose **Tools > Application Log** or
- Use **F8** keyboard shortcut at any time

It is best to save the log file to a physical disk that is different from the disk that holds the deleted data. By doing this, you reduce the risk of writing over the data that you are trying to recover.

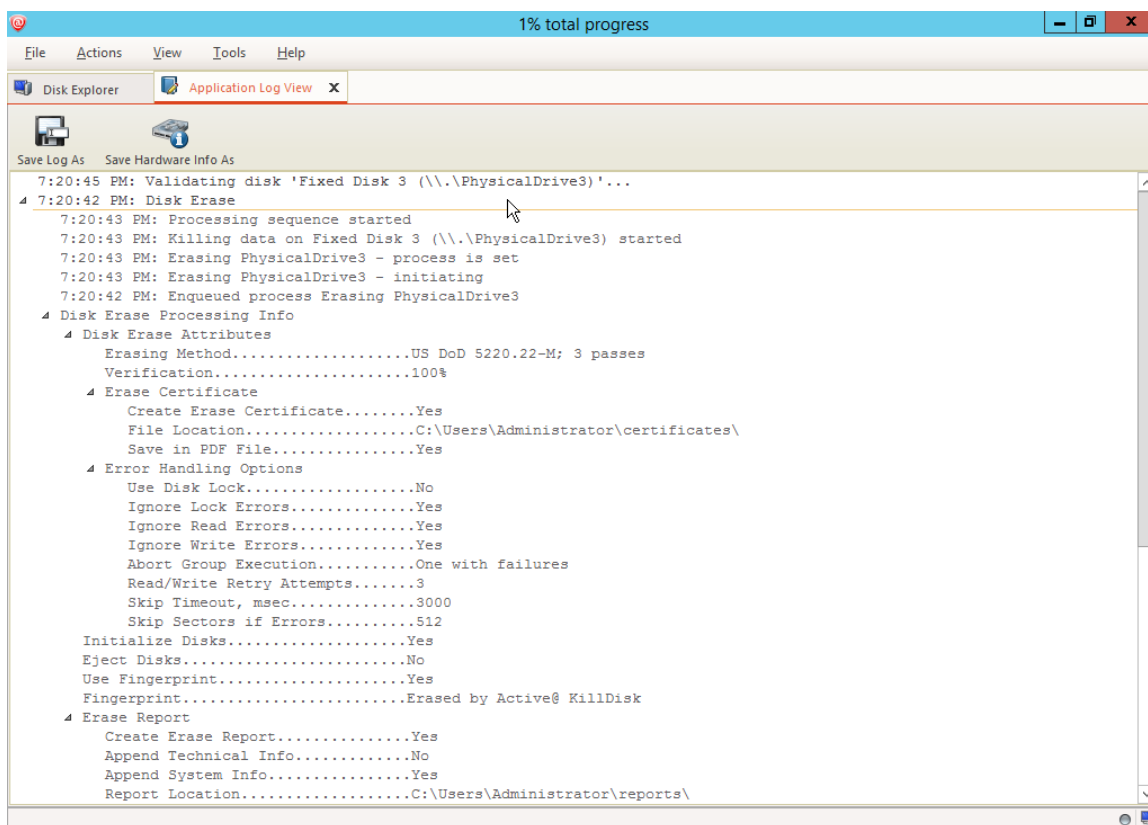


Figure 87: Viewing the application log

Log filter

Show or hide specific entry types in log view:

Show warning entries

Show non-critical warning entries

Show advanced entries

Show advanced entries related to application behavior and data analysis

Show console entries

Duplicate console entries into main log view

Show system entries

Show entries related to operating system activity and state

Font size

Change size of mono-space font used in log view for better experience

Write log on Disk

Writes log entries in dedicated file on disk, located in application directory. **Off** by default.

Expand and Collapse

Expand or collapse all log entries respectively

Clear

Clear log for current application sessions



Tip: We recommend that you attach a copy of the log file to all requests made to our technical support group. The entries in this file will help us resolve certain issues.

Console view

Additional log view (pane) to show log entries related to active feature view to display active process (erasure, disk examination etc.) entries and urgent (critical) messages.

To open console panel use:

- From main menu choose **View > Output** or
- Use **Ctrl+O** keyboard shortcut at any time

Hardware Diagnostic File

If you want to contact our technical support staff for help, a file that contains a summary of your local devices is helpful.

KillDisk allows you to create a summary listing file in XML format. This data format is “human-readable” and can help our technical support staff analyze your computer configuration or point out disk failures or abnormal behavior.

Create a hardware diagnostic file from the **File** menu by clicking the **Save Hardware Info As...** command.



Note: To save time when contacting our technical support staff, we highly recommend that you provide us with a hardware diagnostic file.

Appendix

Glossary

BIOS settings

Basic Input Output Subsystem. This programmable chip controls how information is passed to various devices in the computer system. A typical method to access the BIOS settings screen is to press F1, F2, F8, F10 or ESC during the boot sequence.

boot priority

BIOS settings allow you to run a boot sequence from a floppy drive, a hard drive, a CD/DVD-ROM drive or a USB device. You may configure the order that your computer searches these physical devices for the boot sequence. The first device in the order list has the first boot priority. For example, to boot from a CD/DVD-ROM drive instead of a hard drive, place the CD/DVDROM drive ahead of the hard drive in priority.

compressed cluster

When you set a file or folder property to compress data, the file or folder uses less disk space. While the size of the file is smaller, it must use a whole cluster in order to exist on the hard drive. As a result, compressed clusters contain "file slack space". This space may contain residual confidential data from the file that previously occupied this space. KillDisk can wipe out the residual data without touching the existing data.

cluster

A logical group of disk sectors, managed by the operating system, for storing files. Each cluster is assigned a unique number when it is used. The operating system keeps track of clusters in the hard disk's root records or MFT records. (See lost cluster).

file slack space

The smallest file (and even an empty folder) takes up an entire cluster. A 10- byte file will take up 2,048 bytes if that is the cluster size. File slack space is the unused portion of a cluster. This space may contain residual confidential data from the file that previously occupied this space. KillDisk can wipe out the residual data without touching the existing data.

free cluster

A cluster that is not occupied by a file. This space may contain residual confidential data from the file that previously occupied this space. KillDisk can wipe out the residual data.

deleted boot records

All disks start with a boot sector. In a damaged disk, if the location of the boot records is known, the partition table can be reconstructed. The boot record contains a file system identifier.

ISO

An International Organization for Standardization ISO-9660 file system is a standard CD-ROM file system that allows you to read the same CD-ROM whether you're on a PC, Mac, or other major computer platform. Disk images of ISO-9660 file systems (ISO images) are a common way to electronically transfer the contents of CD-ROMs. They often have the filename extension .ISO (though not necessarily), and are commonly referred to as "ISOs".

lost cluster

A cluster that has an assigned number in the file allocation table, even though it is not assigned to any file. You can free up disk space by reassigning lost clusters. In DOS and Windows, you can find lost clusters with the ScanDisk utility.

MFT records

Master File Table. A file that contains the records of every other file and directory in an NTFS-formatted hard disk drive. The operating system needs this information to access the files.

root records

File Allocation Table. A file that contains the records of every other file and directory in a FAT-formatted hard disk drive. The operating system needs this information to access the files. There are FAT32, FAT16 and FAT versions.

sector

The smallest unit that can be accessed on a disk. Tracks are concentric circles around the disk and the sectors are segments within each circle.

unallocated space

Space on a hard disk where no partition exists. A partition may have been deleted or damaged or a partition may not have been created.

unused space in MFT records

The performance of the computer system depends a lot on the performance of the MFT. When you delete files, the MFT entry for that file is not deleted, it is marked as deleted. This is called unused space in the MFT. If unused space is not removed from the MFT, the size of the table could grow to a point where it becomes fragmented, affecting the performance of the MFT and possibly the performance of the computer. This space may also contain residual confidential data (file names, file attributes, resident file data) from the files that previously occupied these spaces. KillDisk can wipe out the residual data without touching the existing data.

Windows system caching

Windows reserves a specified amount of volatile memory for file system operations. This is done in RAM because it is the quickest way to do these repetitive tasks.

Windows system records

The Windows registry keeps track of almost everything that happens in windows. This enhances performance of the computer when doing repetitive tasks. Over time, these records can take up a lot of space.

Erase Methods and 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 sanitization 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

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.

User Defined

User indicates the number of times the write head passes over each sector. Each overwriting pass is performed with a buffer containing random characters. Enables user to define any disk erase algorithm.

File Name Tags

Sequence number

Sequential number, used for group (batch) processing.

{Sequence #}

{Sequence 0#}

{Sequence 00#}

{Sequence 000#}

Date

Date file name tag uses current date in most cases in different formats:

{Date(YYYYMMDD)}

{Date(YYYY-MM-DD)}

{Date(YMMDD)}

{Date(YYYY)}

{Date(YY)}

{Date(Month)}

{Date(MM)}

{Date(DD)}

Time name tags

{Time(HHmmss)}

{Time(HH-mm-ss)}

{Time(HH)}

{Time(mm)}

{Time(ss)}

Disk name tags

Values for these name tags retrieved from context device:

{Serial ID}

Disk serial number, retrieved from OS or from SMART attributes

{Platform ID}

Disk platform identification (may be vary due to OS format);

{Product ID}

Disk manufacturer id

{Model}

Disk model name (if available);

{Size}

Disk size in gigabytes

{Sectors}

Disk size in sectors

Processing attributes

Disk processing attributes based on execution conditions:

{BatchName}

Batch name, if part of a batch processing.

{BayName}

Label of disk bay (slot).

{Status}

Overall completion status for group processing or separate disk processing status.