Eurosoft
computer reliability solutions

ZeroData™ Windows®

Professional, computer data erasure software, pre-boot and deployable

Permanent, Secure Hard Drive Data Destruction

www.eurosoft-uk.com

ZeroData™ Windows® Support Reference Guide: this document contains important information for setting up various features, test environments and supporting configurations.

Note: Windows PE contains a security feature that will cause end user's systems to reboot without prior notification to the end user after 72 hours of continuous use.

For questions or concerns about this publication or other Eurosoft publications and products please use the contact information below.

Eurosoft (UK) Ltd.
Head Office
3 St. Stephen's Road
Bournemouth
Dorset BH2 6JL
United Kingdom
Tel +44 (0)1202 297315
Fax +44 (0)1202 558280
Email: info@eurosoft-uk.com
Website: www.eurosoft-uk.com

Eurosoft (US) Inc.
US Office
706 Jackson Street
Sioux City, IA 51105
USA
Tel +1 (712) 255-7483
Fax +1 [866] 615-9384
Email: info@eurosoft-us.com
Website: www.eurosoft-us.com

Worldwide Information & Sales
Europe, United States, Pacific Rim
info@eurosoft-uk.com

Worldwide Support
Europe, United States, Pacific Rim
support@eurosoft-uk.com

Visit our web shop for fast on-line sales and the latest news about the best Eurosoft solutions for you.

Or please contact your nearest Eurosoft office should you require additional software, accompanying manuals, or site license.

Notice: Eurosoft (UK) Ltd aims to maintain its products and associated documentation as accurately as possible. Product names, features and revisions, as well as other test and data erasure requirements, compliances and regulations may change from time-to-time. Therefore, it cannot be held accountable for all variances that may occur.

Contents

Minimum System Requirements

ZeroData Windows will run on Microsoft Windows® 7 or later operating systems. These are Windows® server® 2008, 2012, 2016, Windows® 7, Windows® 8 & 8.1, Windows® 10 and Windows® Preinstallation Operating Environment (WinPE) versions of these operating systems. Windows® is a registered trademark of Microsoft Corporation in the United States and other countries.

Document Overview

This document is written to supply information about the basic operation of ZeroData™ Windows®.

ZeroData Windows is a fast, accurate and easy-to-use secure data erasure tool from Eurosoft (UK) Ltd that enables you to completely overwrite all accessible areas of a physical disk (not virtual drives) and supports only disk level secure data erasure. It is assumed readers have greater technical experience than that of basic Windows® operation to gain full product usage. This manual is for ZeroData Windows features.

Starting with build 1.0.3.0117, release packages will include ZeroData Legacy software as well. For details, please see What Is ZeroData Legacy section of the manual (click here to go the section)

Overview Of Disk Sanitization Practices

What is Disk Sanitization ?

Disk sanitization is a process of destroying original contents present in disk by overwriting them with some known data pattern and verifying the write process was carried out successfully. Often, terms like “disk wipe”, “disk erasure”, “secure data erase” or “secure data destruction” are used interchangeably as synonyms for disk sanitization – and these terms are also used interchangeably in this user manual.

IMPORTANT NOTE : Any disk erasure carried out without a verification pass is only safe for personal use. For any disk erased to be redeployed within the same organization or sent to any third parties, a verification step must be preferred.

Disk sanitization is not a task carried out for its own sake, it exists in the context of data security practices as the part where personal and/or organizational data is destroyed before a disk is taken out of active duty.

These data security practices are described in guideline documents describing a collection of tasks and processes that needs to be followed.

Data security guidelines describe techniques to deal with data remanence issue in three categories: clearing, purging/sanitizing, and destruction.

- Clearing is the removal of sensitive data from storage devices in such a way that there is assurance that the data may not be reconstructed using normal system functions or software file/data recovery utilities. The data may still be recoverable, but not without special laboratory techniques.

  Clearing is typically an administrative protection against accidental disclosure within an organization. For example, before a hard drive is re-used within an organization, its contents may be cleared to prevent their accidental disclosure to the next user.

- Purging or sanitizing is the physical rewrite of sensitive data from a system or storage device with the intent that the data cannot be recovered. Purging, proportional to the sensitivity of the data, is generally done before releasing media beyond control, such as before discarding old media, or moving media to a computer with different security requirements.

- Destruction is making the storage media unusable for conventional equipment. Effectiveness of destroying the media varies by medium and method. Depending on recording density of the media, and/or the destruction technique, this may leave data recoverable by laboratory methods. Conversely, destruction using appropriate techniques is the most secure method of preventing retrieval.

- For disks used in computing equipment, Clear and Purge/Sanitize levels are achieved using software, and Purge/Sanitize is carried out before destroying faulty disks as much as possible.

Almost all secure data destruction standards (known as “erasure methods”) are described in these guideline documents and operations that need to be carried out to comply with Clear, Purge/Sanitize and Destruction level of the standard are described.

Secure data destruction operation involves overwriting all accessible areas of a disk, one or multiple times, with some known sequence of data, thereby making retrieval of original data that was present on the disk impossible.

Verification is a crucial part of secure data destruction process and no erasure run is complete without verification. As the data pattern written to the disk is known, disk content can be checked whether the pattern was written correctly or not by comparing content of the disk against this known pattern. In cases where the final data pattern is not known, there are established procedures to verify that the original data on the disk is no more present.

What Are Your Responsibilities For Disk Sanitization ?

Disk sanitization is not a task carried out for its own sake: it exists in the context of data security practices as the part where personal and/or organizational data is destroyed before a disk is taken out of active duty.

These data security practices are described in guideline documents describing a collection of tasks and processes that needs to be followed.

On computer disks, Clear and Purge/Sanitize levels are achieved using software and disk sanitization is carried out instead of destroying healthy disks and before destroying faulty disks.

All these guideline documents describe what an erasure method is supposed to do so that a disk is accepted as a “properly sanitized disk”.

ZeroData Windows has all necessary features to properly sanitize disks:

- ZeroData Windows erasure methods cover all the well-known guidelines in data security field.
- Our transparent, traceable and tamper proof disk and system XML erasure logs and reports conform to most extensive set of requirements set out in data security guidelines.
- ZeroData Windows XML logs are structured not only for automatic processing by other computer programs but are also comprehensible when read by a person with basic English knowledge.
- Therefore, ZeroData Windows can be used as a straight drop-in replacement for any other secure data destruction software without losing any data reported by replaced software.
- With its extensive list of supported data erasure standards, ZeroData Windows relieves you – the organization or person who uses this software – from worrying about whether disk sanitization operation was carried out in the way described in the guideline documents or not.

However, as all guideline documents state clearly, you – the organization or person who uses this software – are responsible for the making sure at least the following points are carried out properly:

- Procedures to proper handling of disks and data contained in them are followed and documented in a traceable manner before a disk is sanitized.
- Procedures to proper sanitization of disks and data contained in them are followed and documented in a traceable manner during disk sanitization.
    - You need to determine which data security guideline or guidelines are relevant for you or your organization, declare them, and keep records of them.
    - You need to determine which level of data remanence measures will be applied and under which conditions they will be applied, declare them, and keep records of them.
    - You need to determine the conditions a disk must meet to be categorized as healthy or faulty, declare them, and keep records of them.
    - You must determine the conditions a disk erasure must meet to be categorized as successful, declare them, and keep records of them.
- Procedures to proper and independent verification of each sanitized disk are followed and documented in a traceable manner after each disk is sanitized. Even though we have complete trust to ZeroData Windows as all our customers do, this is not enough according to the guidelines. You are required to measure effectiveness of your data sanitization processes in a manner that is transparent, meaningful, and timely.

  - regardless of what the disk sanitization software reported to have done,
  - regardless of disk erasure is reported to have succeeded or not,
  - regardless of all previous independent verification procedure results

- Procedures to proper handling of both successfully sanitized disks and failed disks that still contain data are followed and documented in a traceable manner before
  - the disk is redeployed,
  - or the disk is destroyed

- Procedures to process and maintain records of disk sanitization are followed and documented in a traceable manner

In short, you need to choose a data sanitization guidelines document and you need to follow guidelines offered by this document.

If you are bound by U.S. laws, we suggest you follow “NIST SP 800-88 Rev.1” guideline which you can download for free from official NIST site by clicking on Local Download phrase under the Download Paper heading (Click here to open download page)

If you are bound by laws of an ISO/IEC member country, we suggest you follow “ISO/IEC 27040:2015, Information technology — Security techniques — Storage security” guideline which, unfortunately, is not free and does not have any preview edition before purchasing. To get a better idea, you can visit this Wikipedia link (click here to open Wikipedia page) and read what is involved and then later may visit the official ISO/IEC store (click here to open ISO/IEC store page)

Secure data destruction operation involves overwriting all accessible areas of a disk, one or multiple times, with some known sequence of data, thereby making retrieval of original data that was present on the disk impossible.

Verification is a crucial part of secure data destruction process and no erasure run is complete without verification. As the data pattern written to the disk is known, disk content can be checked whether the pattern was written correctly or not by comparing content of the disk against this known pattern. In cases where the final data pattern is not known, there are established procedures to verify that the original data on the disk is no more present.

IMPORTANT NOTE : Any disk erasure without a verification pass is safe for personal use only. For any disk erased to be redeployed within the same organization or sent to any third parties, a verification step must be preferred.

What Do You Need To Decide For Disk Sanitization ?

👍 As you are reading this manual, you made the correct decision by purchasing ZeroData Windows package, and fulfilled the first requirement.

Now, you need to decide on the following:

👍 Which erasure method or methods do you want to apply to disks ? Since you are using ZeroData, you can

- select any method from user interface manually,
- apply a single erasure method to all disks from command line,
- apply different erasure methods for SSD and HDD from command line,
- apply different erasure methods for SSD and HDD from command line,
- apply different actions after erasure ends from command line.

👍 How do you want to apply the erasure method to disks ? From the graphical user interface or command line ? Since you are using ZeroData, you can:

- erase a single disk,
- erase a selection of disks,
- erase all disks in a serial sequence, one after another,
- erase all disks in a parallel sequence, all disks at the same time.

👍 What do you want to do for faulty disks ? Since you are using ZeroData, you can:

- set an acceptable health level for disks before erasure operation and don't attempt to erase disks, below that target, eliminating time consuming erasures from your workflow,
- set an acceptable health level for disks after erasure operation and attempt to erase all disks, then fail, disks with health level below set target after doing your best to erase any trace of data.

👍 How do you want to stop disk erasures ? Since you are using ZeroData, you can:

- wait for all disks are erased, regardless of number of errors encountered (P.S.: Don't do this !)
- wait for all disks are erased, fail and stop erasures based on number of errors (P.S.: Do this !)
- wait for all disks are erased, fail and stop erasures based on calculated health scores.

👍 What type of output do you want to have and how ? Since you are using ZeroData, you can:

- select any combination of text, PDF and XML reports,
- select to create erasure reports after each disk erasure, or after all erasures end,
- select to create a bootable fingerprint on the disk or not.

👍 What type of output do you want to have and how ? Since you are using ZeroData, you can:

- select any combination of text, PDF and XML reports

If you are sanitizing data on behalf of your customers, most of these decisions will already be made by your customers and they will be conveyed to you. In such cases, you will need to match customer requests with features offered by ZeroData Windows.

- If you are processing drives with low volume but highly varied customer requirements, then executing erasures from graphical user interface will suit your needs.

- If you are processing drives with higher volume or almost standardized customer requirements, then turning the requirements into command line scripts and executing erasures from command line window interface will suit your needs.

What are Secure Data Erasure Standards ?

To standardize how data and any media that contains data (called as “data carriers”) are handled across their whole organization, some big organizations have felt the need to establish security practices how these should be handled. The successful practices lived on, gained support, and have become parts of data handling standards which are documented, published, and distributed within their organizations. Destruction of data residing on a data carrier when it reaches end-of-life, is an important aspect of data security procedures employed in these standards.

A data erasure standard refers to the part of data handling standard where data destruction practices are described. These data destruction practices range from how the data in paper printouts should be destroyed, how personnel ID cards are destroyed, how removable media are destroyed and include how the data kept in magnetic and solid-state disks are destroyed.

As far as magnetic and solid-state disks are concerned, physically destroying the disk does not guarantee that information cannot be extracted from the shredded disk parts. For magnetic disks, degaussing the disk with special magnetic devices is one of the solutions, but degaussers do not work on solid-state disks.

Therefore, these data erasure standards include a step to overwrite disk content to make every trace of the original data disappear. Regardless of the data pattern written to disk, the disk is not emptied, instead it is filled with new data specified with the pattern. In cases where the last erasure pass overwrites the value “0” to the whole disk, the disk is treated by some operating systems as empty, but actually it is filled with value “0”. Some firmware commands for SSD’s achieve this by flipping bits to a special pattern using some electronic means or replacing/deleting some cryptographic keys.

Depending on the selected secure erasure method, the procedure may also involve some rounds of verifying written patterns and issuing some firmware commands to be carried out by the disk itself. The patterns written in each pass and sequence of verification rounds are carried out as they are specified in various erasure method definitions.

This step is important for a variety of reasons, determining whether the erased disk is still deployable for re-use or not within the organization is one of them.

What is ZeroData Windows?

ZeroData Windows is a disk sanitization solution developed by Eurosoft (UK) Ltd to facilitate parallel disk wipe operations. Eurosoft also offers hardware diagnostic products running on Windows, pre-boot UEFI and its own DOS-like pre-boot environment to cater your organizational needs.

ZeroData Windows uses the Microsoft Windows environment and is bound by the limitations of Windows environment, it does not use Linux operating system utilized by certain products.

If ZeroData Windows is executed from Windows PE, then limitations of Windows PE apply: the user must add required Windows PE packages and third-party storage drivers to the boot image for devices not supported out-of-box by Windows PE.

With more than 95% of all x86 CPU architecture-based computers running on Windows operating systems, the advantages of executing ZeroData Windows on Windows operating system offers the widest drive data erasure coverage.

ZeroData Windows is flexibly designed to run as a portable MFC application being called from a command line or in its interactive user interface.

The command line approach allows it to simply drop-in as any type of scripted operation and can be deployed as command line scripts or PowerShell scripts. As such, ZeroData Windows is designed for high volume data erasure operations.

The user interface option is optimized to maintain light-weight usability. All functions of ZeroData can be used from the user interface, selecting disks and options to erase disks.

ZeroData Windows is designed to overwrite all accessible area of a physical disk and supports only disk level secure data erasure. Overwriting logical entities such as selected folders or logical volumes are not supported.

What is ZeroData Windows Reporting Console ?

To address cases where the operating system images do not have some of the required capabilities for report creation, or customer workflows requiring processing of logs offline or after the erasure, ZeroData Windows package contains an offline log processing utility named ZeroData Windows Reporting Console.

ZeroData Windows Reporting Console controls the offline printing of erasure certificates/reports , erasure labels containing 1D and 2D barcodes, and 12N QR codes , from the saved ZeroData erasure information of a particular storage media.

This can be done in batches of selected media or singly , it verifies the integrity of the digital signature of a selected erased media, any tampering detected will stop of any of the above documents being generated.

- As .NET 4.6 and other libraries are needed for PDF creation, the user may have chosen not to include the .NET libraries to keep the application size to a minimum under WinPE operating system.
- Alternatively, if using ZeroData Windows in a networked PXE environment, the files may all have been stored on a shared location.

In such cases, the user may elect to store all log files, but print reports and labels only when required.

This utility program comes in a separate folder and can be executed without installing on a computer designed to serve as a log and report management station.

Important Registry Settings For Working With ZeroData Windows Log And Report Files

Your ZeroData Windows distribution contains a folder named “ZDW_UTILITIES” and a subfolder named “RegistrySettings” and there are three registry key files.

- On some systems accessing files on a network share requires setting a registry key on the computer where Reporting Console is running, otherwise the network folders might not be visible in File Explorer windows. This issue arises from Windows UAC and security settings. The registry key named “EnableLinkedConnections.Reg” that will help you to fix this issue through a registry change. For more information on this issue, you might refer to this Microsoft document: Mapped drives are not available - Windows Client | Microsoft Docs

- On most Windows computers, there is a 260-character limit on file paths. To overcome this limit, there is a registry key named “Remove260CharacterPathLimit.reg” that will help you to remove this limit through a registry change.

- In case you need to restore the 260-character limit on file paths, there is a registry key named “Restore260CharacterPathLimit(Default).reg” that will help you to restore back this limit through registry a change.

Please see Appendix J – Applying Suggested Registry Setting Changes on how to add apply these registry keys.

What is ZeroData Legacy ?

ZeroData Legacy (or simply ZeroData) is a secure data erase solution developed by Eurosoft (UK) Ltd to facilitate disk erasures in a DOS like pre-boot environment called EuroDOS. It can both be executed from command line or in an interactive way, and it can run in full DOS environment as well.

Just like all other Eurosoft pre-boot software, ZeroData still remains popular in IT circles and customers are asking for it. Due these reasons, some ZeroData Windows packages include this tool.

If you are unfamiliar with ZeroData Legacy, it can help you in cases where:

- A Windows or WinPE based workflow is not suitable,
- The computer does not support booting from WinPE images,
- The computer has lower hardware specification than required for ZeroData Windows,
- a DOS-like environment is a necessity to erase the disks.

However, ZeroData and ZeroData Windows are vastly different software and the difference in use cases, capabilities, and the output they produce are so big that describing ZeroData Legacy in this manual will cause unneeded confusion.

Therefore, ZeroData Legacy is described in its own user manual which is included in the ZeroData Windows package. Please refer to ZeroData User Manual document when you need to use ZeroData legacy.

Installation and System Requirements for Installing ZeroData Windows Package

Please Read Carefully Before Executing ZeroData Windows

- ZeroData Windows itself is a portable application and does not need to be installed to be executed on a target computer. However, the special ZeroData License USB Device must be connected to the computer unless a special licensing agreement is reached.
- All files and folders contained in the ZeroData Windows folder must be placed in the same folder.
- ZeroData Windows has a graphical user interface and therefore can be executed with or without user interaction to execute parallel disk wipe operations. In both cases, ZeroData Windows must be executed with administrator right, that means it must be “Run as Administrator”.
- ZeroData Windows must be called from a Command Prompt or invoked from a PowerShell window with administrative rights. Please refer to your OS documentation on how to invoke these command windows with administrative rights.

- ZeroData Windows contains different executables to run on 32-bit and 64-bit Windows operating systems. Please make sure you run the correct version on target operating system.
- The computer must be booted from a full Windows operating system boot disk or a Windows PE image booted from a USB disk, CD/DVD or PXE.
- The Windows or Windows PE operating system version must be Windows 7, Windows 8.1 or Windows 10.
- For best storage device compatibility, and when running on UEFI computers, the latest version of 64-bit operating system must be used. Running Windows 10 64-bit, using build 1703 or later is recommended. Older Windows versions like 7, 8 and 8.1 may be used, but they may require additional third-party storage device drivers, therefore creating complications that can be easily be avoided by using Windows 10.
- For Windows PE based executions, the following packages must be added to the boot image: WinPE-StorageWMI and WinPE-EnhancedStorage. Depending on your requirements, you might need to add relevant storage drivers to your Windows PE image like AMD and Intel RAID drivers, Intel RST driver, drivers for the RAID cards you might have and so on.

- PDF reporting option requires presence of .NET 4.6 on the booted Windows or WinPE image to work. For Windows PE based executions, the .NET package must be added to the image. If .NET is not found, PDF reports will not be created even if they are specified in report file type parameter.

- ZeroData Windows is shipped with Eurosoft WinPE Image creator, a utility that enables the user to easily create and maintain ZeroData boot images. These images can be created as a PXE WIM file, CD-ROM or USB Disk. These operations are described later in this manual.

- Removing hidden areas created with firmware features like HPA and DCO partitions, requires power cycling the disk. Therefore, a disk that contains these partitions requires a two-step operation. This is a limitation of the firmware features themselves and is not related to ZeroData Windows itself.

  Essentially HPA and DCO partitions are some form of hacks implemented in disk controller firmware. After an initial upsurge in usage of HPA and DCO partitions, their usage has been in constant decline

and most of current disks don't even support this feature. A Eurosoft client erasing millions of disks per year, has reported that they didn't see an HPA or DCO partition in last 6 years.

Like most firmware commands that can lead to data loss, removing HPA and DCO partitions under Windows based operating systems is not a reliable process.

- Based on customer feedback on HPA/DCO partitions, ZeroData Windows has an option to allow the user to specify whether to remove or not remove HPA/DCO partitions.

- Again, based on customer feedback on HPA/DCO partitions, there is an option to allow the user not to remove hidden partitions and in case HPA/DCO partitions are encountered, disk an error is logged, and erasure labeled as failed without attempting hidden area removal.

- Also based on customer feedback, starting with 1.3.0.117 official release build, ZeroData Windows release package includes legacy ZeroData package and ZeroData User Manual. In case HPA and/or DCO removal process fails when ZeroData Windows is used, legacy ZeroData can be used to remove these partitions.

- Secure Data Erasure Methods like NIST 800-88 Rev 1 utilizing Secure Erase / Enhanced Secure Erase firmware commands as options, require the disk security mode set to be not frozen, but any disk that is connected to the computer during BIOS/UEFI boot process is automatically set to be frozen.

  Under Windows operating system, it is very easy to remove this freeze lock, simply putting the computer into sleep mode and then waking back is all that is required. Unfortunately, Windows operating system does not allow executing Secure Erase / Enhanced Secure Erase firmware commands and allows these commands to run only in Windows PE environment.

  As Windows PE does not have sleep mode capability, applying Secure Erase / Enhanced Secure Erase firmware commands required for NIST methods is only applicable on Windows PE using hot swap capable SAS/SATA ports and power cycling the disks after WinPE boot.

  For secure data erasure methods requiring Secure Erase / Enhanced Secure Erase firmware commands, we recommend using hot swap drive cages that allow disks to be pulled off and pushed back into drive bays whenever possible.

System Requirements to Install ZeroData Windows Application Package to Create ZeroData Windows Deployment Images

- For best storage device compatibility, and when running on UEFI computers, the latest version of 64-bit operating system must be used. Running Windows 10 64-bit, using build 1703 or later is recommended. Older Windows versions like 7, 8 and 8.1 may be used, but they may require additional third-party storage device drivers, therefore creating complications that can be easily be avoided by using Windows 10.

- ZeroData Windows is shipped with Eurosoft WinPE Image creator, a utility that enables the user to easily create and maintain ZeroData boot images. These images can be created as a PXE WIM file, CD-ROM or USB Disk. These operations are described later in this manual.

- PDF reporting option requires presence of .NET 4.6 on the booted Windows to work. If .NET is not found, PDF reports will not be created even if they are specified in report file type parameter.

- To install ZeroData Windows and its Reporting Console utility, 300 MB of free disk space is required. We strongly suggest you apply the registry key additions described in Appendix J on the computer where Reporting Console utility will be executed.

- To create WinPE deployment images, Windows ADK must be installed on the computer where WinPE deployment images will be created.

    - Depending on the chosen features, Windows ADK installation requires downloading multiple gigabytes of data from Microsoft servers and installing them on the computer.
    - We suggest at least 20 GB of available free space on disk.
    - Depending on your internet connection speed, downloading Windows ADK can take a considerable time.

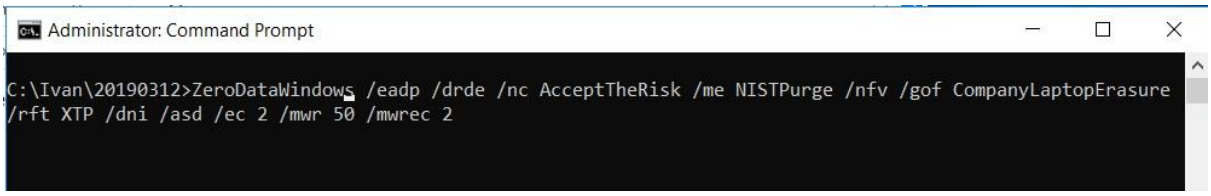
Using ZeroData Windows

Executing ZeroData Windows From Command Line

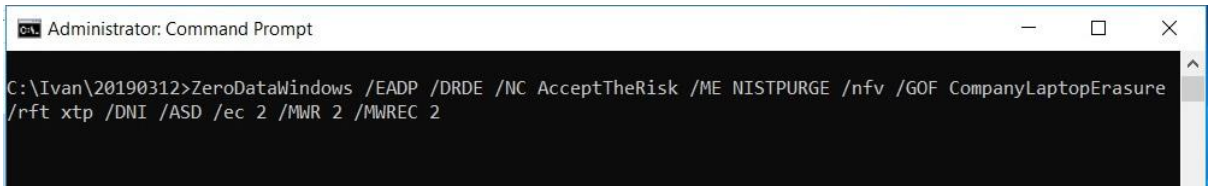
Using a full Windows operating system, ZeroData Windows can be executed from either a Command Prompt or from a PowerShell window started in Administrator mode.

The only syntax difference between these two methods is the ".\" characters preceding any executable in PowerShell syntax, all other syntax is the same for both command window alternatives.

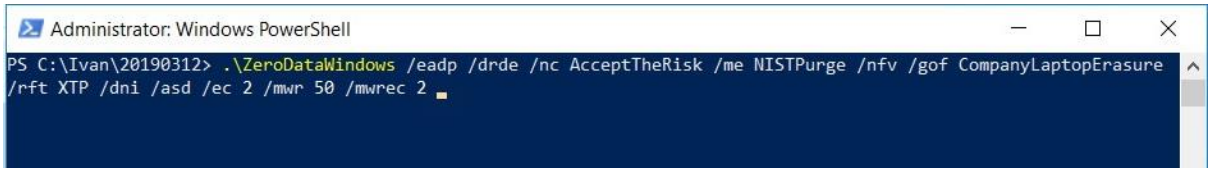
Below is a sample command prompt command line that executes ZeroData Windows with some erasure and report creation options.



All commands in a Windows Command Prompt window are not case sensitive, therefore the above sample command line can also be written like below with the same result. ZeroData Windows has only one special case where the parameter is case sensitive this is the parameter to override the confirmation prompt and it must be typed exactly as "AcceptTheRisk".

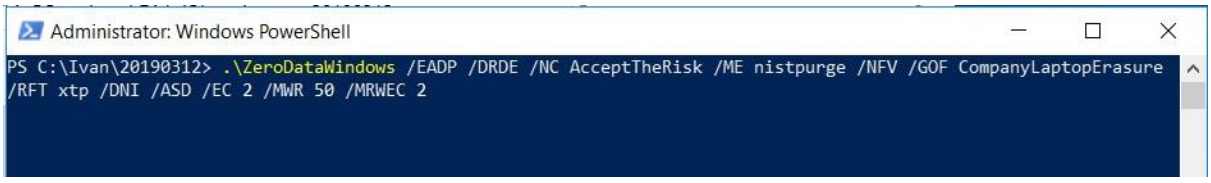


Below is the same sample command line that executes ZeroData Windows with some erasure and report creation options, this time from a Windows PowerShell window.



Windows PowerShell window is generally not case sensitive; therefore, the above sample command line can also be written like below with the same result.

ZeroData Windows has only one special case where the parameter is case sensitive and it must be typed exactly as "AcceptTheRisk", all other parameters are case insensitive.



All command line switches, and their parameters are explained in later sections of this manual.

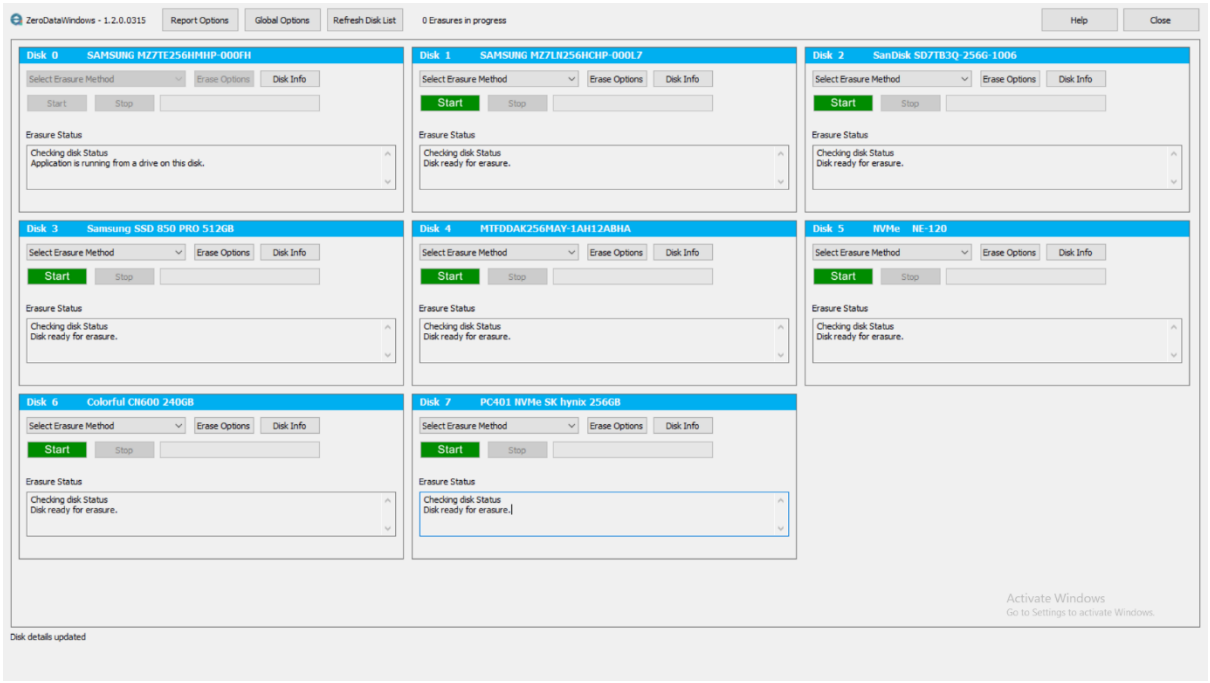
ZeroData Windows switches and parameters are the same regardless of the environment used.

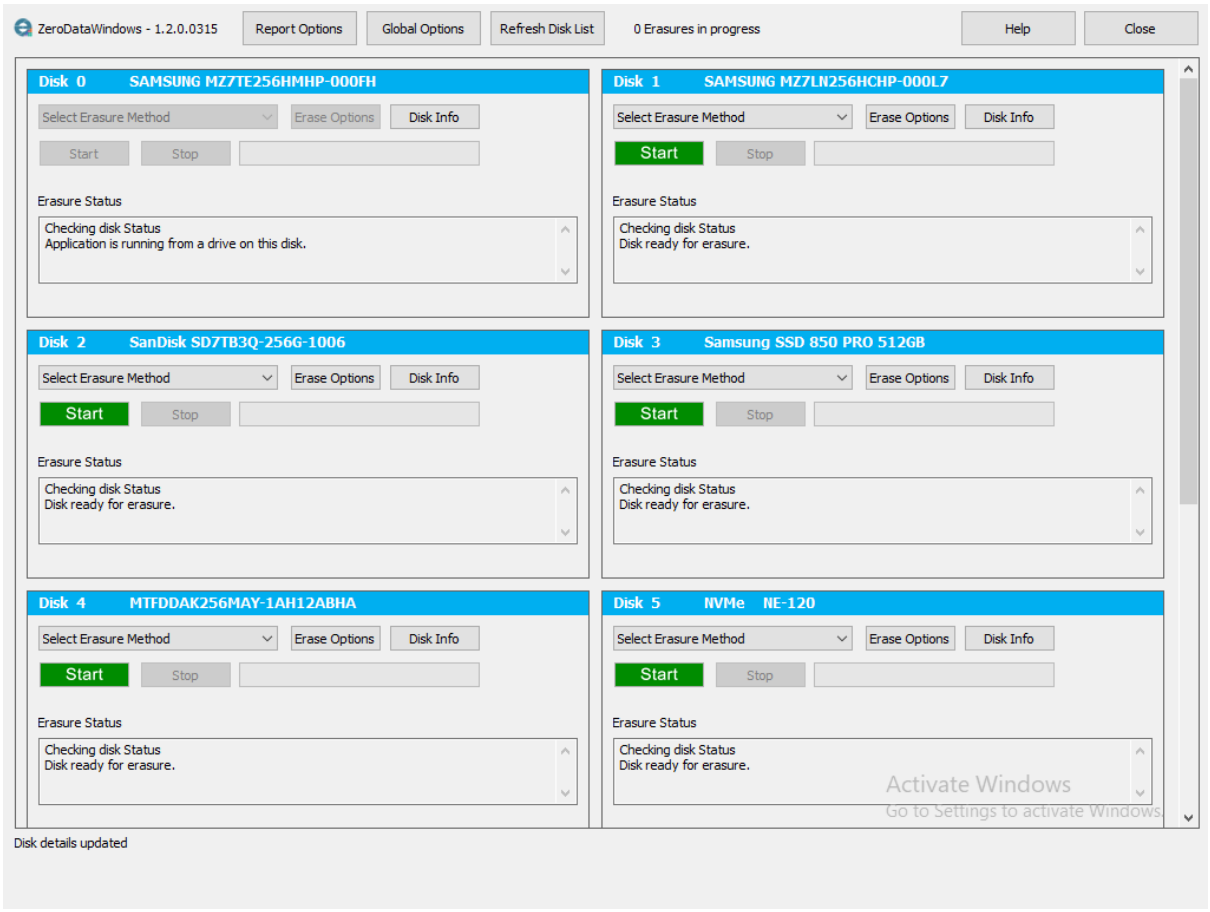
The simplicity of ZeroData Windows switches and parameters make it an ideal drop-in application for any scripted Windows workflow, whether the computer is booted from an external disk or booted over PXE.

Using a PXE environment is described in a separate appendix at the end of this document. The creation and editing of the PXE boot image are made simple by using the Eurosoft Windows PE Image creation tool to set the environment, packages and editing the Startnet.cmd file.

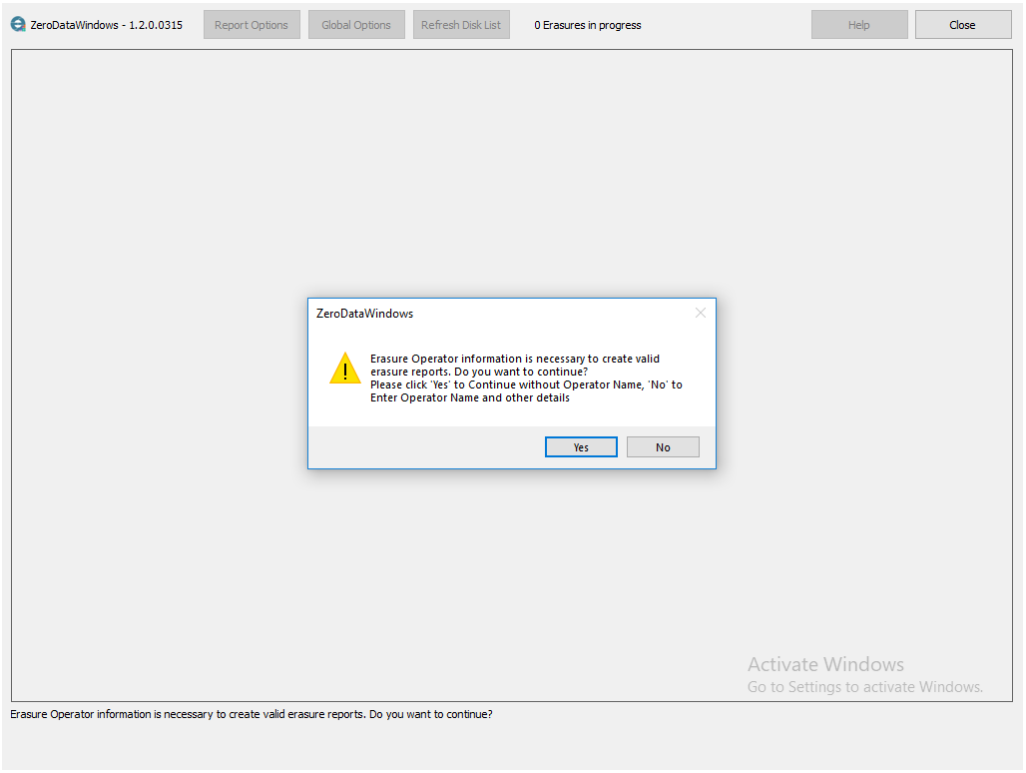
Executing ZeroData Windows Interactively From User Interface

ZeroData Windows is a full screen application that fills the monitor completely. Depending on screen resolution, the number of disks horizontally displayed changes as shown in below sample screenshots.

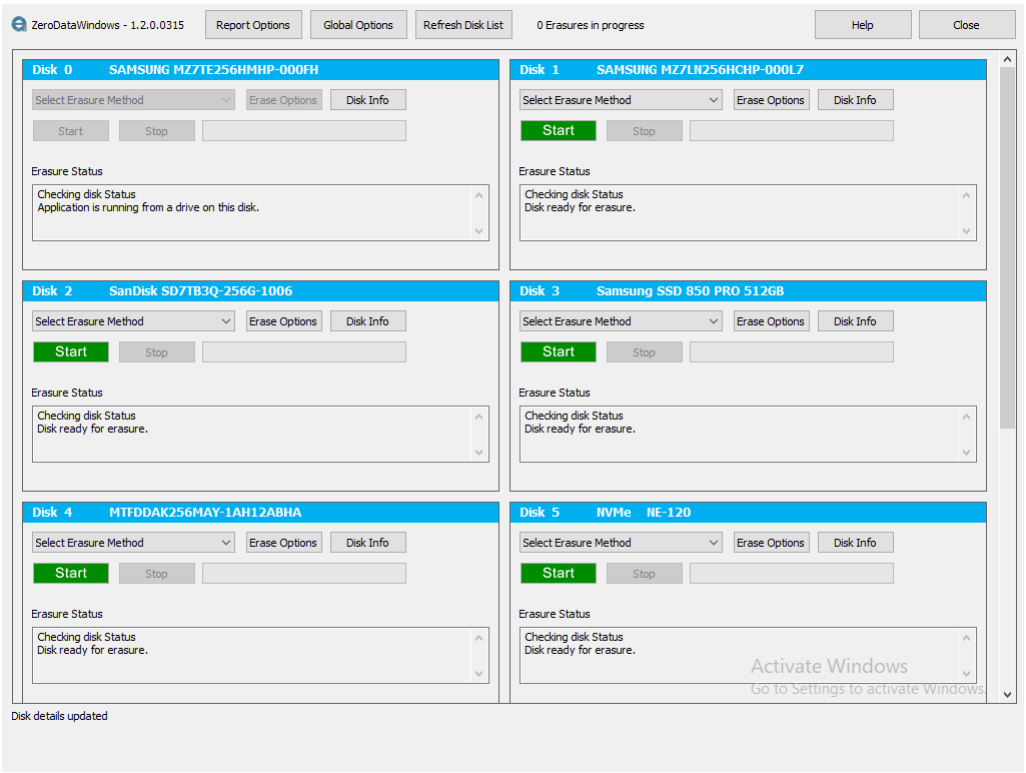




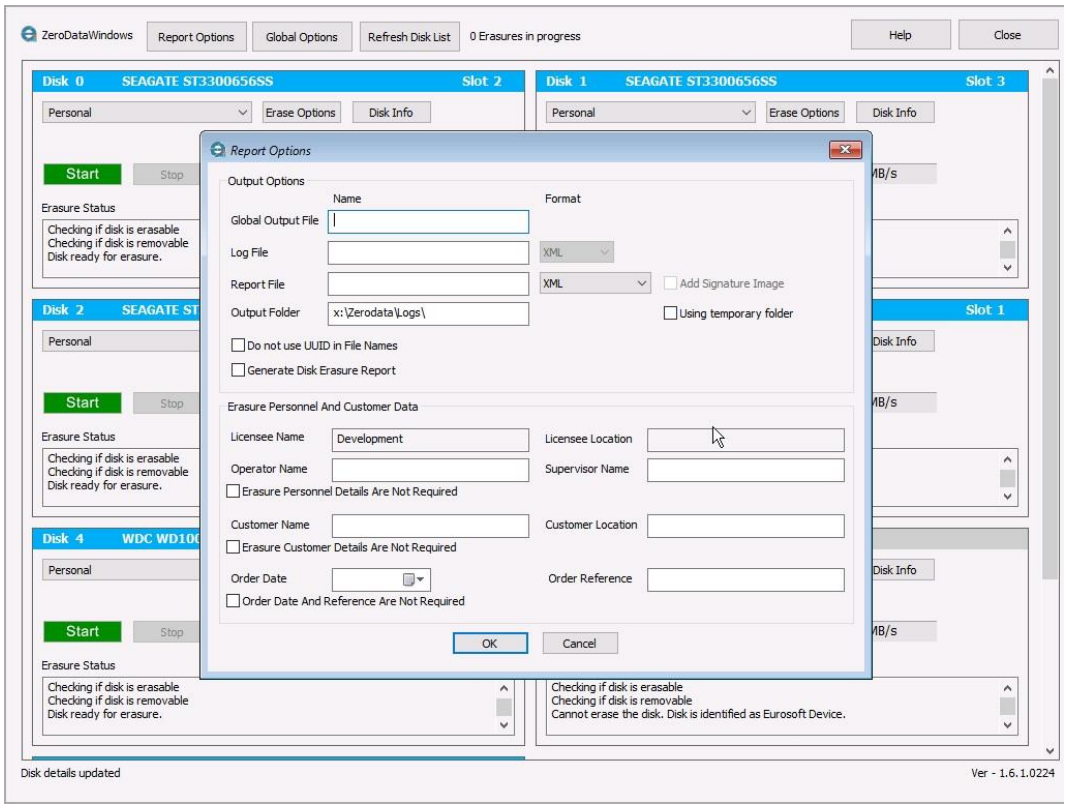
If ZeroData Windows is started directly without specifying “/NC AcceptTheRisk” parameter, a warning message is displayed, and application requires the user to select.



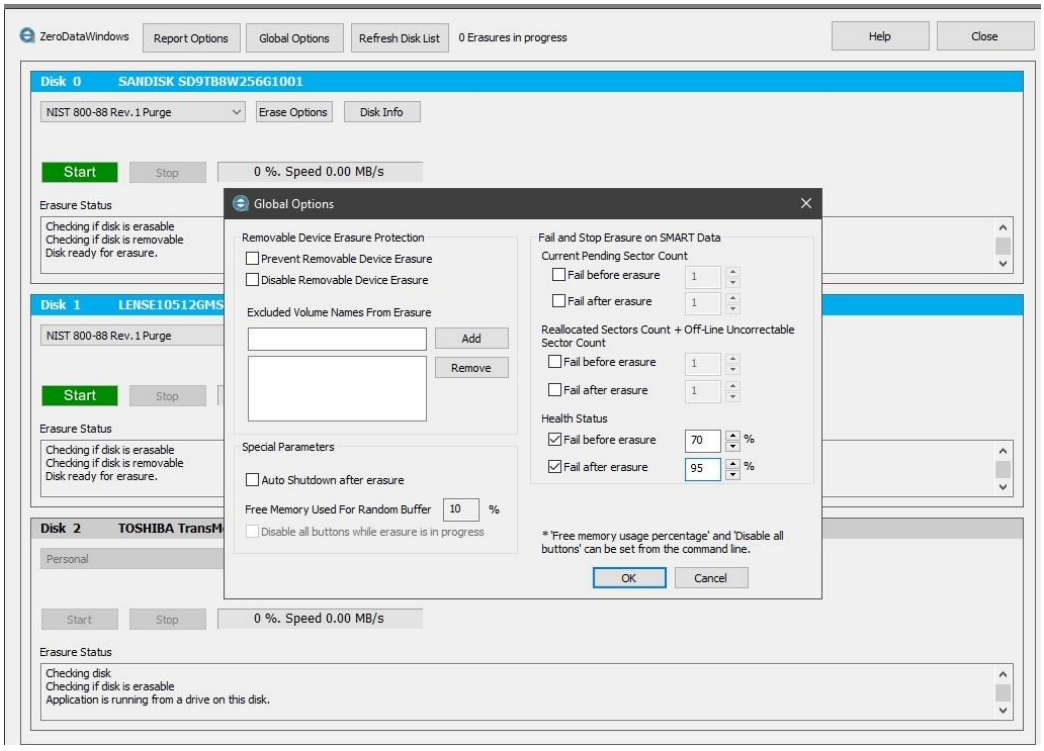
After application is completely loaded, a screen listing detected disks is displayed.



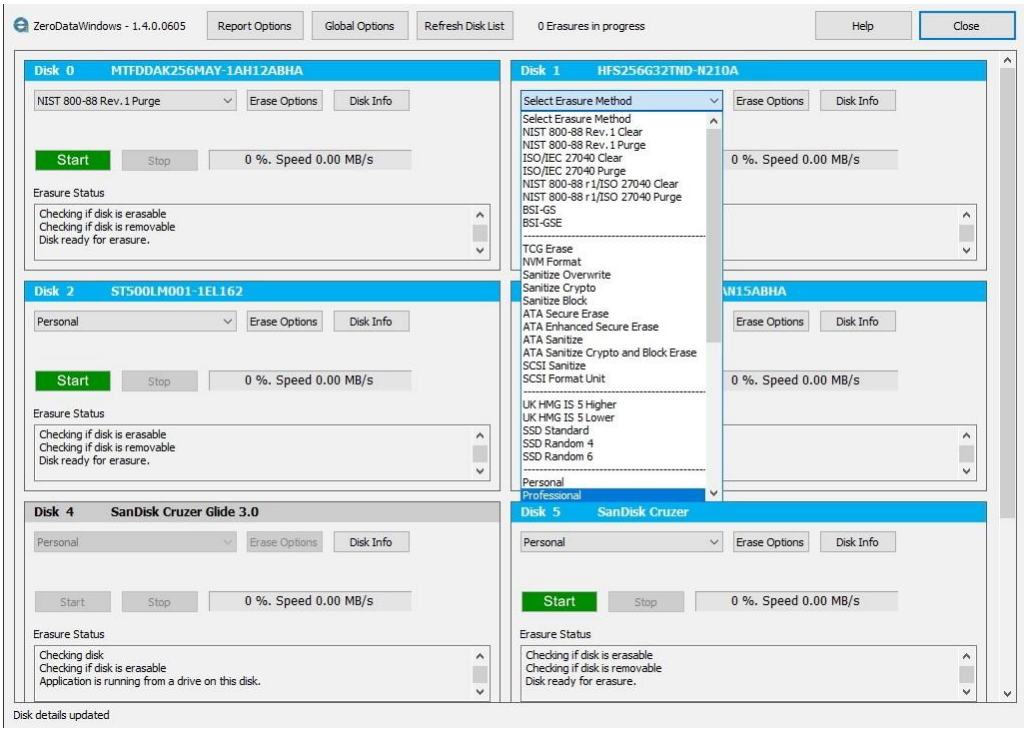
Options related to name and type of report files and details related to erasure personnel and customer can be filled by clicking on Report Options button. Details of these options are described in Specifying Output Options and Specifying Erasure Personnel and Customer Data sections of this manual.



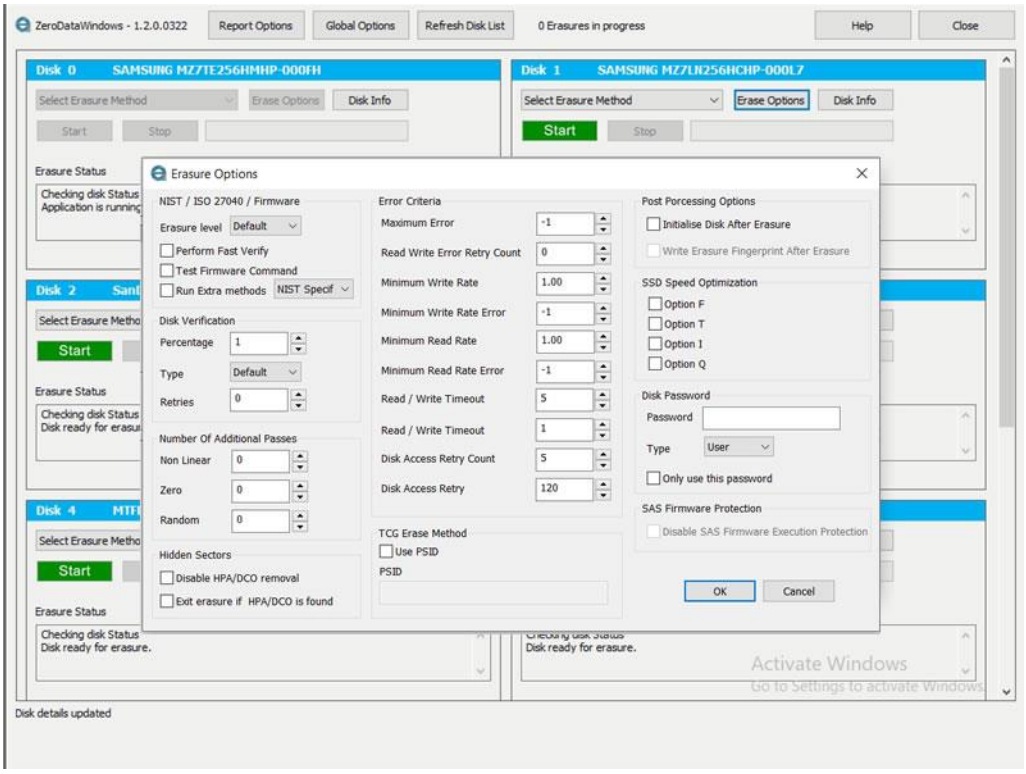
Options governing removable disk erasure protection, special parameters and failure conditions due to reported S.M.A.R.T. values and health scores can be specified by clicking on Global Options button.



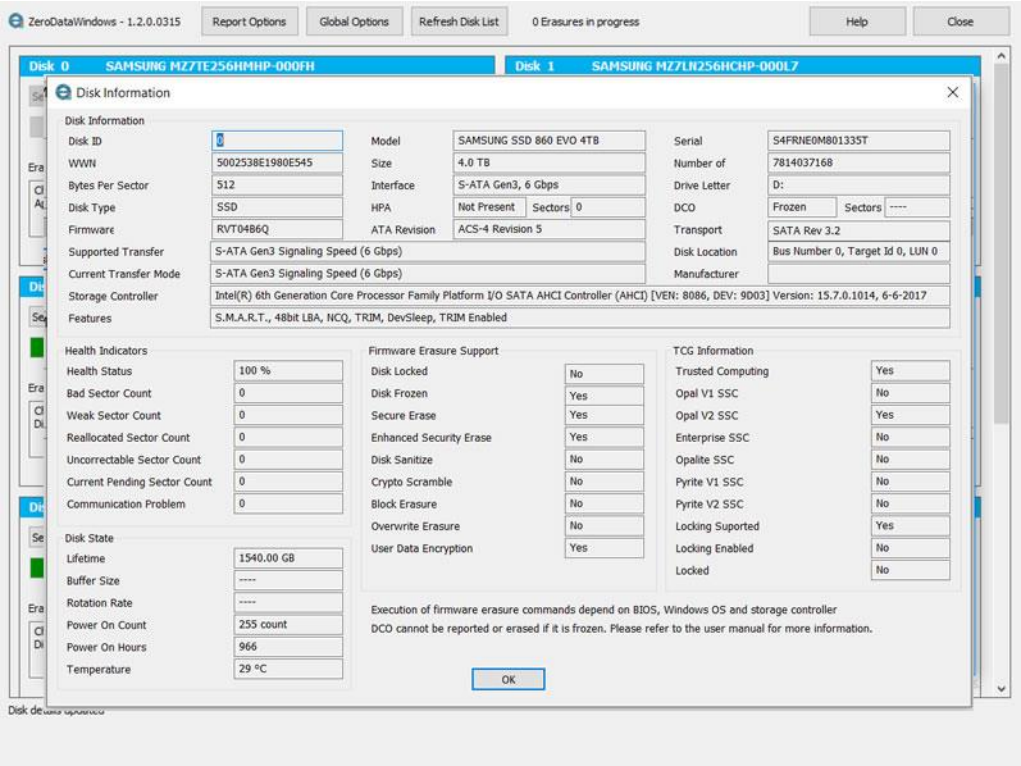
A disk is selected for erasure by selecting an erasure method from “Select Erasure Method” dropdown box where all available erasure methods are listed in groups, with most current erasure standards and firmware erasure methods listed on top and least current overwrite methods listed at bottom. Details for each method is listed in later section of this manual starting from this page.



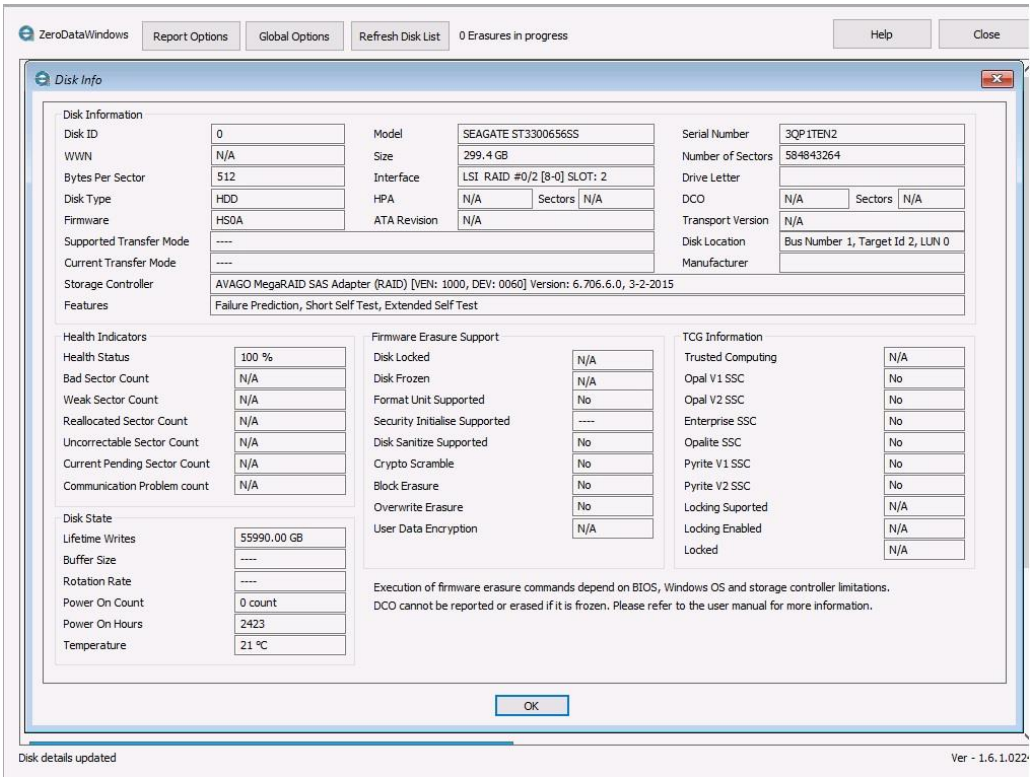
Selecting only the erasure method will erase the selected disk with default parameters for the method. Erasure Options button allows the user to customize these default parameters. Parameters for erasure method, error handling, erasure verification are described later in this manual.



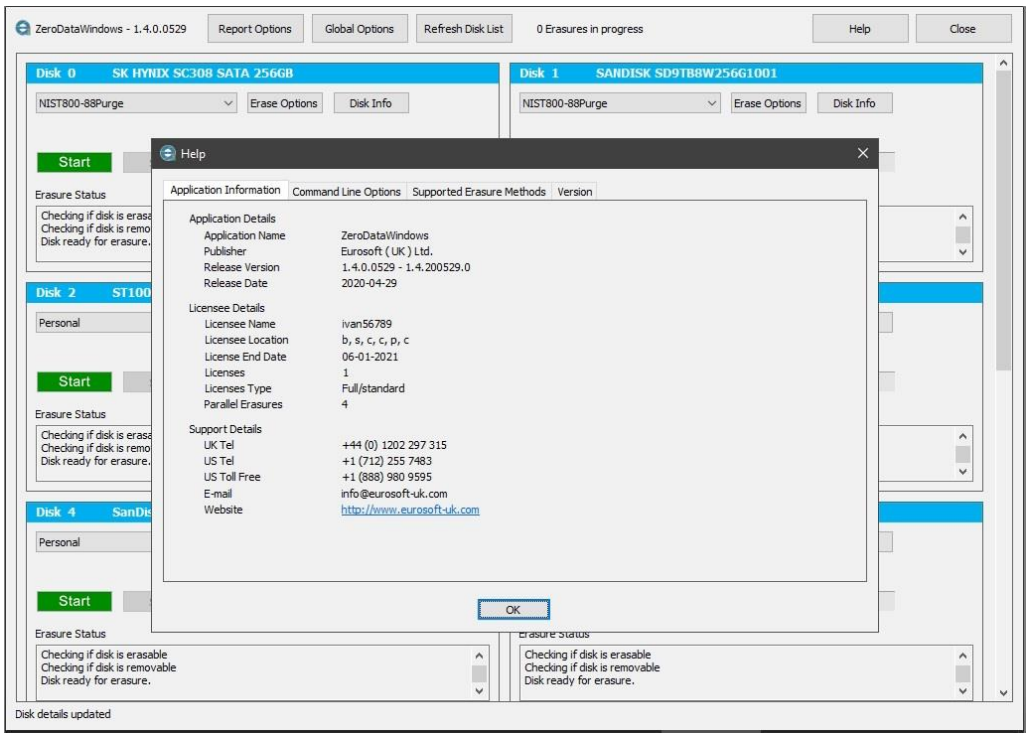
Pressing the Disk Info button displays information about disks in groups based on relevancy to erasure process. A sample screenshot for an SSD is given below.



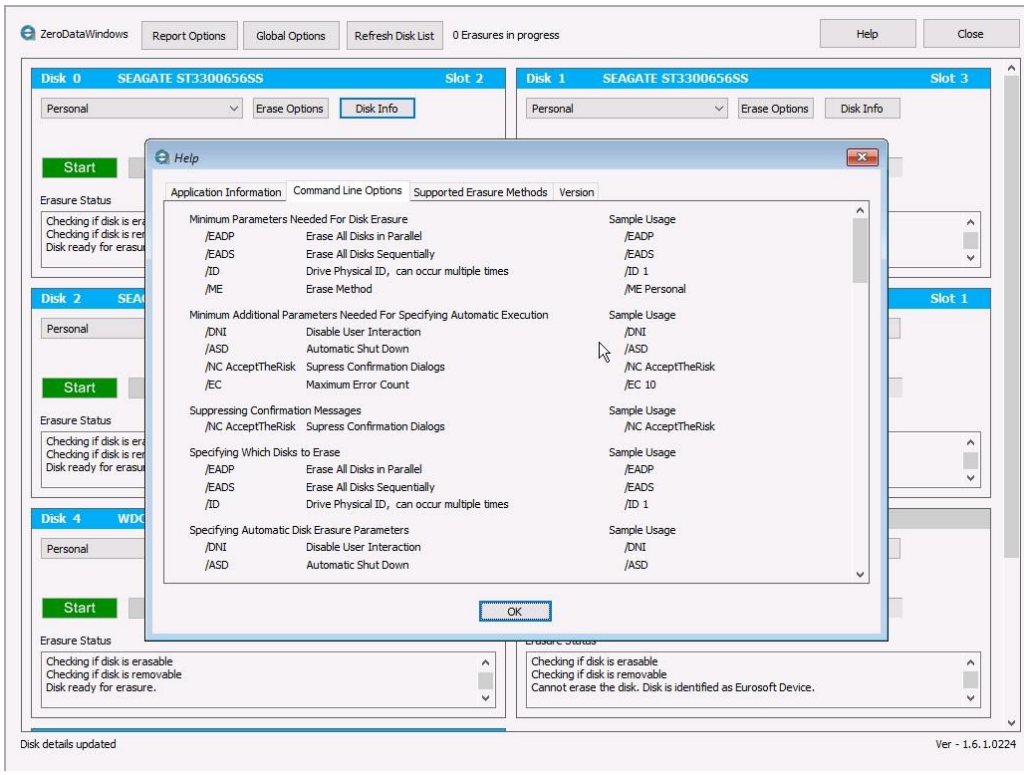
Similarly, a sample screenshot for a SAS disk is given below.



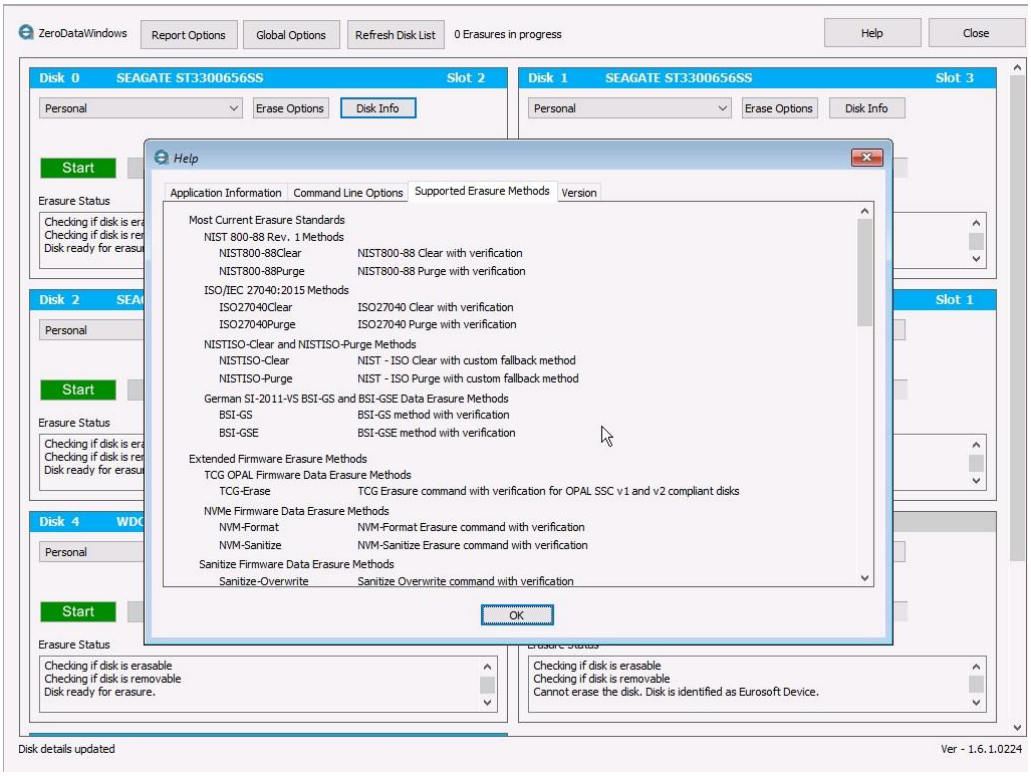
Help button opens the Help window containing four tabs. In first tab, details related to application is displayed.



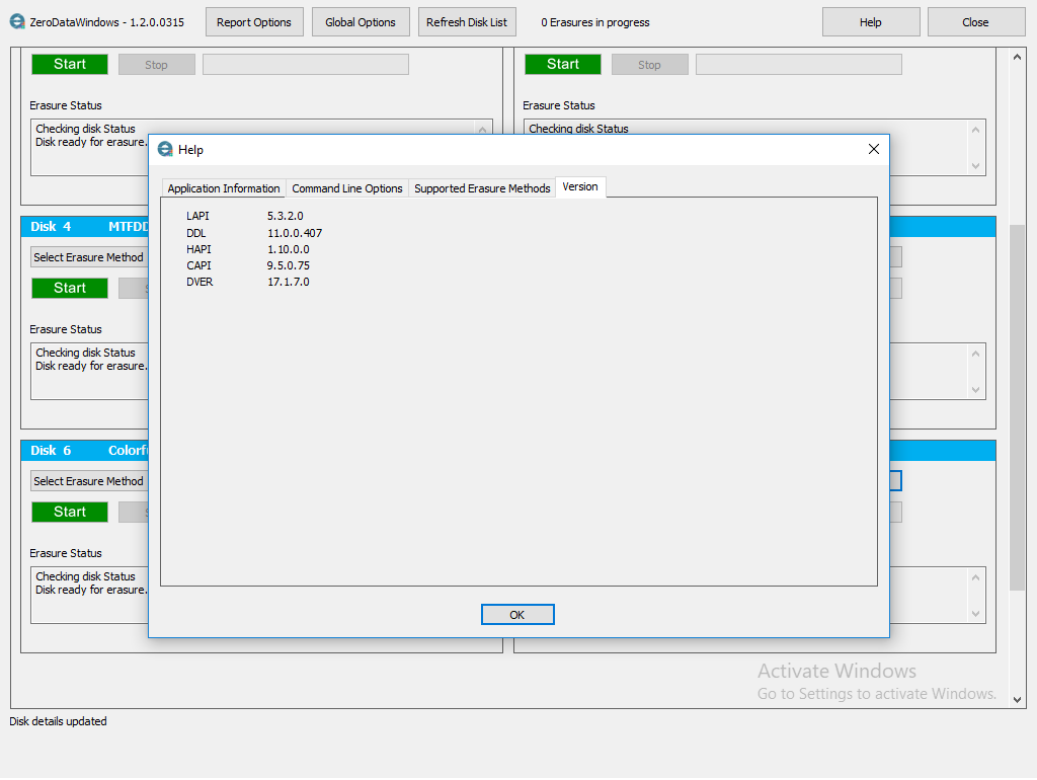
Second tab lists all available command line options.



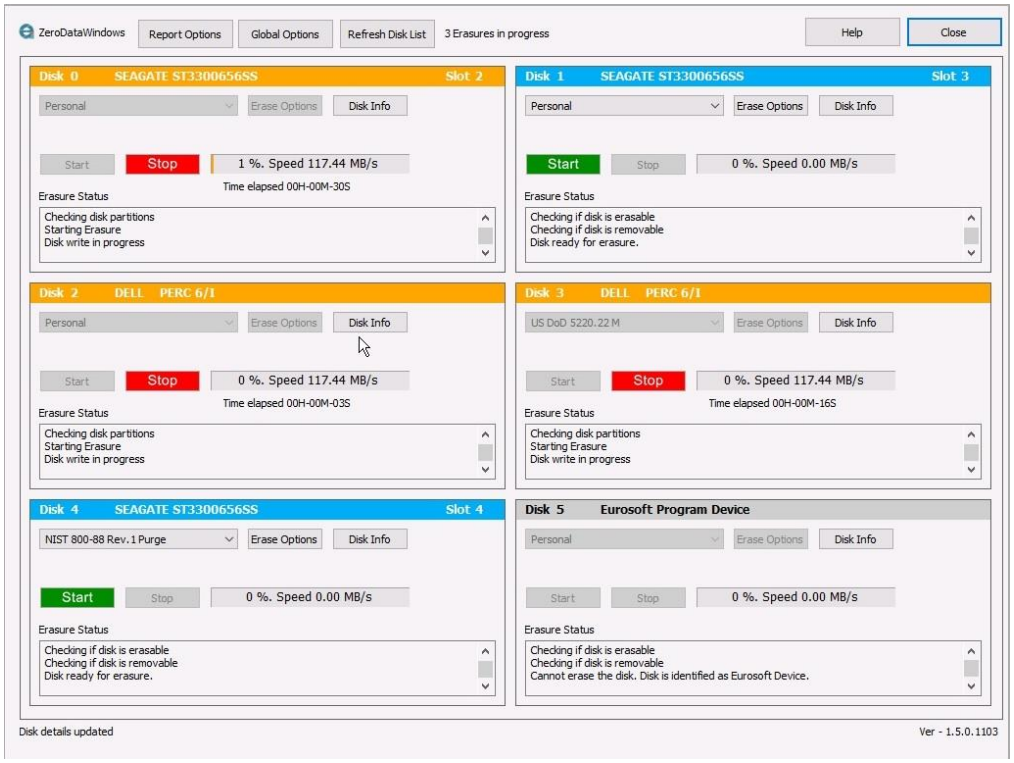
Third tab lists all available erasure methods.



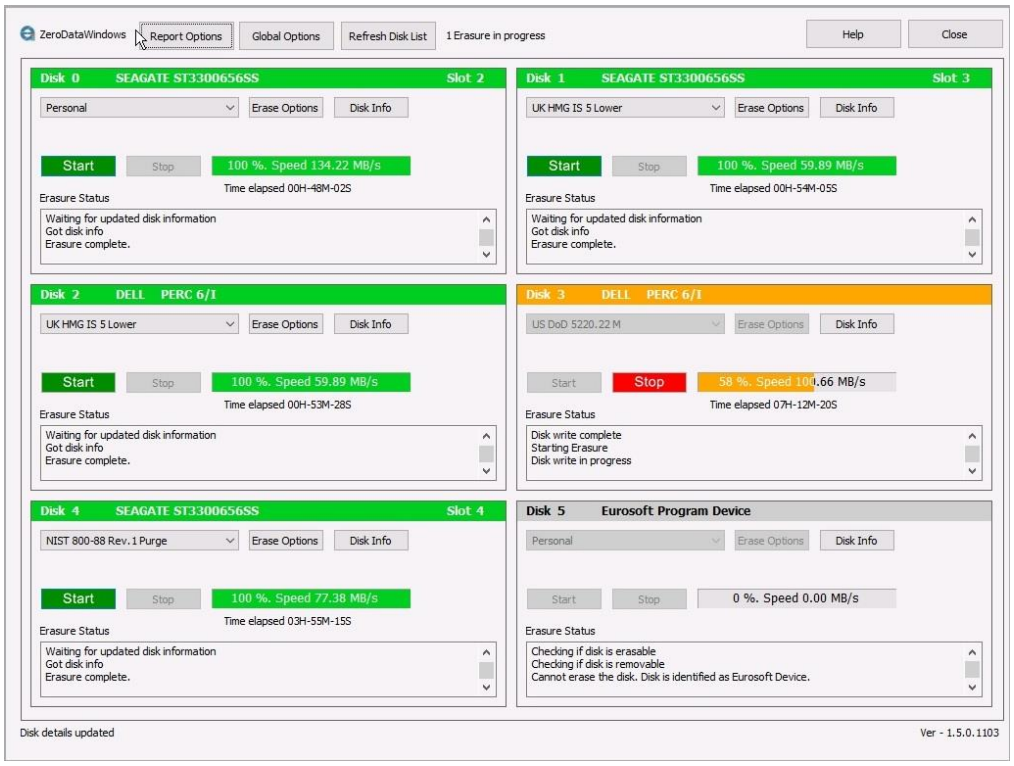
Fourth tab lists version numbers for some internal components.



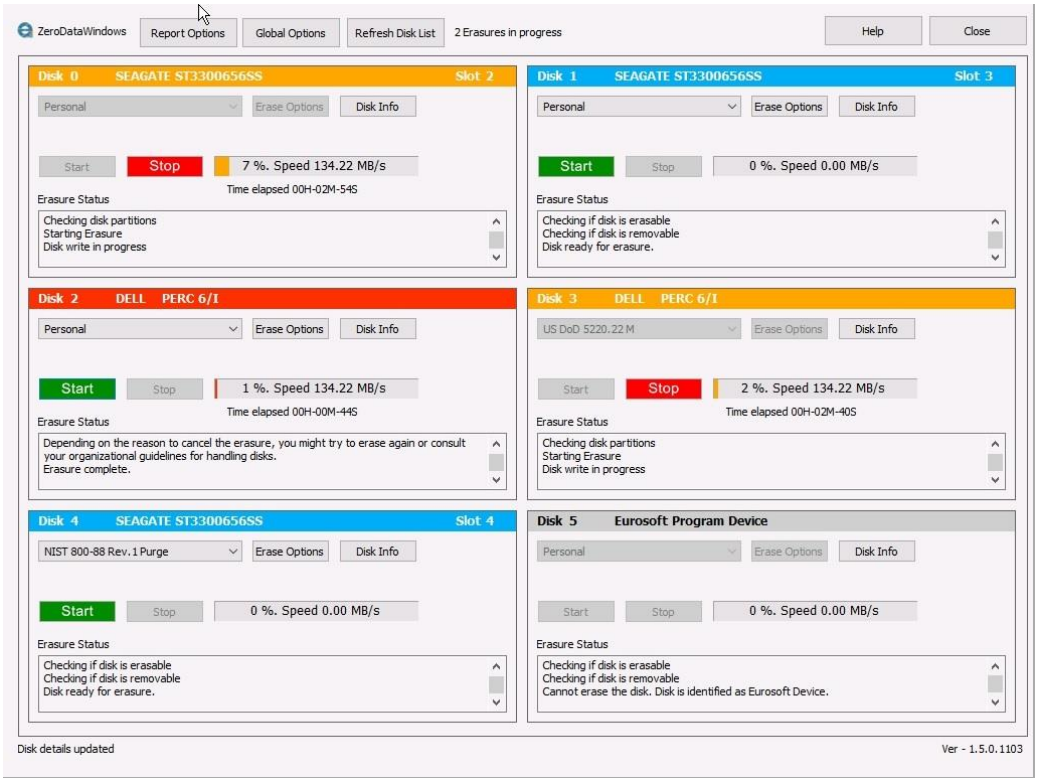
The user can start erasing a disk after selecting an erasure method (and optionally making changes in Erasure Options window) and by clicking on green Start button. Once the erasure starts, the blue header bar will turn to orange, the Start button will be greyed out and the Stop button will turn Red. Erasure progress will be displayed in the orange progress bar and erasure steps will be displayed in the status window. As many disks can be erased in parallel as specified in license file.



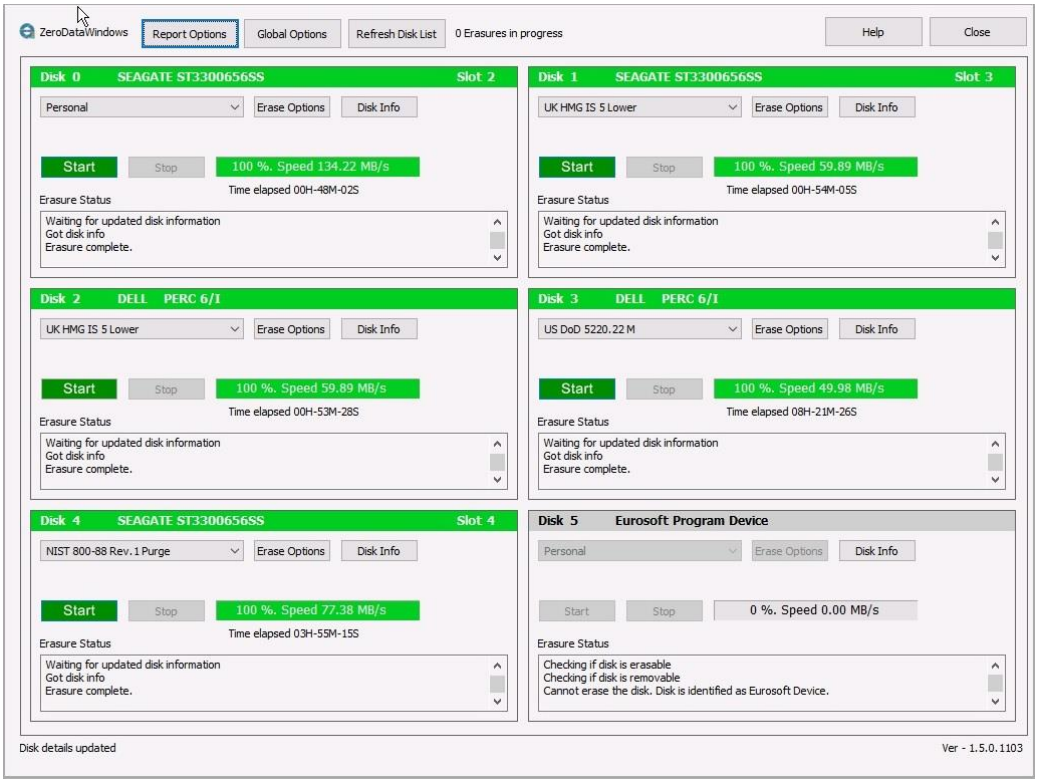
If erasure ends successfully, the blue header bar will turn green, the progress bar will turn green, the Start button will return to its original green color and the Stop button will be greyed out.



In other cases, such as when erasure fails for a reason or erasure is cancelled by user, the blue header bar will turn red.



As you can expect, when all disks are erased successfully, you will see all green screen.



Steps for Starting and Executing ZeroData Windows

Interactive execution of ZeroData Windows follows these steps in sequence:

1. Did you decide on what you need to decide before carrying out disk sanitization ? If not, please go back and decide.

2. Boot computer from the Windows operating system.

3. Presence of hot-plug functionality
    a. If the disk connections do not support hot plug, the disks to be secure erased must be present on the computer at boot time.
    b. If the disk connections support hot plug, the disks to be secure erased can or cannot be present on the computer at boot time. Please refer to documentation of your hot-plug device for its capabilities.

4. ZeroData Windows has built-in precautions to prevent erasure of the following disks:
    a. The OS disk: this is the disk computer has booted from and is different from other disks that might contain operating systems. Especially if the computer is booted to WinPE, other OS disks for that host computer including the one computer was booted from are not protected. If you happen to execute ZeroData Windows in such a case, you must make sure that you are not secure erasing your regular boot disks.
    b. The disk ZeroData Windows is executing from: generally, this disk is the same as the OS disk, but in some cases ZeroData Windows might be executed from a different media like a different USB flash disk or a PXE boot image.
    c. Executing ZeroData Windows with /LD option lists these disks explicitly.

        Based on our extensive testing, we have not encountered a case where above-mentioned disks could be erased using ZeroData Windows. However, please bear in mind to check if the disk to be erased is the one you intend to erase.

    d. In cases where the computer is booted from WinPE and ZeroData Windows is not executed from the WinPE boot disk, the WinPE boot disk can be erased. As WinPE loads itself to computer RAM and then boots from it; the disk containing the WinPE image is not detected as OS disk by Windows. This is a limitation of WinPE and not ZeroData Windows.

5. The following disks can be excluded from the ZeroData Windows erasure run:
    a. All removable disks identified by Windows operating system with a Disk Type “Removable Media”. There are two command line options for this purpose: /DRDE and /XRD, please refer to definition of these command line options to determine which one suits your purpose.
    b. Disks specified by their volume name in calling command line using /XVN parameter. The /XVN parameter can be repeated as many times as required.

        In cases where computer is booted to Windows PE from a removable disk like a USB Flash drive, using one of the above-mentioned parameters needs to be employed to prevent the boot disk from being erased.

6. Browse to the folder where ZeroData Windows files are located.

7. Start a command window or PowerShell window with administrative rights.

8.

a. Execute ZeroData Windows with /EADP parameter to erase as many disks in parallel as specified in license. Use other command line switches to specify how you want erasure to be performed. The general template looks like this:

ZeroData Windows_application_name /EADP {one or more command line switches}

By default, ZeroData Windows application name is “ZeroDataWindows.exe”. It will run even if you rename the application name, however renaming any of the other files will prevent execution.

If no /EADP tag is present, no disk erasure will be carried out and ZeroData Windows will enter interactive mode where disks can be erased by selecting an erasure method and clicking on Start button.

When executing from a command window with a default application name on all disks:

ZeroDataWindows /EADP {one or more command line switches}

When executing from PowerShell window with a default application name on all disks:

.\ZeroDataWindows /EADP {one or more command line switches}

Note that the “.\” characters are required when ZeroDataWindows or any other executable file is called from a PowerShell window.

b. Execute ZeroData Windows with /EADS parameter

ZeroDataWindows /EADS {one or more command line switches} to erase all disks sequentially, one after another.

c. Execute ZeroData Windows with /ID parameter

ZeroDataWindows /ID x {one or more command line switches} to erase only the disk that has ID x.

d. It is possible to exclude disks from erasure. The/XRD command switch excludes all removable disks from erasure. Please refer to relevant section of the manual to learn specifics of these command switches.

More samples are given in Samples for Command Line Option Usage section.

Overview of ZeroData Windows Command Line Options

To execute ZeroData Windows from a Windows command line window, you need to call application name with command line parameters. These parameters are grouped as follows:

- Suppressing Confirmation Messages
- Specifying Which Disks to Erase
- Specifying Automatic Disk Erasure Parameters
- Specifying Removable Disk Erasure Protection
- Specifying Erasure Method Applied To Disks
- Specifying Erasure Method Options For NIST and ISO Erasure Method Execution
- Options For All Firmware Erasure Method Executions
- Specifying Extra Overwrite Passes
- Specifying Post Erasure Options
- Options For Hidden Sector Processing
- Options To Unlock Disks For Erasure
- Options To Enable SCSI / SAS Firmware Erasure Commands
- Options For NVMe Disk Firmware Erasure
- Options For SSD Overwrite Erasure Method Execution
- Specifying Verification Method
- Specifying Output Options
- Specifying Error Handling and Stopping Erasures
- Special Parameters
- Specifying Personnel and Customer Data

The general command line will look like one of the below general cases:

Application_name [mandatory specifying all disks to erase with any combination of parameters]

Specifying which disks to erase is mandatory, other options are optional and defaults are applied in their absence.

If no disk is specified to be erased, then erasure is not carried out and the application starts in interactive mode.

The general form to carry out an erasure is as follows, the items in green color are the minimum parameters to start an erasure from a command line window:

Application_name [Specifying which disks to erase] {Specifying Automatic Disk Erasure Parameters} {Specifying Removable Disk Erasure Protection} {Specifying Erasure Method Applied To Disks} {Specifying Erasure Method Options For NIST and ISO Erasure Method Execution} {Options For All Firmware Erasure Method Executions} {Specifying Extra Overwrite Passes} {Specifying Post Erasure Options} {Options For Hidden Sector Processing} {Options To Unlock Disks For Erasure} {Options To Enable SCSI / SAS Firmware Erasure Commands} {Options For NVMe Disk Firmware Erasure} {Options For SSD Overwrite Erasure Method Execution} {Suppressing Confirmation Messages} {Specifying Verification Method} {Specifying Output Options} {Specifying Error Handling} {Special Parameters} {Specifying Personnel and Customer Data}

The minimum form to carry out an erasure to start an erasure from a command line window is as follows:

Application_name [Specifying which disks to erase] [Specifying Erasure Method Applied To Disks] [Specifying Error Handling]

Description of Command Line Options

To execute ZeroData Windows, you need to call application name with command line options.

When used in a command line, ZeroData Windows options are specified with a "/" character followed by the option identifier. There must be at least one blank character between option identifiers to be recognized; otherwise, the options can't be recognized and processed properly.

Almost all ZeroData Windows option identifiers are short forms of the option names, generally they are made up by adding the first character of the option names together. There are some cases that this convention is not followed.

The option descriptions in following pages are structured in the following manner:

/OptionID < Option Name > < sample use of option identifier preceded by "e.g.," >

Text containing a short description of option.

Minimum Parameters Needed For Disk Erasure

Select one of these :

/EADP **< Erase All Disks in Parallel >** ***e.g., /EADP***

Erases as many disks in parallel as specified in license file (let's say this number is n) - except the boot operating system disk and the disk ZeroData Windows is being executed. In case some disks are faulty or very slow to respond to identification commands, the first batch of n disks may not be the first n disks listed in user interface.

/EADS **< Erase All Disks Sequentially >** ***e.g., /EADS***

Erases all disks sequentially except the boot operating system disk and the disk ZeroData Windows is being executed. Erasure starts with lowest available physical disk ID and moves up to higher ID's. Due to the time required to erase multiple disks in sequence, it is advisable to use in conjunction with /NC AcceptTheRisk option.

/ID **< Drive Physical ID, can occur multiple times >** ***e.g., /ID 1,2,5,29***

Specifies physical disk ID to be erased. In case where more than one disk ID is specified, then these numbers must be separated by commas as shown in the example usage given above.

/ME **< Erase Method >** ***e.g., /ME NIST800-88Purge***

Specifies the erasure method to be applied to specified disk. List of available methods are given in the attachment. When no method is specified, then for magnetic hard disks use Personal method and for solid state disks SSD Standard method are applied.

Note: There is an exception made for NISTISO-Clear and NISTISO-Purge methods, in which case a second method name needs to be supplied. Please see page 43 for details of these methods.

Example:

/me personal /nl 2 /ze /RD 1

In the above example:

all disks will be erased using Personal method and two extra non-linear passes, two zero passes and one random pass will be executed after Personal method.

Note: There is no standard and failsafe method to identify hybrid SSHD disks, these disks are generally identified as HDD, and in very rare cases SSHD's can be identified as SSD. Therefore, there is no guarantee how these disks will be erased.

Minimum Additional Parameters Needed For Specifying Automatic Execution

To specify an automatic erasure, the below given minimum parameters must be added to the "Minimum Parameters Needed For Disk Erasure" described above.

/DNI **< Disable User Interaction >** ***e.g., /DNI***

This option allows the user to disable any user interaction while ZeroData Windows is running. User cannot click anything on the ZeroData Windows application window. If the disk hangs during erasure, there will be no way to stop the erasures as user interface buttons will be disabled. Therefore, application of /DNI switch requires /EC switch to be set. If /DNI switch is set but /EC switch is not set, this will be treated as an error.

/ASD **< Automatic Shut Down >** ***e.g., /ASD***

This option allows the user to automatically shut down ZeroData Windows when all erasure operations end. Disks completing erasure will be displayed on screen as 100% complete until all erasures end the application window is closed.

Highly Recommended Parameters For Disks With Suspected Faults

When it is suspected that one or more disks in an erasure batch run contain some faults, it is important to limit the durations for disk access tries. Especially in refurbishing operations, there will be very bad disks, with lots of re-allocated sectors, bad sectors and poor health status. The below given parameters help to limit time lost when such bad and reallocated sectors are encountered.

/EC **< Maximum Error Count >** ***e.g., /EC 10***

This option sets maximum count of errors encountered during erasure process before erasure operation is stopped. The default for this option is "-1" meaning the erasure will continue until the whole erasure method is applied even if errors are encountered while writing to disk and reading from the disk. To stop erasure process earlier, users can set this option to a value that suits their criteria. Most users will set this count to 1 to identify faulty disks as soon as possible and decommission faulty disks with physical destruction methods.

/DART **< Disk Access Retries Timeout >** ***e.g., /DART 30***

This option sets a timeout limit in seconds for disk access retries. In case a timeout occurs, the operation is cancelled and attempted again.

/DARC **< Disk Access Retry Count >** ***e.g., /DARC 3***

This option sets the number of disk access retries before an error is logged. Especially after firmware erasure commands, some disks need some time to respond to commands that access the disk for read or write operations. By setting the number for Disk Access Retry Count, the user can give the disk time to respond.

/PHFBE **< Minimum Health Percentage Score to Fail Before Erasure >** ***e.g., / PHFBE 80***

This option fails erasure if health percentage score reported by disk firmware before erasure are less than the value specified with this parameter. You can set an acceptable health level for disks before erasure operation and don't attempt to erase disks below that target, eliminating time consuming erasures from your workflow.

/PHFAE **< Minimum Health Percentage Score to Fail After Erasure >** ***e.g., / PHFAE 80***

This option fails erasure if health percentage score reported by disk firmware after erasure are less than the value specified with this parameter. You can set an acceptable health level for disks after erasure operation and attempt to erase all disks, then fail disks with health level below set target after doing your best to erase any trace of data.

Suppressing Confirmation Messages

/NC AcceptTheRisk **< Suppress Confirmation Dialogs >** ***e.g., /NC AcceptTheRisk***

If fully automated mode of operation is required, dialogs asking for interactive input must be suppressed. By specifying "/NC AcceptTheRisk" users are confirming that they are aware of the effects of the set command options, what will be carried out on selected disks based on these settings and they do not want to deal with interactive confirmation dialogs.

Specifying Which Disks to Erase

/EADP **< Erase All Disks Parallel >** ***e.g. /EADP***

Erases as many disks in parallel as specified in license file (let's say this number is n) - except the boot operating system disk and the disk ZeroData Windows is being executed. In case some disks are faulty or very slow to respond to identification commands, the first batch of n disks may not be the first n disks listed in user interface.

/EADS **< Erase All Disks Sequential >** ***e.g., /EADS***

Erases all disks sequentially except the boot operating system disk and the disk ZeroData Windows is being executed. Erasure starts with lowest available physical disk ID and moves up to higher ID's. Due to the time required to erase multiple disks in sequence, it is advisable to use in conjunction with /NC AcceptTheRisk option.

/ID **< Drive Physical ID, can occur multiple times >** ***e.g., /ID 1,2,5,29***

Specifies physical disk ID to be erased. In case where more than one disk ID is specified, then these numbers must be separated by commas as shown in the example usage given above.

Specifying Automatic Disk Erasure Parameters

/DNI **< Disable User Interaction >** ***e.g., /DNI***

This option allows the user to disable any user interaction while ZeroData Windows is running. User cannot click anything on the ZeroData Windows application window. If the disk hangs during erasure, there will be no way to stop the erasures as user interface buttons will be disabled. Therefore, application of /DNI switch requires /EC switch to be set. If /DNI switch is set but /EC switch is not set, this will be treated as an error.

/ASD **< Automatic Shut Down >** ***e.g., /ASD***

This option allows the user to automatically shut down ZeroData Windows when all erasure operations end. Disks completing erasure will be displayed on screen as 100% complete until all erasures end the application window is closed.

Specifying Removable Disk Erasure Protection

/DRDE **< Disable Removable Disk Erasure >** ***e.g., /DRDE***

Disables erasure of removable disks like USB flash disks and media cards. Although they are not erased, removable disks are also checked for erasure and their presence and information are reported in erasure logs.

/XRD **< Exclude Removable Disks from Erasure >** ***e.g., /XRD***

Prevents removable devices being added to erasure queue and therefore excludes them from erasure. Although disks may be present in USB ports or media card readers, they are not checked and not reported in erasure logs.

/XVN **< Exclude Volume Name, can occur multiple times >**

e.g., /XVN "Eurosoft Test Device","Vol1","Data","Win10","OS"

Specifies one or more disks identified by its volume name to be excluded from erasure. The Volume Name is the Volume Name displayed to the user on Windows Disk Manager; in case there are blank characters in Volume Name, they must be specified within quotation marks. If the user has specific disk(s) that he does not want to erase but those disks must be attached to the computer while disks are erased, then all those disks can be input as command line parameters separated by commas as shown in the example usage given above.

Specifying Erasure Method Applied To Disks

/ME **< Erase Method >** ***e.g., /ME NIST800-88Purge***

Specifies the erasure method to be applied to specified disk. List of available methods are given in the attachment. When no method is specified, then for magnetic hard disks use Personal method and for solid state disks SSD Standard method are applied.

Note: There is an exception made for NISTISO-Clear and NISTISO-Purge methods, in which case a second method name needs to be supplied. Please see page 43 for details of these methods.

Example:

/me personal /nl 2 /ze /RD 1

In the above example:

all disks will be erased using Personal method and two extra non-linear passes, two zero passes and one random pass will be executed after Personal method.

Note: There is no standard and failsafe method to identify hybrid SSHD disks, these disks are generally identified as HDD, and in very rare cases SSHD's can be identified as SSD. Therefore, there is no guarantee how these disks will be erased.

/HDD **< optional /ME, /ZE, /RD, /NL parameters >**

e.g., /HDD /ME NistISO-Purge USDoD /ZE 1 /RD 1 /NL 2

On some systems a combination of magnetic HDD and electronic SSD may be present, and the erasure organization might be required to use different erasure methods for SSD and HDD. With this option a specific erasure method can be applied to disks identified as HDD 's.

In above sample, only HDD's will be attempted to be erased using NistISO-Purge method, when NistISO-Purge fails USDoD method will be executed as fallback erasure method; after erasure operation ends, one zero, one random and two non-linear overwrite passes will be applied only to HDD's.

/HDD can be used in combination with /ME and /SSD parameters.

Example:

/me personal /nl 2 /hdd /me nistiso-purge usdod /ze 2 /ssd /me nistiso-purge ssdstandard /nl 1

In the above example:

all disks will be erased using Personal method and two extra non-linear passes will be executed after Personal method.

- disks identified as HDD will be erased using NistISO-Purge method, if NistISO-Purge method fails, then disks will be erased using US DoD method; then two extra zero passes and two non-linear passes will be applied on top the executed erasure method.

- disks identified as SSD will be erased using NistISO-Purge method, if NistISO-Purge method fails, then disks will be erased using SSDStandard method, and only one non-linear pass will be executed on top of the executed erasure method.

Note: There is no standard and failsafe method to identify hybrid SSHD disks, these disks are generally identified as HDD, and in very rare cases SSHD's can be identified as SSD. Therefore, there is no guarantee how these disks will be erased.

/SSD **< optional /ME, /ZE, /RD, /NL parameters >**

e.g., /SSD /ME NistISO-Purge Personal /ZE 1 /RD 1 /NL 2

On some systems a combination of magnetic HDD and electronic SSD may be present, and the erasure organization might be bound to use different erasure methods for SSD and HDD. With this option a specific erasure method can be applied to disks identified as SSD's.

In above sample, only SSD's will be attempted to be erased using NistISO-Purge method, NistISO-Purge it fails Personal method will be executed as fallback erasure method; after erasure operation ends, one zero, one random and two non-linear overwrite passes will be applied only to SSD's.

/SSD can be used in combination with /ME and /HDD parameters.

Example:

/me personal /nl 2 /hdd /me nistiso-purge usdod /ze 2 /ssd /me nistiso-purge ssdstandard /nl 1

In the above example:

- all disks will be erased using Personal method and two extra non-linear passes will be executed after Personal method.
- disks identified as HDD will be erased using NistISO-Purge method, if NistISO-Purge method fails, then disks will be erased using US DoD method; then two extra zero passes and two non-linear passes will be applied on top the executed erasure method.
- disks identified as SSD will be erased using NistISO-Purge method, if NistISO-Purge method fails, then disks will be erased using SSDStandard method, and only one non-linear pass will be executed on top of the executed erasure method.

Note: There is no standard and failsafe method to identify hybrid SSHD disks, these disks are generally identified as HDD, in very rare cases SSHD's can be identified as SSD. Therefore, there is no guarantee how these disks will be erased.

Options For NIST and ISO Erasure Method Execution

/NIEREM < NIST/ISO27040 Optional and Extra Method Application > *e.g., /NIEREM 1*

NIST 800-88 Revision 1 standard (nist800-88purge and nist800-88clear erasure methods in ZeroData Windows) and ISO/IEC 27040 standard (iso27040purge and iso27040clear erasure methods in ZeroData Windows) define a data destruction procedure in a clearly stated sequence. On top of these "standard" sequences, there are "optional" sequences of steps that can be applied as well. Based on customer feedback, this functionality has been extended to allow extra sequence of steps with this parameter.

Command line execution of this option is as follows:

zerodatawindows.exe /me nist800-88purge /nierem { 0 | 1 } ...

where

/nierem 0 executes the "optional sequence of steps defined in NIST 800-88 Revision 1 and ISO/IEC 27040 standards. See details on respective erasure method descriptions.

/nierem 1 adds a new sequence of steps NIST 800-88 Revision 1 and ISO/IEC 27040 standards, first the "default" sequence of steps is applied - if the last executed step of data erasure is a successfully executed and verified firmware command, then an extra write zeroes pass is applied to the disk and a verification pass is applied. If the last executed step of data erasure executed is a successfully executed and verified regular overwrite pass, then no extra write zeroes pass is applied to the disk.

/NIELVL < NIST/ISO27040 overwrite level, 0 = default, 1 = Long > *e.g. /NIELVL 1*

Firmware overwrite related methods have two options: default overwrite and long overwrite. If this parameter is not specified, then the default method is applied for SANITIZE Overwrite and regular disk write passes which is a single pass. In case /NIELVL 1 is specified, then the long method is applied: for SANITIZE Overwrite, this corresponds to 3 overwrite passes and 1 invert pass; for regular disk write, this corresponds to 2 random passes.

/NIELVL parameter should only be specified for NIST800-88Purge, NIST800-88Clear, ISO27040Purge and ISO27040Clear methods. If any other method is specified, this option is discarded.

Options For All Firmware Erasure Method Executions

/FFV **< Apply Fast Verification for Firmware Commands >** ***e.g., /FFV***

Applicable for all firmware erasure methods. When specified, ZeroData Windows uses a carefully selected 1.6 GB of disk space for verifying erasure effectiveness. Is not applied to overwrite erasure methods.

/TFF **< Test Firmware Erasure Commands First Before Actual Erasure >** ***e.g., /TFF***

Applicable for all firmware erasure methods. When specified, if erasure method specified by /ME parameter contains a firmware erasure command, ZeroData Windows applies firmware erasure commands first to check if these commands are really supported by the disk and if these commands really work. Is not applied to overwrite erasure methods.

As an optimization, we suggest you add the "/tff" parameter to your command line.

If an erasure method involves firmware erasure commands, ZeroData Windows follows NIST 800-88 Rev 1 / ISO 27040 procedure, namely:

1. write test pattern,
2. verify the test pattern,
3. run firmware command,
4. verify test pattern.

However, we came across disks which report to support a specific firmware erasure command, but that command fails every time we attempt it. In these cases, time spent on the three steps involving writing and verifying test pattern on 10% of the disk is wasted.

Based on customer feedback, we have developed /tff (test firmware command first) parameter.

If /tff is used, ZeroData Windows tries to execute firmware erasure command(s) - except those perform a full disk overwrite operation internally - without any preliminary step. If firmware erasure command(s) is successful, then steps 1 to 4 are carried out as defined in the erasure method; if firmware erasure command(s) is not successful, then all the steps 1 – 4 are skipped. In cases where the firmware command in question performs a full disk overwrite internally, then steps 1 – 4 are executed in sequence.

From erasure duration perspective, the actual firmware command(s) takes much less than a minute, but steps 1, 2 and 4 take multiple minutes: by using /tff, multiple minute losses can be prevented, and I worst case the time loss is small as the risk of increased erase duration is "much less than a minute to execute the firmware command(s)".

Specifying Extra Overwrite Passes

/NL **< Number of Additional Non-Linear Passes >** ***e.g., /NL 2***

Specifies the number of additional non-linear passes that will be applied after the selected method is executed. It can be any number between 1 and 99. If not specified, no additional passes will be applied.

/ZE **< Number of Additional Zero Passes >** ***e.g., /ZE 5***

Specifies the number of additional zero passes that will be applied after the selected method is executed. It can be any number between 1 and 99. If not specified, no additional passes will be applied.

/RD **< Number of Additional Random Passes >** ***e.g., /RD 2***

Specifies the number of additional random passes that will be applied after the selected method is executed. It can be any number between 1 and 99. If not specified, no additional passes will be applied.

Specifying Post Erasure Options

/DI **< 0.1 % Disk Initialization >** ***e.g., /DI***

Specifies a disk initialization pass as last pass that will be applied after the selected method is executed. If not specified, no initialization will be applied.

/WFP **< Write Fingerprint to First Sector After Erasure >** ***e.g., /WFP***

This option writes a short bootable fingerprint containing information on disk erasure to first sectors of the disk.

/LDS **< Log Disk Sectors>** ***e.g., /LDS 0-1***

In some cases, logging contents of some disk sectors after erasure might be desired, generally several sectors from the beginning of the disk are logged as a visual proof of successful disk erasure. /LDS parameter is designed for this purpose. When this parameter is specified in the command line, contents of specified sectors are logged into the log files and these logged sector contents are output in reports. When used in combination of /WFP parameter described above, it can be used to log the contents of bootable erasure fingerprint. For example, when the command line to execute ZeroData Windows has /WFP switch to write a bootable fingerprint report to erased disks, adding "/LDS 1" to command line switches will output the contents of sector 1 of erased disks to logs and reports - as the bootable fingerprint contents are written to sector 1, the fingerprint written to the disk will be dumped to logs and reports of erased disks.

The following examples show how this parameter can be used.

/LDS 1 ***log disk sector 1 into log files and reports***

/LDS 0-1 ***log disk sector 0 to sector 1 into log files and reports***

/TDO **< Take Disks Offline >** ***e.g., /TDO***

When this option is used, disks are taken offline after erasure. This option is particularly useful when disks are taken out of computers and erased in bulk at erasure stations. However, if it is used when ZeroData Windows is used as part of system refurbishing workflow and boot images will be installed to systems after erasure, then imaging will fail as disks will be offline.

Options For Hidden Sector Processing

/DHAR **< Disable Hidden Area Removal >** ***e.g., /DHAR***

Secure erasure procedures require removal of hidden areas that may be present on the disks. By default, hidden area removal is attempted to remove any hidden areas like DCO and HPA partitions before starting the overwriting passes. Removal of hidden areas requires firmware commands to be applied to the disk and then requires the disk to be removed and reinstalled after successful removal of hidden areas. Therefore, if hidden areas are found and removed, the erasure operation ends. To secure erase the disk, erasure must be attempted again.

/EHAF **< Exit If Hidden Area Found >** ***e.g., /EHAF***

Secure erasure procedures require removal of hidden areas that may be present on the disks. By default, hidden area removal is attempted to remove any hidden areas like DCO and HPA partitions before starting the overwriting passes. However, there may be cases when hidden area removal is not desired and erasure must be labeled as failed. In this case /EHAF parameter can be used.

/IDSC **< Ignore Disk Sector Count >** ***e.g., /IDSC***

Success of hidden area removal is determined by comparing number of sectors reported by disk before and after hidden area removal. A temporary disk status and number of sectors value is written to the disk before disk is rebooted. After reboot, these values are retrieved from the disk and compared to current number of sectors. On some disks, this process fails, and the disk enters a reboot loop. /IDSC parameter bypasses this loop and applies erasure.

Options To Unlock Disks For Erasure

/PASS **< User Supplied Password to Unlock the Disk >** ***e.g., /PASS Disk Password***

ZeroData Windows has a built-in list of passwords to unlock disks if they are locked. In cases where passwords do not work or the user has knowledge of a usable password, it can be supplied using /PASS switch and ZeroData will use this password.

/PT **< Password Type Supplied by User >** ***e.g., /PT 1***

There are two types of passwords to unlock a disk: User or Master, consequently the user can supply one of these passwords and must declare which password he supplies. Possible values are 0: user password, 1: master password.

/OUUP **< Only Use User Password >** ***e.g., /OUUP***

By default, ZeroData Windows uses passwords from the inbuilt list to unlock a disk, after that the user supplied password is used. If /OUUP is supplied, the inbuilt list is skipped and only user supplied password is applied to the disk.

Options To Enable SCSI / SAS Firmware Erasure Commands

/DSP **< Disable SAS Firmware Erasure Protection >** ***e.g., /DSP***

Almost all existing SAS RAID controllers block firmware erasure commands sent to disk connected to them and pure SAS controller cards that do not block firmware commands are rarely used. Some SAS RAID controllers show an aggressive behavior to maintain RAID volume integrity and regularly check disks attached to them, even if they are not part of any RAID volume. As these checks break execution of firmware erasure commands and render the disk unusable, ZeroData Windows does not apply firmware erasure commands by default. If /DSP is present in command line, this protection is lifted, and firmware erasure commands are passed to the SAS controller.

Options For NVMe Disk Firmware Erasure

/DNDC **< Disable NVMe Driver Change >** ***e.g., /DNDC***

As standard Microsoft NVMe driver blocks firmware erasure commands, ZeroData Windows swaps NVMe driver when it is started by default to issue these commands. However, some rare NVMe disk models reject this driver swap operation and reboot the computer. For such cases, using this option will disable swapping NVMe driver change operation.

/DNBL **< Disable NVMe Blacklist >** ***e.g., /DNBL***

Some rare NVMe disk models reject firmware erasure commands or do not accurately report supported firmware erasure commands. ZeroData Windows keeps a list of known disks that cause this behavior as they are reported by customers and firmware erasure is not executed on these known disks. If, for some reason, it is wanted to disable this list of known disks, using this option needs to be used.

/DCD **< Delay while doing a driver change in seconds >** ***e.g., /DCD 60***

On some systems a delay needs to be present for driver change to be successful. With this option a specific delay duration can be specified in seconds.

Options For SSD Overwrite Erasure Method Execution

/SDO **< SSD Disk Optimization Before Overwrite Erasure >** ***e.g., /SDO FITQ***

Firmware methods are the preferred erasure methods for solid state disks; however, these erasure methods cannot be executed every time and erasure operations must use regular overwrite passes. As explained in Appendices A, B and D, solid state disk erasure speeds are not always acceptable due various reasons.

Even if they are not firmware commands, experimental studies have shown that some operations have a positive effect on regular overwrite speeds which in turn leads to shorter erasure durations. Four of these operations are combined under /SDO parameter.

These operations and their option names are as follows :

- F – Write 1.6 GB of data to random locations on the disk and read back from these locations, basically apply first two steps of /FFV option.
- I – Initialize the SSD disk
- T – Apply SSD TRIM operation
- Q – Apply Quick Format on SSD disk

/SDO parameter can accept one or more of these options, and the options can be written in any sequence. Regardless of the written sequence, execution sequence will always be F → I → T → Q .

For example,

- if the /SDO is specified like ***… /SDO QIF …,*** then, execution sequence will be F → I → Q.
- if the /SDO is specified like ***… /SDO FQT …,*** then, execution sequence will be F → T → Q.
- if the /SDO is specified like ***… /SDO FQT …,*** then, execution sequence will be F → T → Q.
- if the /SDO is specified like ***… /SDO FQTI …,*** then, execution sequence will be F → I → T → Q.

Specifying Verification Pass Parameters

/VP **< Verification Percentage >** ***e.g., /VP 1***

ZeroData Windows allows the user to set percentage of data to be verified of last overwrite pass. This value can be set between 1 and 100. Default value is 1, meaning 1% of data written in previous overwriting pass is verified.

/PV **< Pass Verification >** ***e.g., /PV All***

ZeroData Windows allows the user to set at which passes verification will be carried out. The available options are

- All: a verification pass will be executed after each overwriting pass
- Last: a verification pass will be executed after the last pass
- None: none of the verification passes defined in the erasure method are executed

If this option is not set, then verification is carried out as defined by the erasure method.

/PR **< Max. Pass Retries if Verification fails >** ***e.g.,/PR 1***

ZeroData Windows allows the user to set the number of times to retry the last overwrite pass that has failed verification. If this option is not set, then the default value of 1 is applied, meaning the pass that failed verification will be repeated once and verification will be attempted again.

As an example, assume “/PV Last /PR 3” are specified for an erasure method. Then after the last write pass, verification will be attempted.

- If verification fails, then the last write pass will be executed again and pass verification will be attempted again, and value of PR will be set to 1.
- If verification fails again, then the last write pass will be executed again and pass verification will be attempted again , and value of PR will be set to 2.
- If verification fails again, then the last write pass will be executed again and pass verification will be attempted again, and value of PR will be set to 3.

If verification fails again, no more pass retries will be attempted and erasure operation will stop.

Specifying Output Options

Default File Name

When ZeroData Windows is executed without specifying a file name,

- a default file name in the form of “date-time + erasure UUID” are used for files,
- however, a default file name in the form of “date-time + erasure UUID + Disk ID + Disk Serial Number + Disk World Wide Number + Date + Time” are assigned automatically to log files,
- notice that date-time occurs at the start of the file name and date + time occurs at the end of file name. The second date + time information is added to distinguish files in cases where a disk is erased multiple times in the same erasure session – which is possible when ZeroData Windows is used to erase disks manually from the user interface,
- If file type is not explicitly specified with /RFT option, then default file type of XML will be applied to all files,
- Report files will be added “_rep”, log files will be added “_log” to their ends.

/GDER **<Generate Report Each Disk Erasure >** ***e.g., /GDER***

By default, an erasure report is created when all disk erasures complete and ZeroData Windows is shut down. Using this option, an erasure report is created for each disk when erasure of the disk ends, without waiting for ZeroData Windows to complete all erasures and shut down.

/GOF **< Global Output File Name >** ***e.g., /GOF GOFile***

This option sets the name for log and report files, extensions for file types like TXT and XML are attached automatically. The file name string can be up to 128 characters. If surrounding “ and “ characters are used, then surrounding “ and “ characters around the file name string will use up 2 characters from the allowed 128 characters.

If this option is specified,

- a default file name in the form of “global output file name + erasure UUID” are used for files,
- the log files name will be in the form of “global output file name + erasure UUID + Disk ID + Disk Serial Number + Disk World Wide Number + Date + Time”,
- If file type is not explicitly specified with /RFT option, then default file type of XML will be applied to all files,
- Report files will be added “_rep”, log files will be added “_log” to their ends.

/NUUID **< No Default Values Added To Combined Log and Report Filenames >** ***e.g., /NUUID***

As ZeroData Windows file names are unique, it is not possible to have an exact file name. In cases where an exact file name is required for combined log and report file names – for example, for the sake of processing logs and reports in scripts that expect a static file name or a file name with a different naming convention -, this option can be used.

Important : Windows operating system does not allow multiple files with the same name to be located under a folder, and a new file with the same name will be written over the old file already present in the folder. Therefore, using exact file names without any timestamps or UUID values is not a good idea if the user wants to store all output files in a single folder and batch process them to create reports later. Therefore /NUUID must be used be very carefully.

/OFP **< Output File Path >** ***e.g., /OFP "e:\erase-logs"***

By default, ZeroData Windows output files are generated under a folder named Logs under application root folder. It is possible to change output file folder with this parameter. File paths must follow standard Windows file path format and must be enclosed in double quotes for them to be correctly recognized by Windows operating system. The output file path string can be up to 60 characters including surrounding " and " characters.

/UTF **< Use Temporary Folder for Output Files >** ***e.g., /OFP "e:\erase-logs" /UTF***

This option writes erasure logs to the "Logs" folder as temporary folder before copying output files to the folder specified using the /OFP parameter.

/LFN **< Specific Log File Name >** ***e.g., /LFN LogFile***

This option sets a specific name applied only to log files; report files will not be affected. "_log" will be added to the end. The file name string can be up to 60 characters including surrounding " and " characters. The log name supplied with /LFN parameter takes precedence over name supplied with /GOF parameter.

/RFN **< Specific Report File Name >** ***e.g., /RFN Refile***

This option sets a specific name applied only to report files, log files will not be affected. "_rep" will be added to the end. The file name string can be up to 60 characters including surrounding " and " characters.

/RFT **< Report File Type (combination of XML, TXT, PDF) >** ***e.g., /RFT TXT***

This option sets specific format applied only to report files, log files will not be affected. Available options are:

- TXT: to set report files to be output as text file
- XML: to set report files to be output as XML files
- PDF: to set report files to be output as PDF files
- XP: to set report files to be output as both XML and PDF files
- XT: to set report files to be output as both XML and text files
- XTP: to set report files to be output as XML, text and PDF files

/EDL **< Enable Debug Log >** ***e.g., /EDL***

This option creates two log files called "EDopLog.txt" and "EDHxaLog.xml" which are used to debug potential issues.

/LTP **< Log Throughput >** ***e.g., /LTP 1***

This option should not be run unless asked by Eurosoft support. It creates log files to track read and write speeds for erasure passes. There are two parameters, 1 and 2, each creating a different file with different content.

Specifying Error Handling and Stopping Erasures

/EC **< Maximum Error Count >** ***e.g., /EC 10***

This option sets maximum count of errors encountered during erasure process before erasure operation is stopped. The default for this option is “-1” meaning the erasure will continue until the whole erasure method is applied even if errors are encountered while writing to disk and reading from the disk. To stop erasure process earlier, users can set this option to a value that suits their criteria. Most users will set this count to 1 to identify faulty disks as soon as possible and decommission faulty disks with physical destruction methods.

/RWERC **< Read Write Error Retry Count >** ***e.g., /RWERC 10***

This option sets count of retries when a read or write error is encountered during erasure process. By default, this value is set to 0, meaning no retries will be carried out.

As an example, assume /RWERC 2 is specified. If a write or read error is encountered, then the operation will be attempted again on the location that gave error (RWERC = 1). If a write or read error is encountered again, then the operation will be attempted again on the location that gave error (RWERC = 2). If a write or read error is encountered, then the operation will not be attempted again on this location as RWERC setting has been reached and operation will be continued on the next location.

/MWR **< Min. Write Rate (MB/s) >** ***e.g., /MWR 1***

This option sets minimum speed encountered during write passes to identify disks with lower write speed set by the user. Deploying a disk with low performance will cause problems for the user of the disk and the organization authorizing the use of low performance disk. The unit of this option is MB/s and default value is set to 1, meaning a disk that has areas with write speeds less than 1 MB/s are identified as faulty and erasure operation is flagged as failed. If /MWREC option is not set, then erasure operation is continued until the erasure method ends regardless of the number of slow disk areas encountered. Fractional values like 0.1 are accepted as well and may prove to be helpful for old removable storage devices like media cards. Negative values are not accepted.

/MWREC **< Min. Write Rate Error Count >** ***e.g., /MWREC 1***

This option sets count of minimum write rate errors encountered during erasure process before erasure operation is stopped. The default for this option is “-1” meaning the erasure will continue until the whole erasure method is applied even if write rate errors are encountered while writing to disk. To stop erasure process earlier, users can set this option to a value that suits their criteria. Most users will set this count to 1 to identify disks with slow performance as soon as possible and decommission faulty disks with physical destruction methods.

/MRR **< Min. Read Rate (MB/s) >** ***e.g., /MRR 1***

This option sets minimum speed encountered during read passes to identify disks with lower read speed set by the user. Deploying a disk with low performance will cause problems for the user of the disk and the organization authorizing the use of low performance disk. The unit of this option is MB/s and default value is set to 1, meaning a disk that has areas with read speeds less than 1 MB/s are identified as faulty and erasure operation is flagged as failed. If /MRREC option is not set, then erasure operation is continued until the erasure method ends regardless of the number of slow disk areas encountered. Fractional values like 0.1 are accepted as well and may prove to be helpful for old removable storage devices like media cards. Negative values are not accepted.

/MRREC **< Min. Read Rate Error Count >** ***e.g., /MRREC 1***

This option sets count of minimum read rate errors encountered during erasure process before erasure operation is stopped. The default for this option is "-1" meaning the erasure will continue until the whole erasure method is applied even if read rate errors are encountered while reading from disk. To stop erasure process earlier, the user can set this option to a value that suits their criteria. Most users will set this count to 1 to identify disks with slow performance as soon as possible and decommission faulty disks with physical destruction methods.

/RWT **< Read / Write Timeout (sec) >** ***e.g., /RWT 5***

This option sets a timeout limit in seconds for disk operations. In case a timeout occurs, the operation is cancelled and attempted again.

/RWTC **< Read / Write Timeout Count >** ***e.g., /RWTC 5***

This option sets maximum count of read / write timeout errors encountered during erasure process before erasure operation is stopped. The default for this option is "-1" meaning the erasure will continue until the whole erasure method is applied even if read/write timeout errors are encountered while reading from disk. To stop erasure process earlier, users can set this option to a value that suits their criteria. Most users will set this count to 1 to identify disks with slow performance as soon as possible and decommission faulty disks with physical destruction methods.

/DART **< Disk Access Retries Timeout >** ***e.g., /DART 30***

This option sets a timeout limit in seconds for disk access retries. In case a timeout occurs, the operation is cancelled and attempted again.

/DARC **< Disk Access Retry Count >** ***e.g., /DARC 3***

This option sets the number of disk access retires before an error is logged. Especially after firmware erasure commands, some disks need some time to respond to commands that access the disk for read or write operations. By setting the number for Disk Access Retry Count, the user can give the disk time to respond.

/FBDSB **< Failing Number of Bad Disk Sectors Before Erasure >** ***e.g., /FBDSB 5***

This option fails erasure if number of bad sectors reported by disk firmware before erasure are more than the value specified with this parameter. You can set an acceptable number of bad sectors for disks before erasure operation and do not attempt to erase disks above that target, eliminating time consuming erasures from your workflow.

/FBDSA **< Failing Number of Bad Disk Sectors After Erasure >** ***e.g., / FBDSA 5***

This option fails erasure if number of bad sectors reported by disk firmware after erasure are more than the value specified with this parameter. You can set an acceptable number of bad sectors for disks after erasure operation and attempt to erase all disks, then fail disks above that target after doing your best to erase any trace of data.

/FWDSB **< Failing Number of Weak Disk Sectors Before Erasure >** ***e.g., / FWDSB 5***

This option fails erasure if number of weak sectors reported by disk firmware before erasure are more than the value specified with this parameter. You can set an acceptable number of weak sectors for disks before erasure operation and do not attempt to erase disks above that target, eliminating time consuming erasures from your workflow.

/FWDSA **< Failing Number of Bad Disk Sectors After Erasure >** ***e.g., / FWDSA 5***

This option fails erasure if number of weak sectors reported by disk firmware after erasure are more than the value specified with this parameter. You can set an acceptable number of weak sectors for disks after erasure operation and attempt to erase all disks, then fail disks above that target after doing your best to erase any trace of data.

/PHFBE **< Minimum Health Percentage Score to Fail Before Erasure >** ***e.g., / PHFBE 80***

This option fails erasure if health percentage score reported by disk firmware before erasure are less than the value specified with this parameter. You can set an acceptable health level for disks before erasure operation and do not attempt to erase disks below that target, eliminating time consuming erasures from your workflow.

/PHFAE **< Minimum Health Percentage Score to Fail After Erasure >** ***e.g., / PHFAE 80***

This option fails erasure if health percentage score reported by disk firmware after erasure are less than the value specified with this parameter. You can set an acceptable health level for disks after erasure operation and attempt to erase all disks, then fail disks with health level below set target after doing your best to erase any trace of data.

Special Parameters

/DNI **< Disable User Interaction >** ***e.g., /DNI***

This option allows the user to disable any user interaction while ZeroData Windows is running. User cannot click anything on the ZeroData Windows application window. If the disk hangs during erasure, there will be no way to stop the erasures as user interface buttons will be disabled. Therefore, application of /DNI switch requires /EC switch to be set. If /DNI switch is set but /EC switch is not set, this will be treated as an error.

/ASD **< Automatic Shut Down >** ***e.g., /ASD***

This option allows the user to automatically shut down ZeroData Windows when all erasure operations end. Disks completing erasure will be displayed on screen as 100% complete until all erasures end the application window is closed.

/FMUP **< ZeroData Free Memory Usage Percentage >** ***e.g., /FMUP 10***

This option allows the user to set the percentage of memory ZeroData Windows can use to store erasure patterns that will be written to disks. Especially for random data streams used in regular overwrite methods, creating a block of random data and writing it to the disk and repeating this sequence takes time and becomes a bottleneck for high-speed SATA, PCIe and NVMe SSD's. To overcome this limitation, ZeroData Windows first creates a buffer in the memory as specified with this parameter and fills it with data pattern; then the disks are fed data from this buffer.

(*) IMPORTANT NOTE: on computers that have active RAM Disk functionality, Windows may fail to report the amount of free RAM correctly. Windows can only report free memory as by taking installed memory and subtracting (the amount of RAM used by Windows and applications and size of data present on the RAM disk). For example, if the computer has 8 GB of RAM, 2 GB is used by Windows and applications and 4 GB of RAM disk with no data on it; then Windows reports amount of free RAM as 6 GB. However, if an application tries to allocate more than 2 GB of memory for the buffer, memory allocation errors occur as 4 GB RAM is allocated to RAM disk and only 2 GB of RAM is available for any application. This is a limitation of Windows and RAM disk software being used and is not related to ZeroData Windows itself.

Specifying Erasure Personnel and Customer Data

/EON **< Erasure Operator Name >** ***e.g., /EON "Operator Name"***

This option allows the user to supply an Erasure Operator Name to be used in reporting the erasure results. THIS INFORMATION IS REQUIRED FOR ERASURE OPERATION TO BE CARRIED OUT, UNLESS "/NC AcceptTheRisk" OR /NEP PARAMETERS ARE PRESENT. If not supplied in the command line, an error message is shown, and erasure will not start.

/ESN **< Erasure Supervisor Name >** ***e.g., /ESN "Supervisor Name"***

This option allows the user to supply an Erasure Supervisor Name to be used in reporting the erasure results.

/NEP **< No Erasure Personnel Details >** ***e.g., /NEP***

This option allows the user to bypass the need to supply an Erasure Operator and/or Supervisor Name to be used in reporting the erasure results.

/ASI **< Add Signature Graphics to PDF reports >** ***e.g., /ASI***

This option outputs graphics files containing scanned signatures of erasure operator and erasure supervisor to sections reserved for this purpose in PDF reports. For successful usage, the following conditions must be met :

- The folder containing the signature scans must be named Signature and must reside in the same folder as ZeroData Windows executable file,
- Scanned signature files must be in PNG format,
- Background color of the signature must be white as ZeroData Windows PDF reports have white background,
- Operator signature file must be named Operator.png,
- Supervisor signature file must be named Supervisor.png,
- The placeholder reserved for both signature files has a width of 400 pixels and a height of 110 pixels. If signature files have different width and height, then they are scaled to fit within placeholder sizes. Having signature files as close to the placeholder scale as possible will prevent issues like incomplete signature images being added to PDF reports. A good rule of thumb for the signature files would be a width to height ration of 4 to 1, meaning the width value of the signature should be 4 times bigger than the height value. For example, a signature file of 960 pixels width by 240 pixels height (width/ height ration is 4 / 1) will have much less problems with being displayed correctly then a signature file of 480 pixels width by 960 pixels height (width / height ratio is 1 / 2).

/CN **< Customer Name >** ***e.g., /EON "Customer Name"***

This option allows the user to supply a Customer Name to be used in reporting the erasure results.

/CL **< Customer Location >** ***e.g., /CL "Customer Location"***

This option allows the user to supply customer location information to be used in reporting the results.

/NCD **< No Customer Details >** ***e.g., /NCD***

This option allows the user to bypass the need to supply Customer Name and/or Customer Location to be used in reporting the erasure results.

/ORD **< Order Date >** ***e.g., /ORD 29-08-2017***

This option allows the user to supply Order Date to be used in reporting the erasure results.

/ORR **< Order Reference >** ***e.g., /ORR "Order Reference"***

This option allows the user to supply order reference information to be used in reporting the erasure results.

/NOD **< No Order Details >** ***e.g., /NOD***

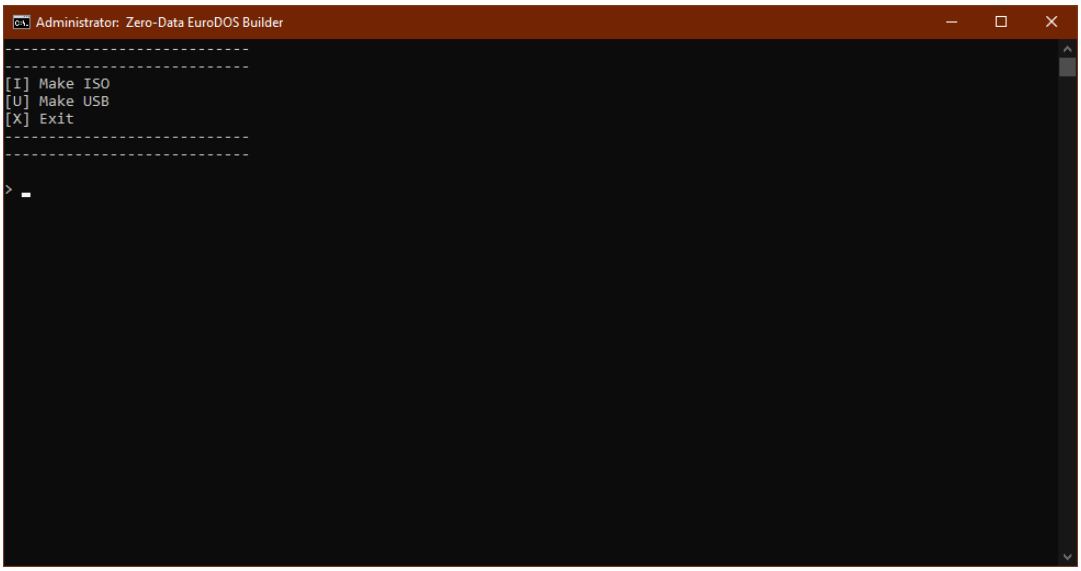
This option allows the user to bypass the need to supply Order Date and/or Order Reference to be used in reporting the erasure results.

Booting ZeroData Legacy Application

ZeroData Windows has roots in original self-boot ZeroData application, which is renamed as ZeroData Legacy as it can only boot on BIOS based older computers. Based on customer requirements, your ZeroData Windows package might include this software tool as well.

To create a self-bootable ZeroData Legacy application, please follow below given instructions.

1) Execute Runme.cmd from the Eurosoft program device **Runme.cmd**



2) Follow the instructions to run the program on your Windows PC; you can select **"Make ISO [I] Make USB [U] or Exit [X]"**.

    a. To create a bootable USB, insert a USB key and select the device volume and drive letter when prompted.

    b. To create a CD/DVD please burn the ISO created in the Pc-Check Custom Media subdirectory in the normal way**.**

    c. Press any key to continue and/or [X] to exit the tool.

    d. Your media is now bootable and can be used in the normal way.

Note: To run Pc-Check EuroDOS on UEFI compliant systems, you must first enable the BIOS Legacy (or CSM) mode and disable secure boot options. Remember to restore the original BIOS settings of the unit under test.

Using ZeroData Windows Reporting Console

ZeroData Windows records a wealth of information in XML log files, and has features to report the results in XML, text, PDF formats; and the user can specify which combination of these three formats are created by processing the log files.

While XML and text reports don't have any .NET dependency, PDF report creation requires basic .NET 4.6 functionality to be present in the operating system. Therefore, the WinPE-NetFX package must be injected into WinPE images.

Note: Microsoft documentation states the following: "Install WinPE-WMI before you install WinPE-NetFX."

Injecting this package is easy when Eurosoft WinPE Image Creator is used to create WinPE boot images. However, we have come across cases where customers are not allowed to inject .NET functionality to older images due hardware limitations and WinPE scratch space settings. In such cases, creation of PDF reports is not possible.

There are also cases where customers don't want to create PDF reports for every erasure but want to have capability to create PDF reports later: for example, when a printable report is asked during an audit or a client asks for printable reports on an individual basis or customers just want to print labels.

ZeroData Windows log and report files provide an audit trail for each operation and employ digital signatures as a means of tamper proofing report files. In theory, digital signatures would assure the recipient of a digital document that the received document has not been tampered with. However, in practice verifying content of digital files based on digital signatures requires a special application fit for the documents sent and digital signature method employed by document issuer.

To address both above-mentioned issues, ZeroData Windows package contains a ZDW_Utilities folder containing ZDWReportingConsole.exe. This application requires administrative rights to run.

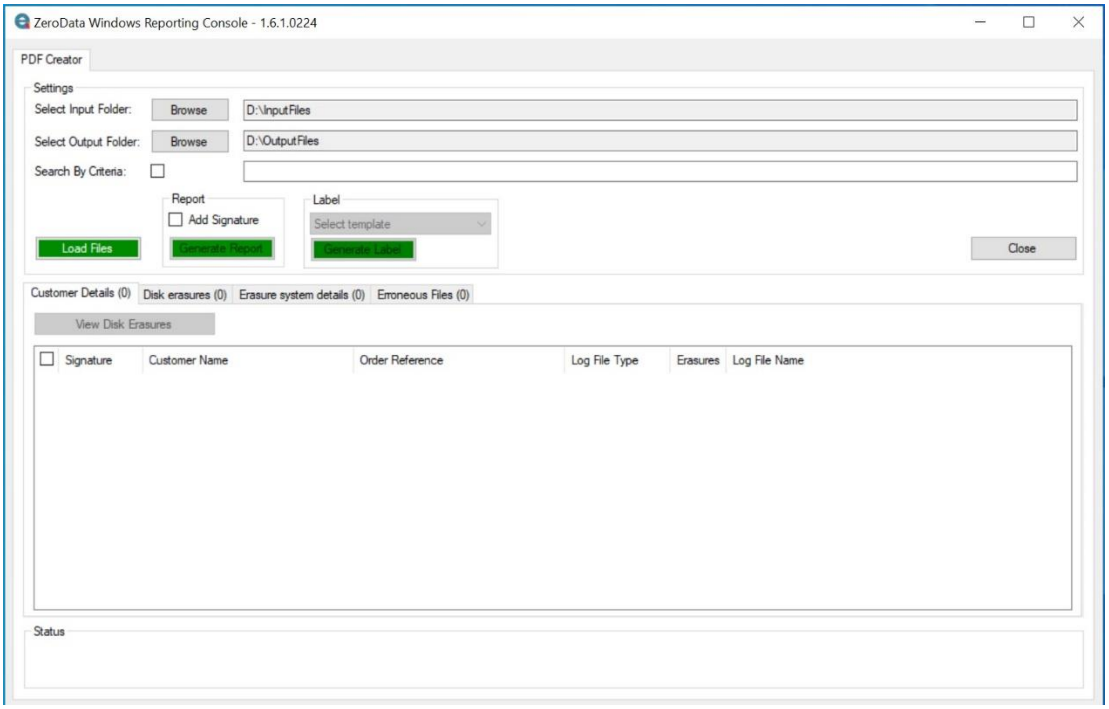
ZeroData Windows Reporting Console uses file names to group relevant files together and treats them as belonging together for processing. For example, files named report1_x_y_z are grouped together and processed together to create report files, whereas files named report2_x_y_z are also grouped together to create report files.

Important : Windows operating system does not allow multiple files with the same name to be located under a folder. Therefore, using exact file names without any timestamps or UUID values is not a good idea if the user wants to store all output files and batch process them to create reports later.

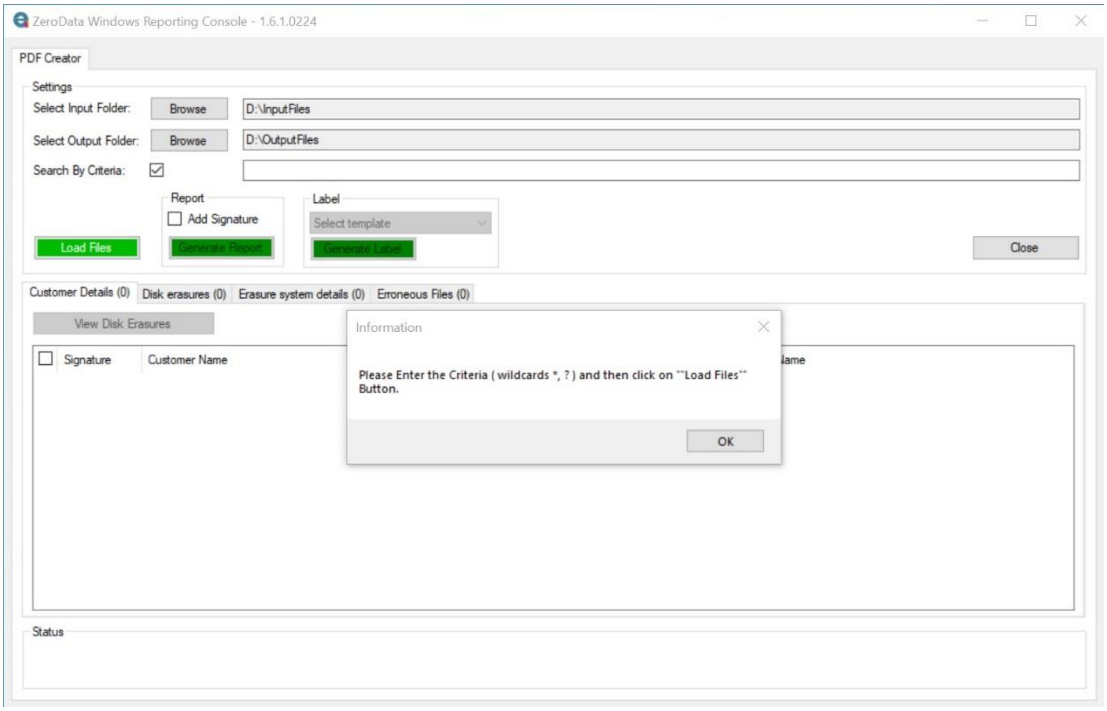
Creating PDF Reports in Reporting Console

When ZDWReportingConsole.exe is started, the user is greeted with focus on PDF Creator tab. The last used input and output folders are populated by default, but the user can change them by clicking on respective Browse button and selecting desired folder.

At this stage, only “Load Files” button is active (denoted by white letters on green background) and other buttons are inactive (denoted by black letters on dark green background).



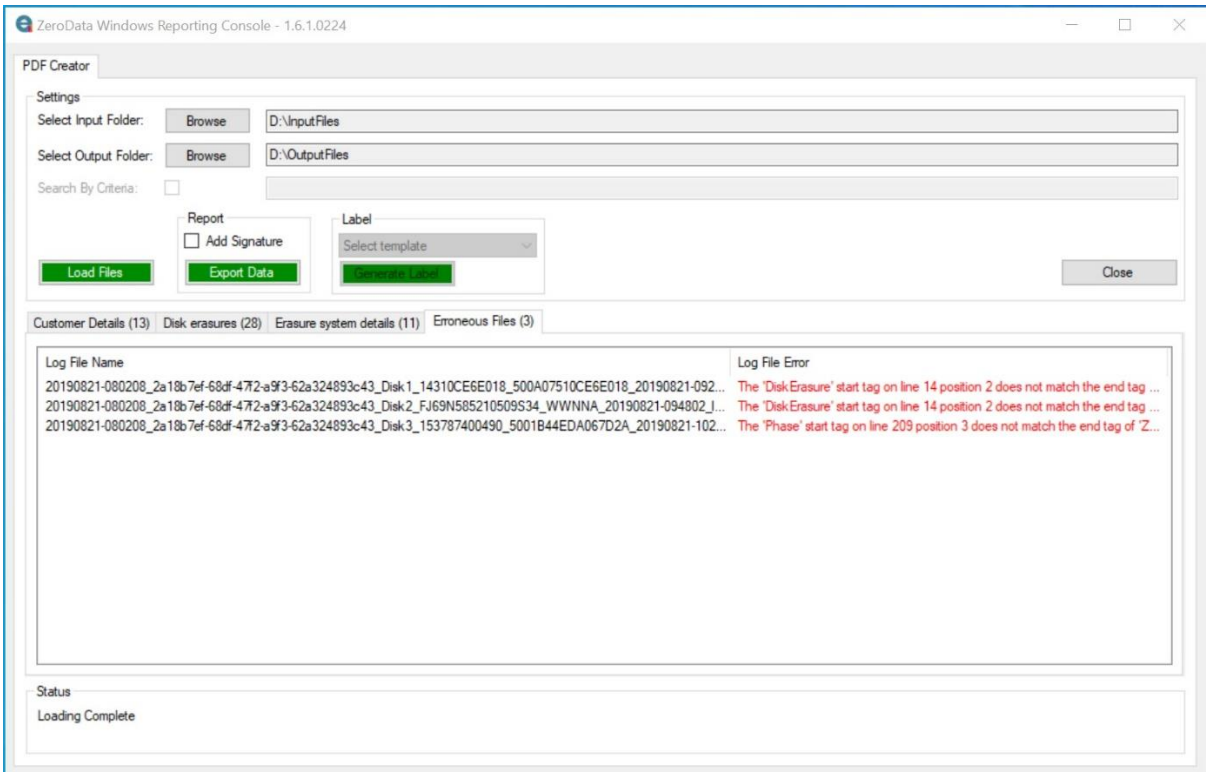
It is also possible to display only files containing certain phrases in their names by clicking on Search by Criteria check box, inputting phrase to search and then clicking on the Load Files button.



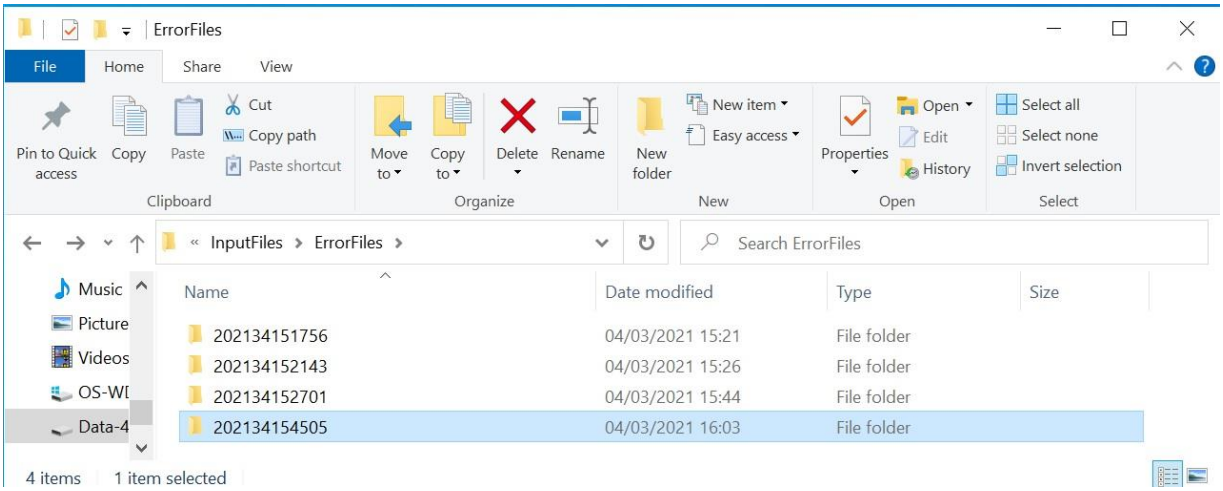
After the Input and Output Folders have been selected and optionally a Search by Criteria phrase is entered, the Load Files button is pressed. Files in input folder will be processed for contents to display disk erasure information.

PDF Creator tab has four different views to group and display erasure logs: Customer Details, Disk Erasures, Erasure System Details and Erroneous Files.

If XML processing errors are encountered while processing the files in the Input Folder, then focus will be in Erroneous Files tab, as shown below. In this tab, files are grouped by Log File Name and a brief description of XML file error that prevented the file to be processed. Notice that the “Generate Report” changes to “Export Data”.



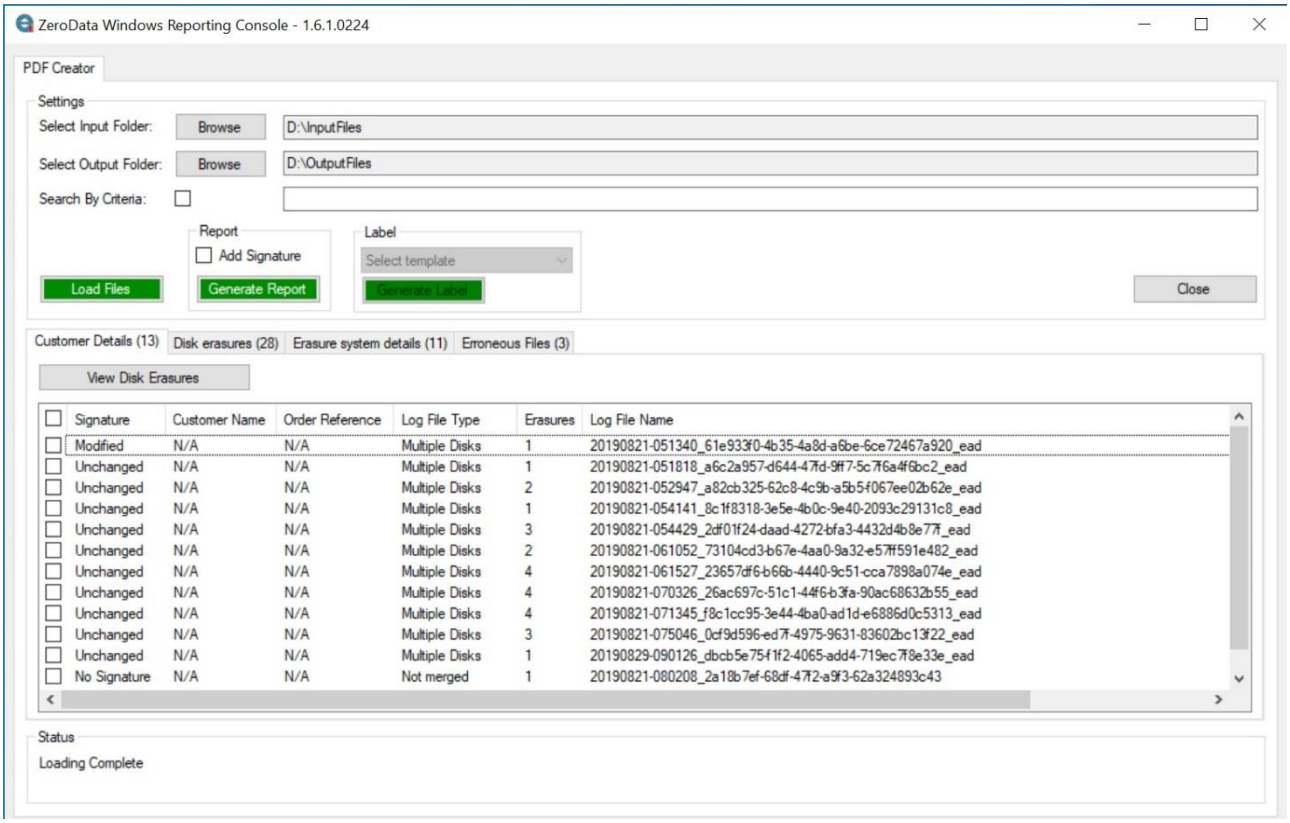
If there are files with errors, then a folder named “ErrorFiles” is created under selected Input folder, and then a subfolder named according to current date and time are created under “ErrorFiles” folder. Then, files with errors are moved to this new subfolder and a file named “ErrorDetails.csv” is created and put in the same subfolder.



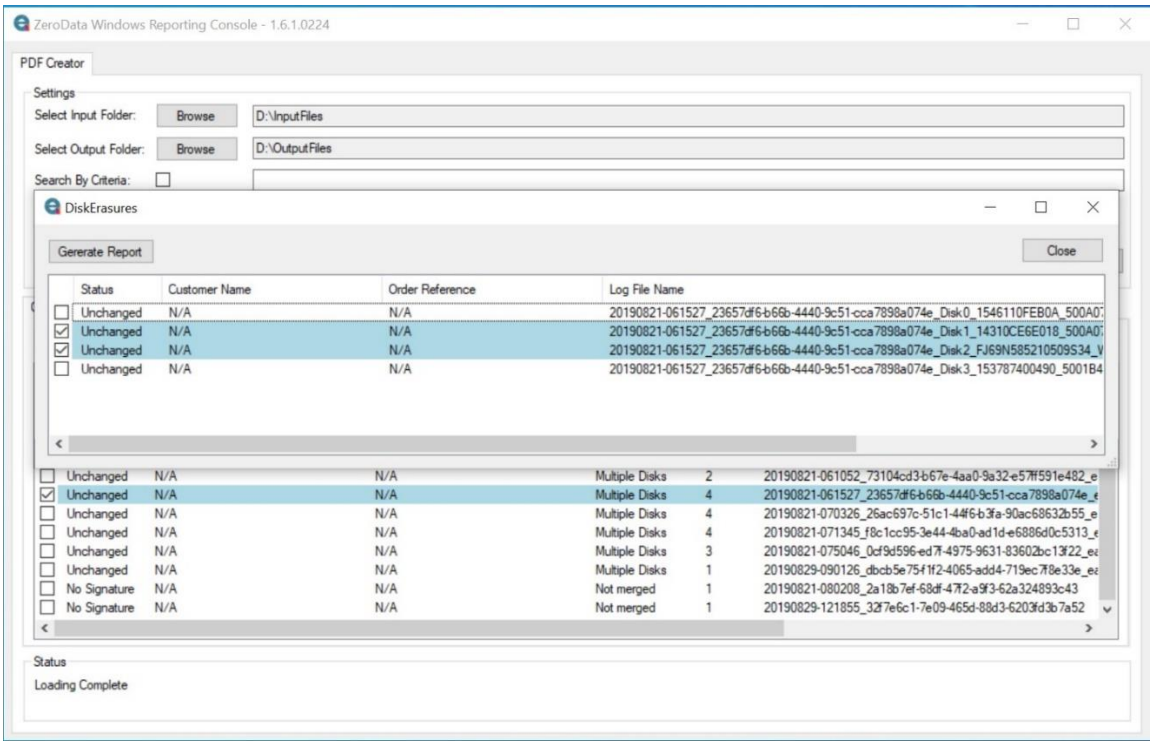
Customer Details tab is shown below. As default, all files are grouped together by Customer Name and Order Reference, then whether it is a single disk or multiple disk log, number of disk erasures recorded in the log file and the full name of log file.

Notice that there is a checkbox above Generate Report button. This option outputs graphics files containing scanned signatures of erasure operator and erasure supervisor to sections reserved for this purpose in PDF reports. For successful usage, the following conditions must be met :

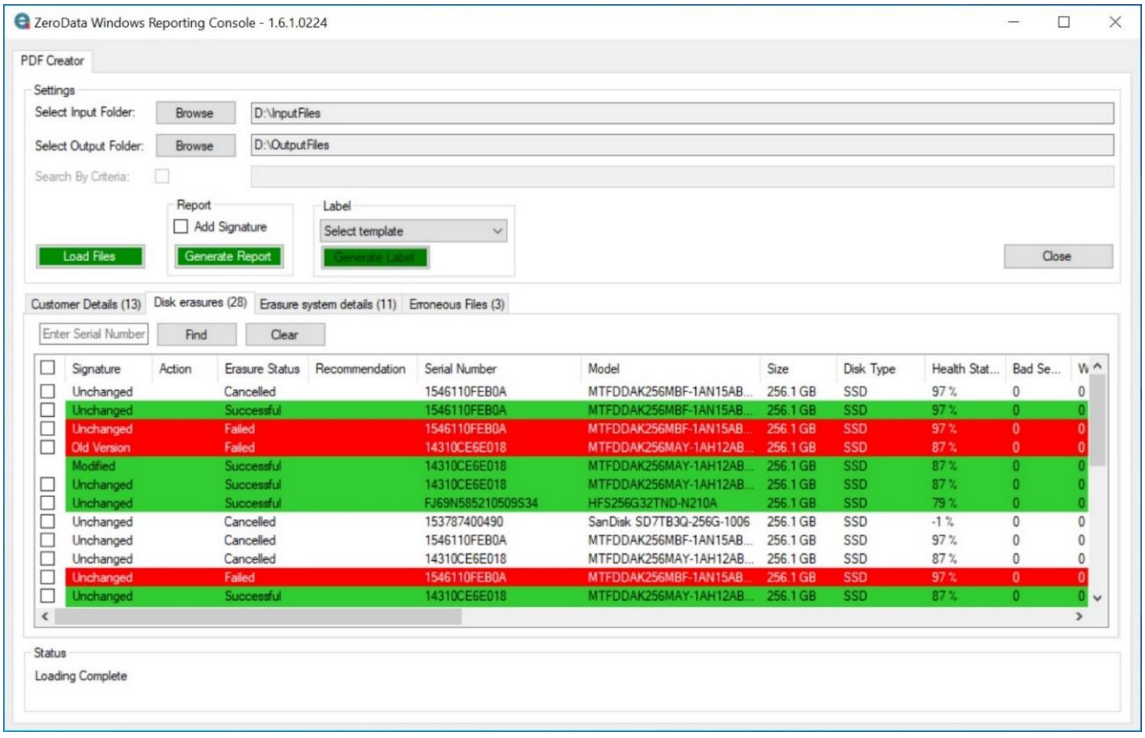
- The folder containing the signature scans must be named Signature and must reside in the same folder as ZeroData Windows executable file,
- Scanned signature files must be in PNG format,
- Background color of the signature must be white as ZeroData Windows PDF reports have white background,
- Operator signature file must be named Operator.png,
- Supervisor signature file must be named Supervisor.png,
- The placeholder reserved for both signature files has a width of 400 pixels and a height of 110 pixels. If signature files have different width and height, then they are scaled to fit within placeholder sizes. Having signature files as close to the placeholder scale as possible will prevent issues like incomplete signature images being added to PDF reports. A good rule of thumb for the signature files would be a width to height ration of 4 to 1, meaning the width value of the signature should be 4 times bigger than the height value. For example, a signature file of 960 pixels width by 240 pixels height (width/ height ration is 4 / 1) will have much less problems with being displayed correctly then a signature file of 480 pixels width by 960 pixels height (width / height ratio is 1 / 2).



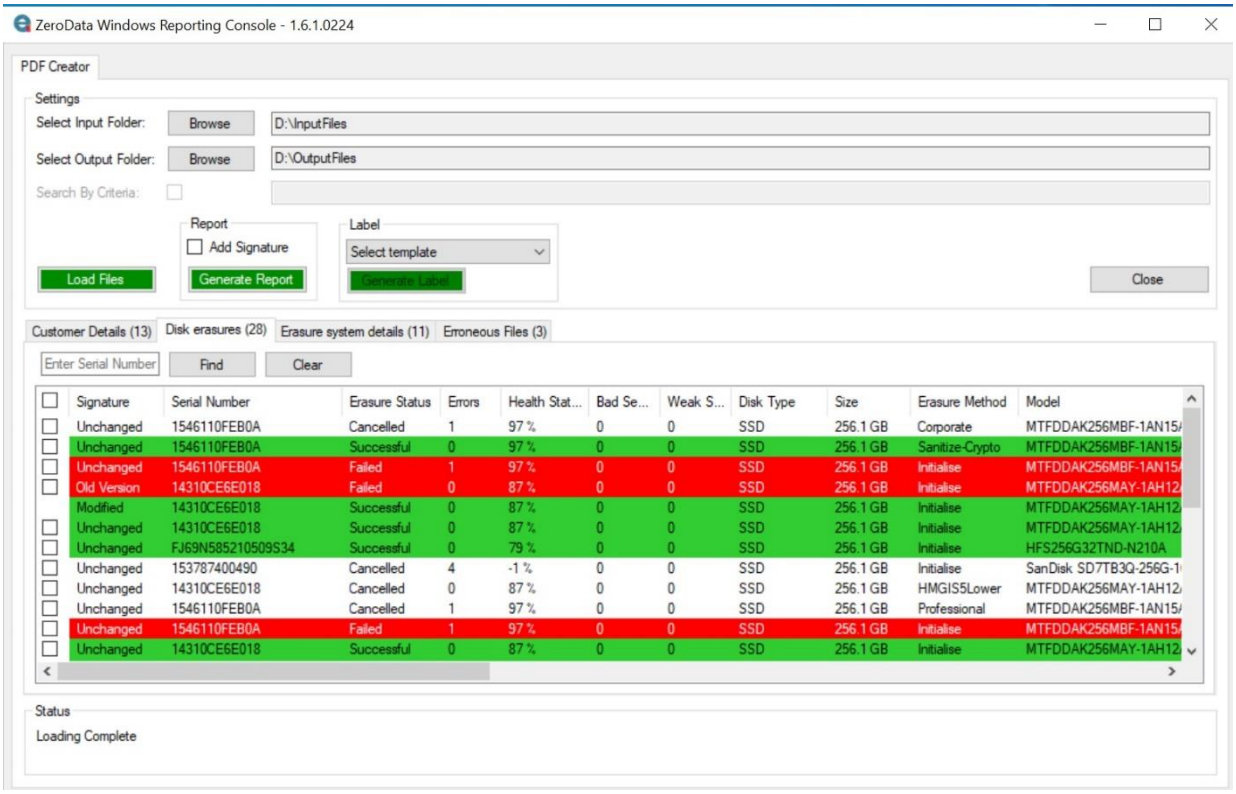
In case a log file with multiple disk erasures is selected, individual Disk Erasures can be seen by selecting the erasure and clicking on “View Disk Erasures” button as shown below. It Is possible to select the log files and generate reports in the “Disk Erasures” window that opens.



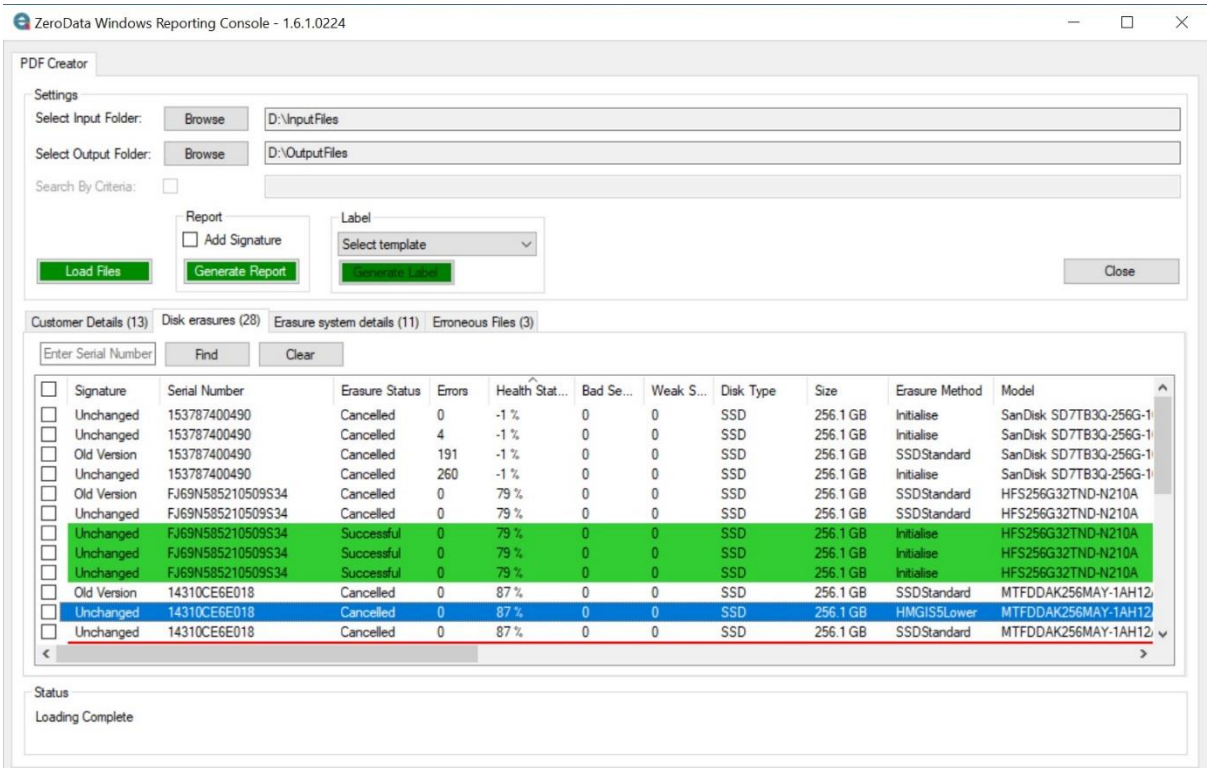
Disk Erasures tab is shown below. The following data are available in columns: Disk Type, Model, Size, Serial Number, Size, Health Status, Erasure Method, Erasure Time, Erasure Duration, Erasure Status, Errors, Manufacturer, Initialised, Bootable, Lifetime Writes, Bad Sectors, Weak Sectors, Communication Failures, Customer Name, Order Reference, Log File Name, and GUID fields. Failed erasures are marked red, successful erasures are marked green and cancelled erasures are unmarked in white.



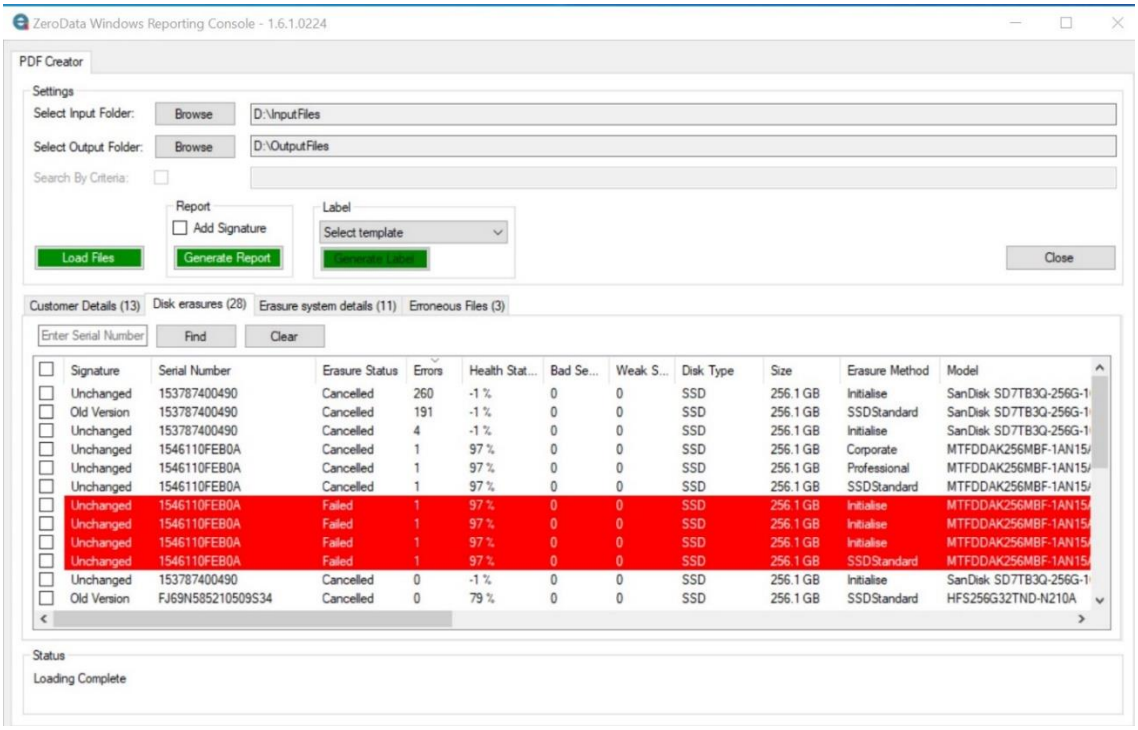
As shown below, it is possible to order these columns according to your display preference simply by dragging and dropping the columns into desired display order.



It is possible to sort the erasure summaries in ascending or descending order simply by double clicking on column headers. Below given screenshot shows erasures displayed in ascending order based on Health Status column.

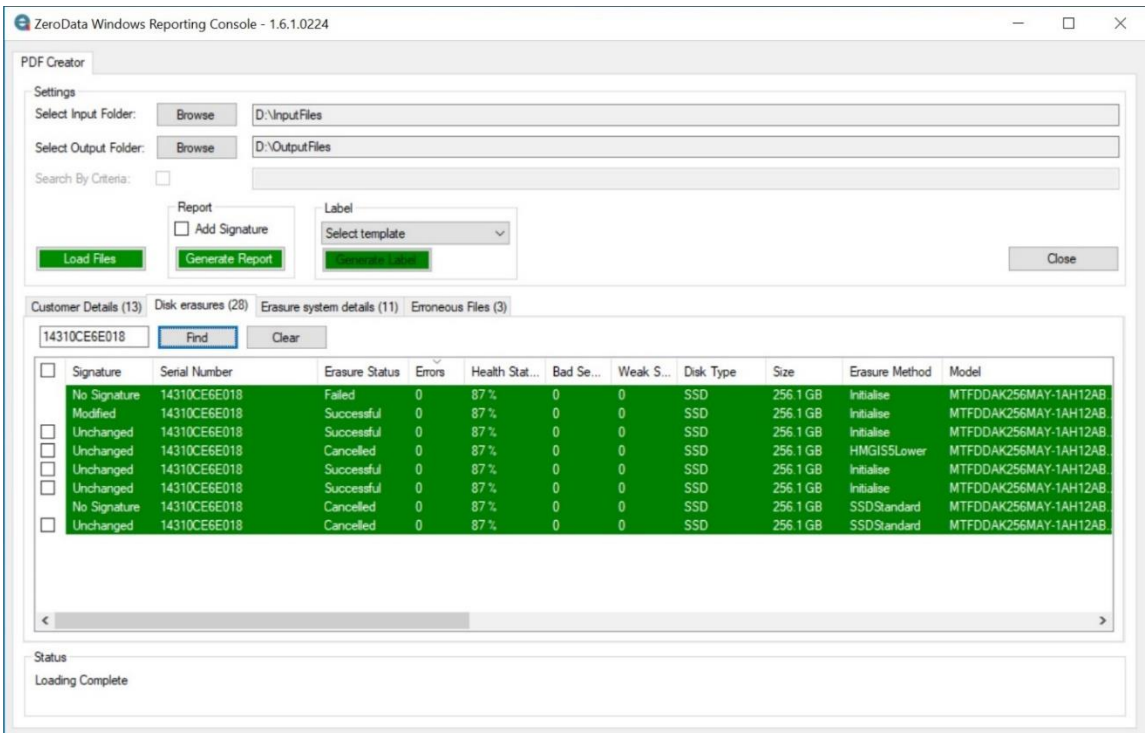


Below given screenshot shows several erasures displayed in descending order based on Errors column.

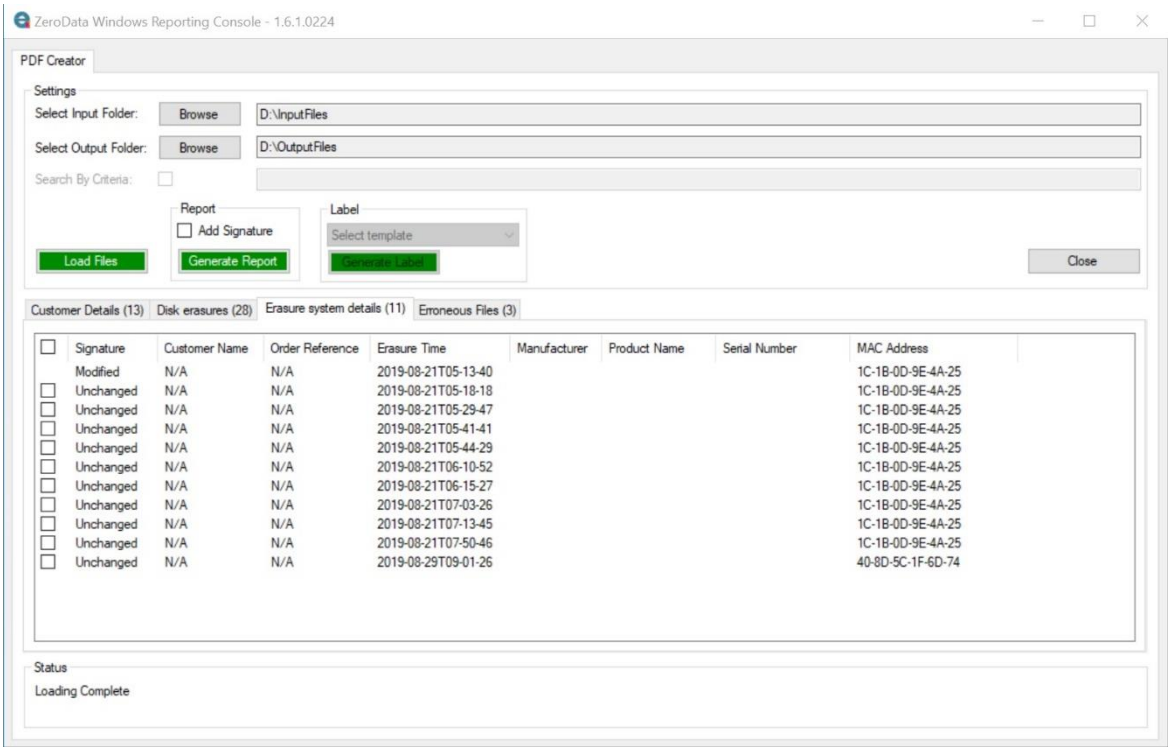


It is possible to search for a disk erasure result using its serial number. The serial number is entered in the “Enter Serial Number” box.

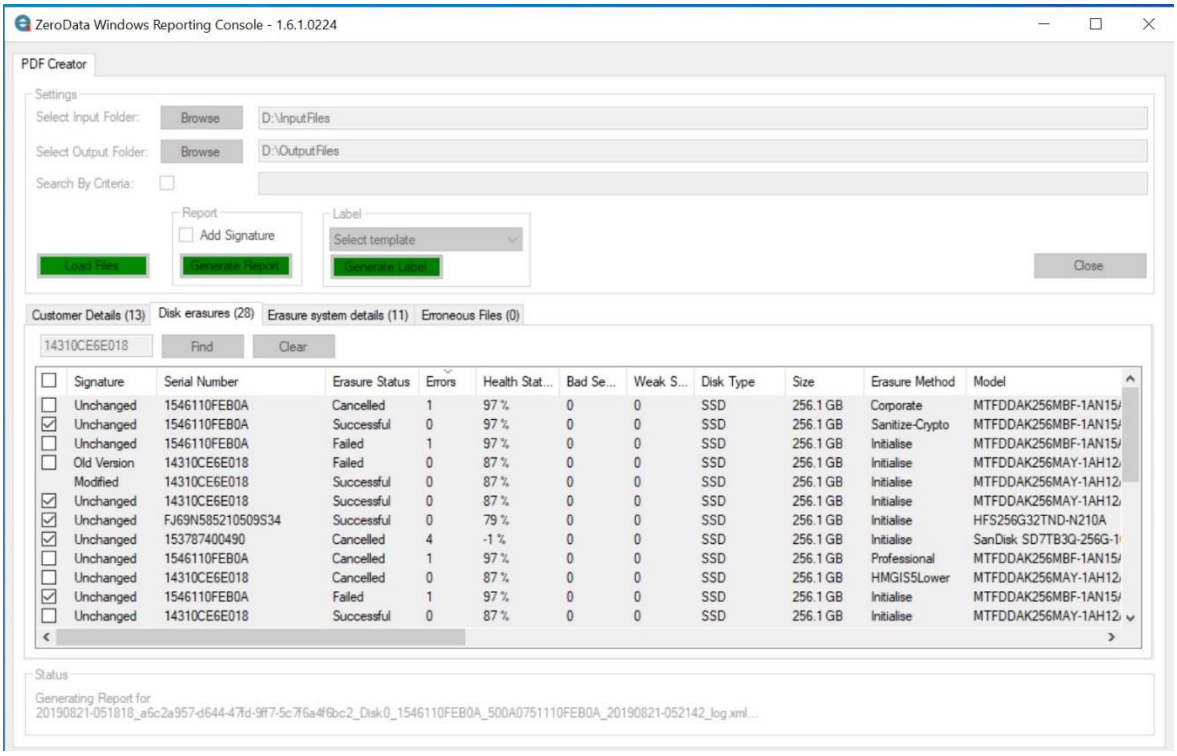
When “Find” button is clicked, the search result is displayed. In the sample screenshot given below, the same disk has been erased multiple times and log files for these multiple runs are present in the Input Folder. Search results can be cleared by clicking on “Clear” button.



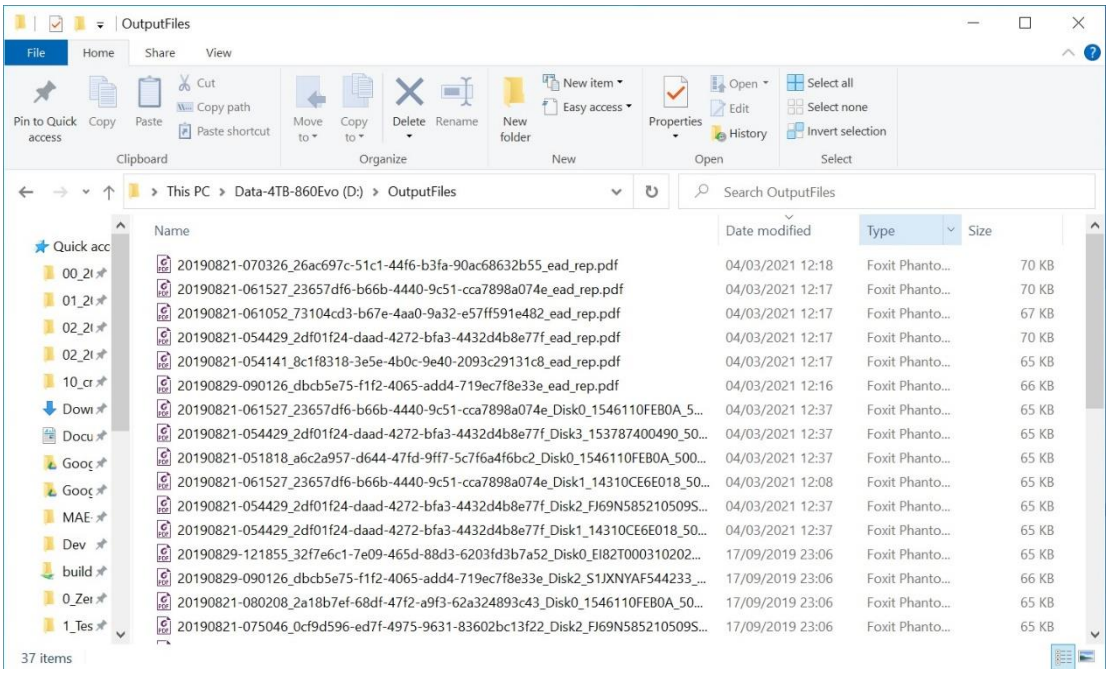
Erasure System Details tab is shown below. As default, all files are grouped together by Customer Name and Order Reference, then by Erasure Time, Manufacturer, Product Name, Serial Number and MAC Address.



No matter which tab is active, one or more files must be selected, and the Generate Report button must be pressed to create reports. In the screenshot below, five files are selected, and Generate Report button is pressed. When more than one file is selected and processed, the file currently being processed is displayed at the status box located in the bottom of application window.



Below screenshot shows multiple PDF report files created at specified Output folder.



PDF report files generated by this application have no difference than the ones generated by ZeroData Windows after disk erasure. The distinction lies when the reports are created: Reporting Console can create reports on past erasures. In these samples, erasure logs from 21/08/2019 were processed in 04/03/2021 and reports were created around 18 months after disk erasures had been carried out.

Sample PDF reports are given in following pages.

The first sample PDF report shows details of a 256 GB Micron 1100 SSD erased using NIST 800-88 Rev.1 Purge erasure method where the SANITIZE Block Erasure firmware command has successfully erased the disk. Starting with ZeroData Windows version 1.6, it is possible to output contents of graphics files into fields reserved for Data Erasure Operator signature and Data Erasure Supervisor signature.

The second sample PDF report shows details of a 120 GB Western Digital SSD that has failed erasure due its health score before erasure being 79% and a higher health score was set for disks to fail before erasing them. The disk has not been erased due this check and therefore the S.M.A.R.T. After Erasure values are empty. Starting with ZeroData Windows version 1.5, log files have a new tag group named <ZDRecommendation> that contains recommendation text for failing disks. In this case, as the SSD was viewed as unfit for re-use due the health score of 79%, the recommendation is to destroy the disk.

The third sample PDF report shows details of a 4.0 TB HGST HDD where erasure was cancelled by the user. An appropriate recommendation message is output to notify the user that the erasure is not completed due the user has cancelled the erasure.

ZeroData Disk Erasure Certificate

Eurosoft (UK) Ltd

Licensee Name: **Development**
Operator Name: **ΓÇ£Johnny AppleseedΓÇ¥** Supervisor Name: **ΓÇ£Jason WhiteΓÇ¥**
Log UUID: **262eb2ba-1f9b-4131-a89b-78ebcfe844e0**
Data Erasure Software Used: **ZeroData ver. 1.6.1.0305 built on: 2021-03-05**

Erasure Operation Details Passed: 1 Failed: 0

Disk: 0 Information

Vendor: **N/A**
Model: **MICRON_1100_MTFDDAK256TBN**
Nominal Size: **256.1 GB**
Disk Type: **SSD**
Serial Number: **17511A7F1226**
WWN: **500A07511A7F1226**
Size: **238.5 GB**
Sector Size: **512**
Sectors: **500118192**
HPA: **Not Present**
DCO: **N/A**
Interface: **S-ATA Gen3, 6 Gbps**
Power On Count: **205**
Power On Hours: **1376**
Total Host Writes: **9310.00 GB**
Reallocated Sectors Before: **0**
Uncorrectable Sectors Before: **0**
Current Pending Sectors Before: **0**
Reallocated Sectors After: **0**
Uncorrectable Sectors After: **0**
Current Pending Sectors After: **0**
Bad Sectors Before Erasure: **0**
Bad Sectors After Erasure: **0**
Health Status: **97 %**
Health Status After Erasure: **97 %**
Storage Controller: **Intel(R) Chipset SATA/PCIe RST Premium Controller (RAID) [VEN: 8086, DEV: 2822] Version: 17.9.1.1009, 6-2-2020**

Erasure Operation

Status: **Successful**
Failed Count: **0**
Erasure Passes: **1**
Verify Passes: **1**
Fingerprint Written:
Started At: **2021-03-09 08-26-14**
Ended At: **2021-03-09 08-26-57**
Total Duration: **00H-00M-43S**
Erasure Method: **NIST800-88Purge**
Method: **SANITIZE Block erasure**
Method Used:
Extra Methods: **N/A**

Erasure System Hardware Details

Manufacturer: **To Be Filled By O.E.M.**
Product Name: **To Be Filled By O.E.M.**
Version: **To Be Filled By O.E.M.**
Serial Number: **To Be Filled By O.E.M.**
UUID: **A3C28570-AEFE-0000-0000-000000000000**
SKU: **To Be Filled By O.E.M.**
BaseBoard: **ASRock, Z390 Pro4, NULL, M80-B8007504808, NULL**
Processor: **CPU0, Central Processor, BFEBFBFF000906EC, Intel(R) Core(TM) i5-9600K CPU @ 3.70GHz, Core: Intel64 Family 6 Model 158 Stepping 12**
BIOS Details: **American Megatrends Inc., Version: P4.30, Date: 08/12/2019**
Installed Memory: **8 GB**
OS Details: **Version: Windows (TM) 10 Preinstallation Environment [6.3], ServicePack : 0.0, 64Bit: True**
UEFI Enabled: **True**

Report Details

Report UUID: **fb29aa9e-5e46-42d5-a638-5275cd312746**
Report Date: **2021-03-09 08-25-12**
Software Used: **ZeroData ver. 1.6.1.0305 built on: 2021-03-05**
Digital Signature: **z8c8NETD7iQEQnCy/0OJpVDvA0dulZguaMFbVTdZOGSp/lAcxzjQpGsGkYtAzdwyVdI17lKkGQTdn+fT2fZ6MTeN8plQbGhsmmuzEz0QbYQckCkzLielU4rmQ1hWb5x8Z9PHjf59QwLj08yi40cVJ9hlCJCVHDiaZ70EnovXNy2lwN3jvOUBP8xk7UWYMoGTHvriuZg7qdwAaM0zwoQnRvjNFSwrwmfetwX4S47GlJbemYeqhjX4zlMHaKu4Pz7d**

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

Data Erasure Operator

Data Erasure Supervisor

1/1

ZeroData Disk Erasure Certificate

Eurosoft (UK) Ltd

Licensee Name: **Development**
Operator Name: **ΓÇ£Johnny AppleseedΓÇ¥** Supervisor Name: **ΓÇ£Jason WhiteΓÇ¥**
Log UUID: **262eb2ba-1f9b-4131-a89b-78ebcfe844e0**
Data Erasure Software Used: **ZeroData ver. 1.6.1.0305 built on: 2021-03-05**

Erasure Operation Details Passed: 0 Failed: 1

Disk: 1 Information

Vendor: **N/A** | Model: **WDC WDS120G2G0A-00JH30** | Nominal Size: **120.0 GB**
Disk Type: **SSD** | Serial Number: **180873800087** | WWN: **5001B448B6BF6186**
Size: **111.8 GB** | Sector Size: **512** | Sectors: **234455040**
HPA: **Not Present** | DCO: **N/A** | Interface: **S-ATA Gen3, 6 Gbps**
Power On Count: | Power On Hours: | Total Host Writes:
Reallocated Sectors Before: **0** | Uncorrectable Sectors Before: **0** | Current Pending Sectors Before: **0**
Reallocated Sectors After: | Uncorrectable Sectors After: | Current Pending Sectors After:
Bad Sectors Before Erasure: **0** | Bad Sectors After Erasure: | Health Status: **79 %**
Health Status After Erasure: | Storage Controller: **Intel(R) Chipset SATA/PCIe RST Premium Controller (RAID) [VEN: 8086, DEV: 2822] Version: 17.9.1.1009, 6-2-2020**

Erasure Operation

Status: **Failed** | Failed Count: **79**
Erasure Passes: **0** | Verify Passes: **0** | Fingerprint Written:
Started At: **2021-03-09 08-26-14** | Ended At: **2021-03-09 08-26-14** | Total Duration: **00H-00M-00S**
Erasure Method: **Check SMART Data** | Method: **Health Status Percentage**
Method Used: | Extra Methods: **N/A**

⊗ Disk health status below threshold. Please destroy disk. Health: 79 %

Erasure System Hardware Details

Manufacturer: **To Be Filled By O.E.M.** | Product Name: **To Be Filled By O.E.M.** | Version: **To Be Filled By O.E.M.**
Serial Number: **To Be Filled By O.E.M.** | UUID: **A3C28570-AEFE-0000-0000-000000000000** | SKU: **To Be Filled By O.E.M.**
BaseBoard: **ASRock, Z390 Pro4, NULL, M80-B8007504808, NULL**
Processor: **CPU0, Central Processor, BFEBFBFF000906EC, Intel(R) Core(TM) i5-9600K CPU @ 3.70GHz, Core: Intel64 Family 6 Model 158 Stepping 12**
BIOS Details: **American Megatrends Inc., Version: P4.30, Date: 08/12/2019**
Installed Memory: **8 GB**
OS Details: **Version: Windows (TM) 10 Preinstallation Environment [6.3], ServicePack : 0.0, 64Bit: True**
UEFI Enabled: **True**

Report Details

Report UUID: **a03770a0-c187-42a5-b326-e54ef9096607**
Report Date: **2021-03-09 08-25-12**
Software Used: **ZeroData ver. 1.6.1.0305 built on: 2021-03-05**
Digital Signature: **wbqpEXMDtaN651in9Ql//cEyIARS5QqzJAHlj7BpGjZDhN01Js4BqEGw5UD7Fd9fjlKcJNiGwld97Baoy+k7mTs64lXL8wPGZaaHdts5 WQsYW/pMeb/rx13SFq1KN6ZCdhcKYhyb4RyndCoHjuWaaw/e+Rs7ay9F/G8x3BcgnPZFViJatTZln2jdlT7keL88GD7WEOYaxOlYFy zEbEH4ukmry3G7Hp1ydojpl9WToClR1YvDlNO9/E24PA0BpHpv**

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

Data Erasure Operator

Data Erasure Supervisor

1/1

ZeroData Disk Erasure Certificate

Eurosoft (UK) Ltd

Licensee Name: **Development**
Operator Name: **ΓÇ£Johnny AppleseedΓÇ¥** Supervisor Name: **ΓÇ£Jason WhiteΓÇ¥**
Log UUID: **262eb2ba-1f9b-4131-a89b-78ebcfe844e0**
Data Erasure Software Used: **ZeroData ver. 1.6.1.0305 built on: 2021-03-05**

Erasure Operation Details Passed: 0 Failed: 1

Disk: 2 Information

Vendor: **Hitachi Global Storage Technologies** Model: **HGST HUS726T4TALA6L1** Nominal Size: **4.0 TB**
Disk Type: **HDD** Serial Number: **V6G51H4S** WWN: **5000CCA097C24B71**
Size: **3.6 TB** Sector Size: **512** Sectors: **7814037168**
HPA: **Not Present** DCO: **N/A** Interface: **S-ATA Gen3, 6 Gbps**
Power On Count: **69** Power On Hours: **2825** Total Host Writes: **0.00 GB**
Reallocated Sectors Before: **0** Uncorrectable Sectors Before: **0** Current Pending Sectors Before: **0**
Reallocated Sectors After: **0** Uncorrectable Sectors After: **0** Current Pending Sectors After: **0**
Bad Sectors Before Erasure: **0** Bad Sectors After Erasure: **0** Health Status: **100 %**
Health Status After Erasure: **100 %** Storage Controller: **Intel(R) Chipset SATA/PCIe RST Premium Controller (RAID) [VEN: 8086, DEV: 2822] Version: 17.9.1.1009, 6-2-2020**

Erasure Operation

Status: **Cancelled by user** Failed Count: **0**
Erasure Passes: **1** Verify Passes: **0** Fingerprint Written:
Started At: **2021-03-09 08-26-14** Ended At: **2021-03-09 08-27-45** Total Duration: **00H-01M-31S**
Erasure Method: **NIST800-88Purge** Method: **TCG Opal**
Method Used: Extra Methods: **N/A**

⊗ The operator cancelled the erasure task. Cannot successfully erase all data from the disk. Depending on the reason to cancel the erasure, you might try to erase again or consult your organizational guidelines for handling disks.

Erasure System Hardware Details

Manufacturer: **To Be Filled By O.E.M.** Product Name: **To Be Filled By O.E.M.** Version: **To Be Filled By O.E.M.**
Serial Number: **To Be Filled By O.E.M.** UUID: **A3C28570-AEFE-0000-0000-000000000000** SKU: **To Be Filled By O.E.M.**
BaseBoard: **ASRock, Z390 Pro4, NULL, M80-B8007504808, NULL**
Processor: **CPU0, Central Processor, BFEBFBFF000906EC, Intel(R) Core(TM) i5-9600K CPU @ 3.70GHz, Core: Intel64 Family 6 Model 158 Stepping 12**
BIOS Details: **American Megatrends Inc., Version: P4.30, Date: 08/12/2019**
Installed Memory: **8 GB**
OS Details: **Version: Windows (TM) 10 Preinstallation Environment [6.3], ServicePack : 0.0, 64Bit: True**
UEFI Enabled: **True**

Report Details

Report UUID: **c065ef65-3415-4047-bd85-b1c8a1c68476**
Report Date: **2021-03-09 08-25-12**
Software Used: **ZeroData ver. 1.6.1.0305 built on: 2021-03-05**
Digital Signature: **R25CUdeGCgqXbaXiSW43KF52gYhWFhQWOpbxzry1ySO9W0n2EztbckwfMkEYejaID6B/TQk1vfbojJGRI/c3cg7n28dvUJKxW9KE97bcWbx+fii20r0XhaPdK2ucT79PgcyiyMkvwmlusFSZ0srJs2GThQyohDW712ppp1yTjciWi6YV7L8W8PczViR4+l2MO4I7Dm0cTkIlEKQ7Z4bUAQ0YY9mJl/m6LMp6XhNz/aTwR3juPFWPBrLhEa34U1v7**

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

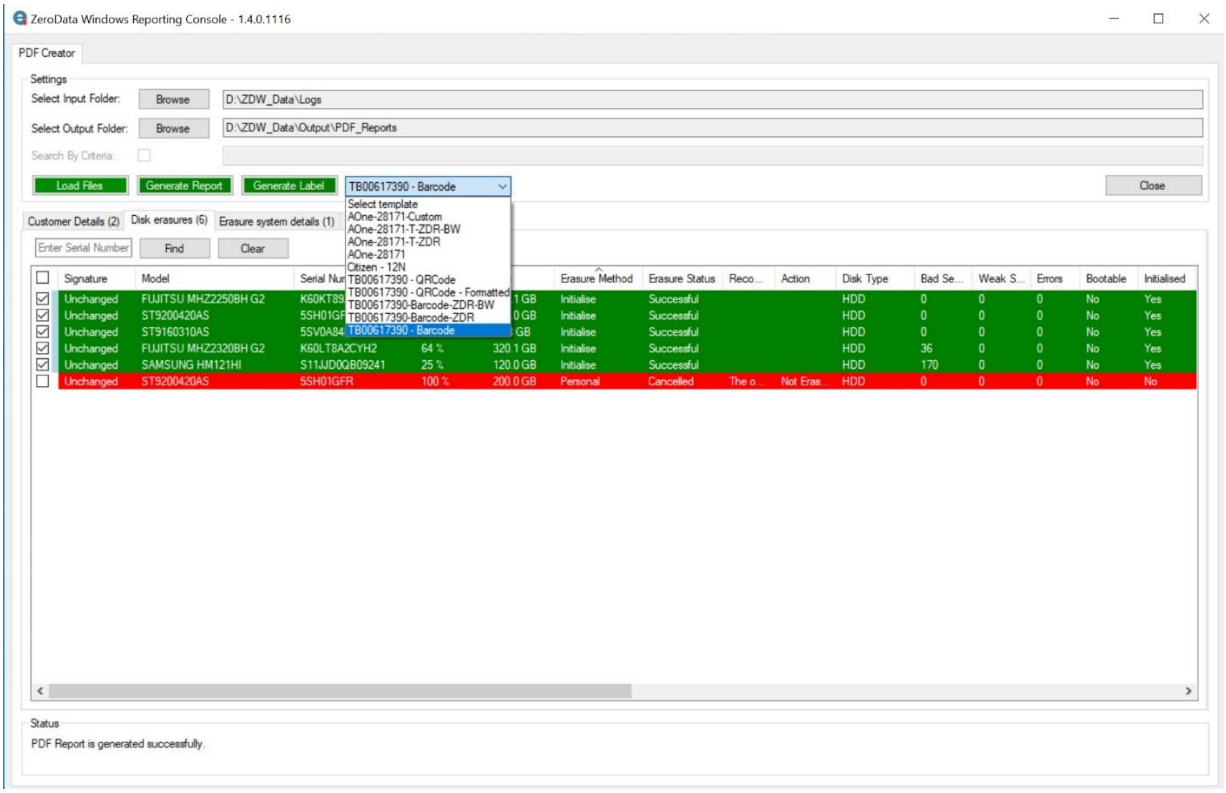
Data Erasure Operator

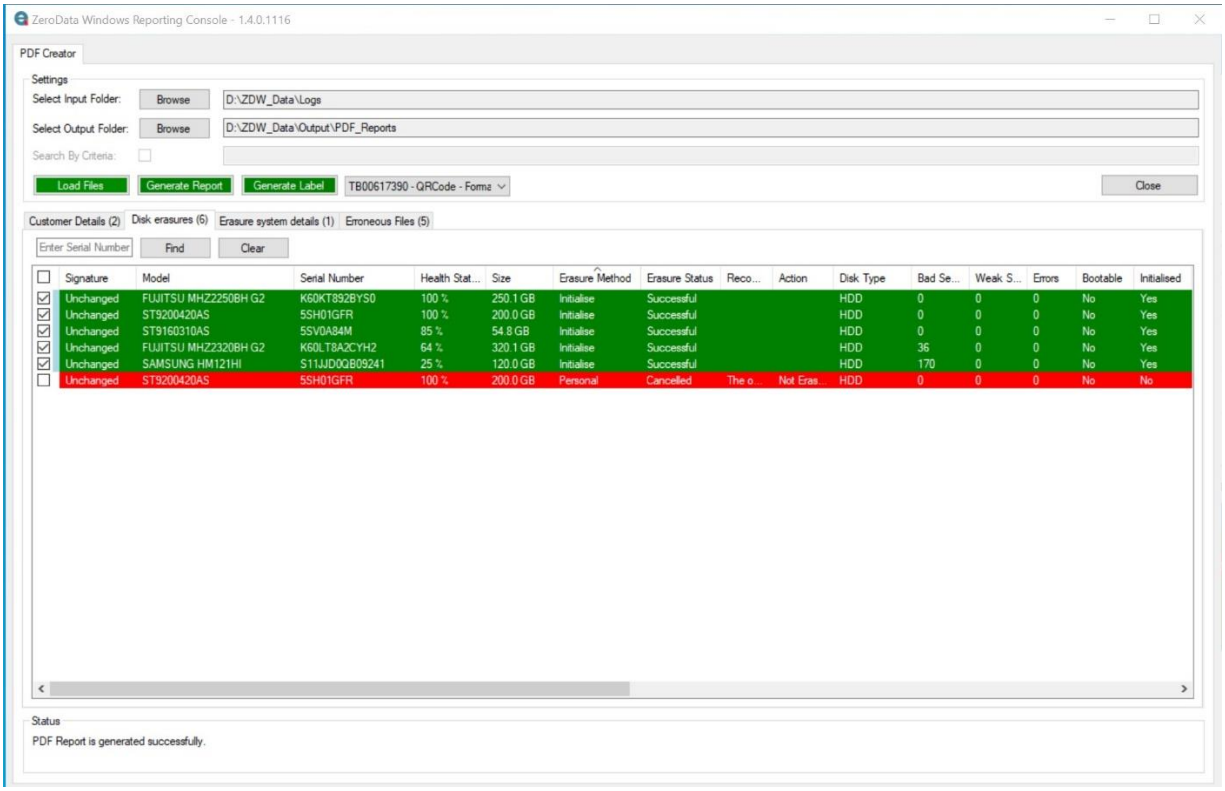
Data Erasure Supervisor

1/1

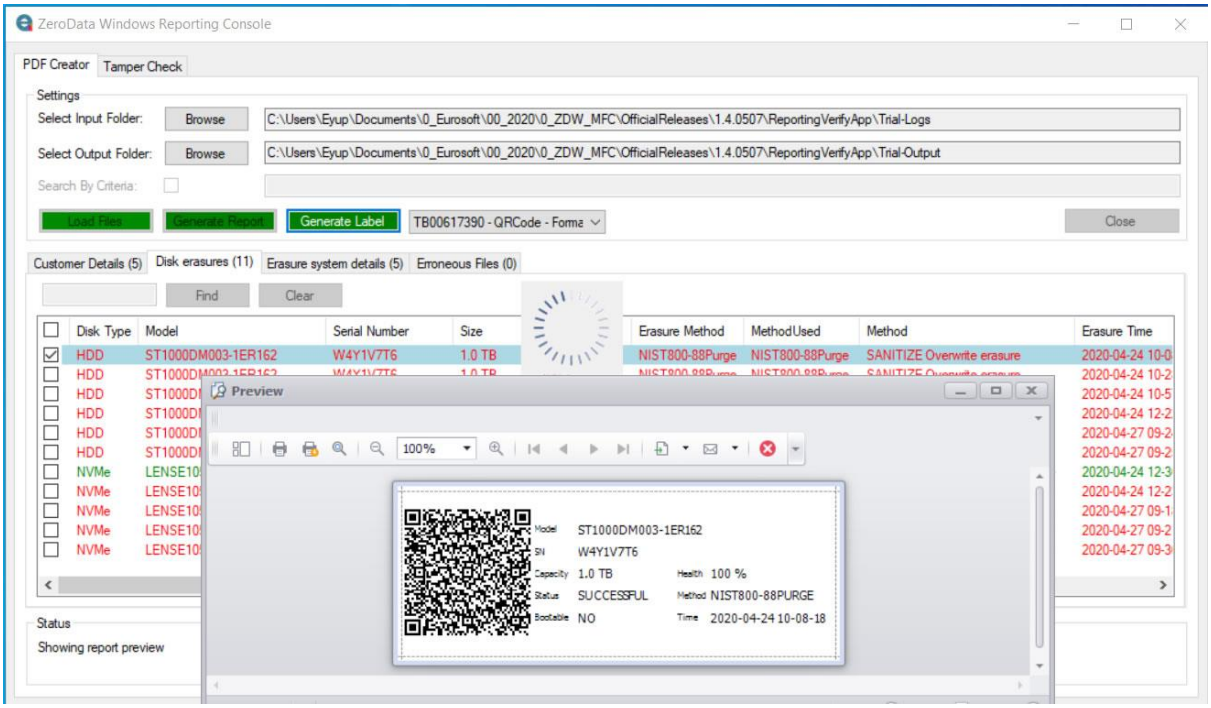
Creating PDF Labels in Reporting Console

ZeroData Windows Reporting Console has ability to output labels containing selected disk information with 1D and 2D barcodes (also known as QR codes). As another feature, ZeroData Windows Reporting Console is the first application to print 12N QR labels. To print a label, first a disk erasure is selected, and then a template is selected.

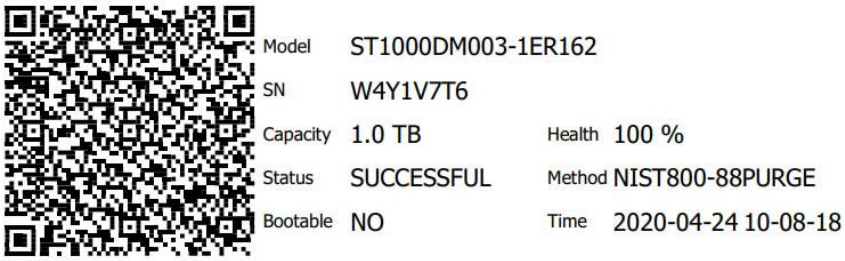




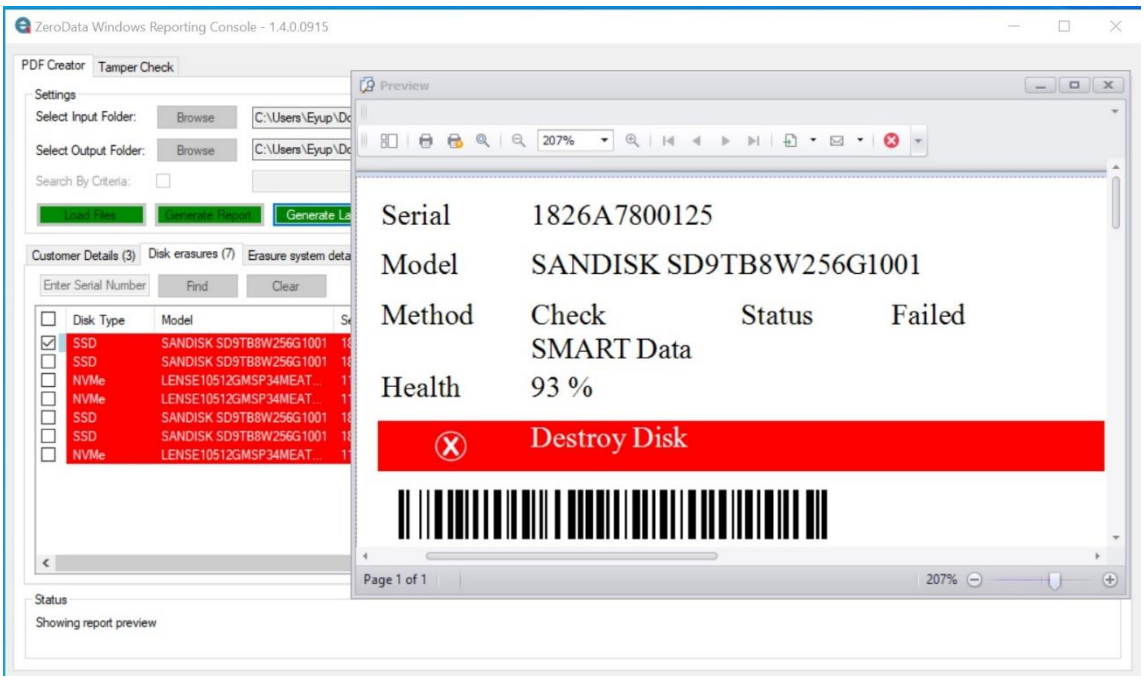
After these selections, “Generate Label” button becomes active. Clicking on “Generate Label” button opens the Printer Selection Window. It is possible to preview the label before printing by clicking on “Preview Label” button.

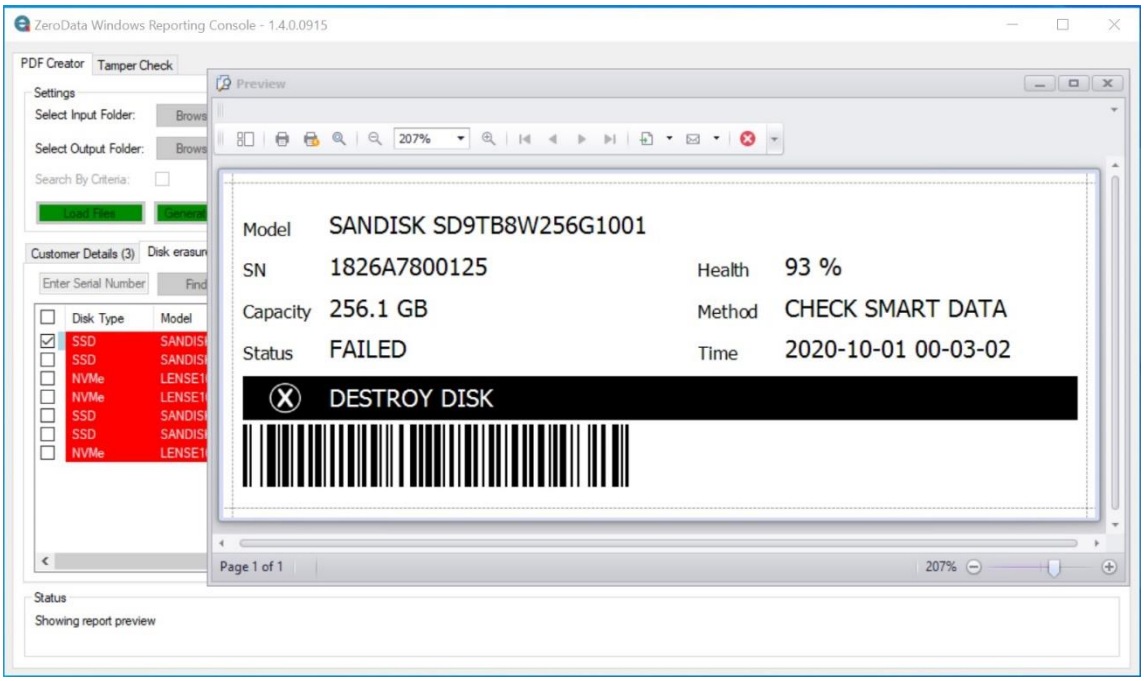


A sample label with a 2D (QR) barcode is shown below.

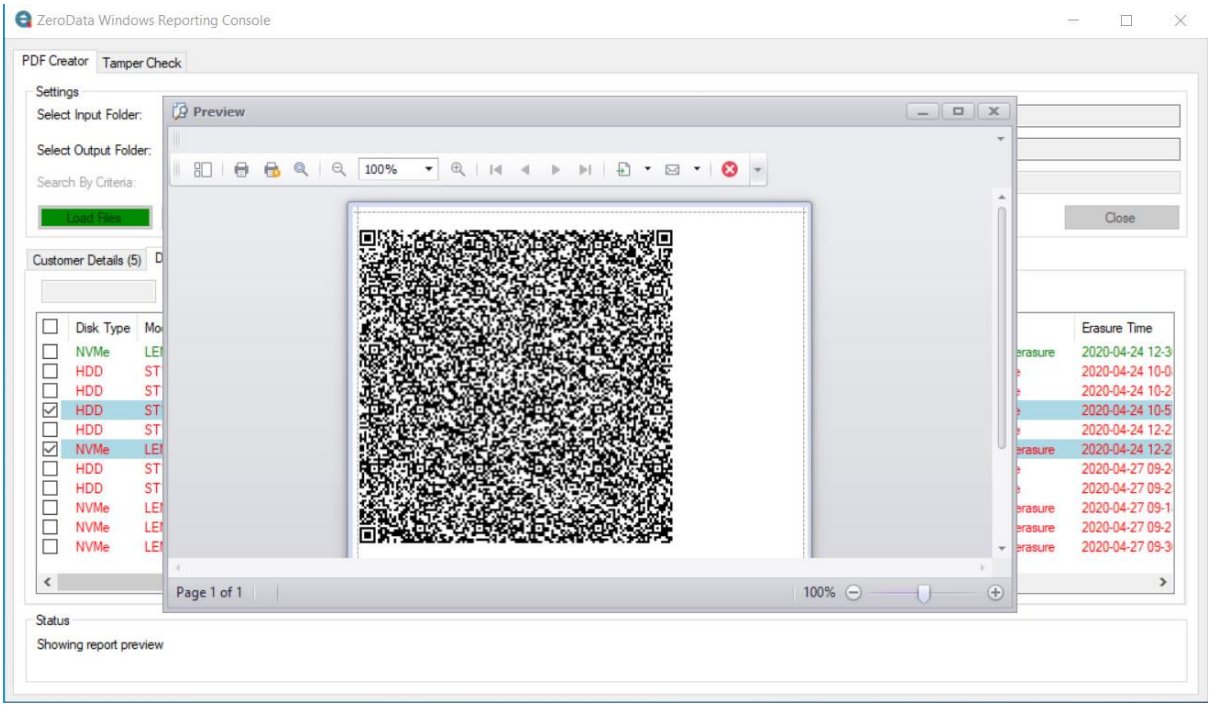


Starting with ZeroData Windows 1.5, it is possible to fail disks based on health scores. New disk label types containing short recommendation text in color and black-and-white have been added.



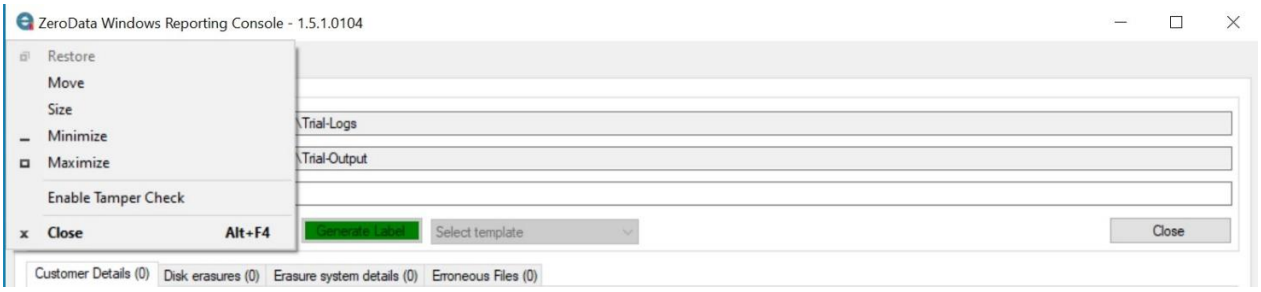


A sample 12N QR label is shown in below screenshot.

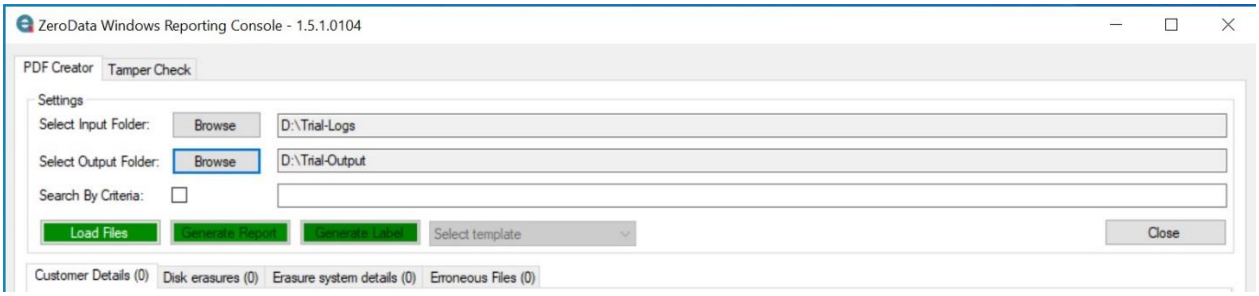


Verifying Authenticity of XML logs in Reporting Console

ZeroData Windows Reporting Console has a second tab, used to verify the XML and PDF test result files are authentic and not tampered with. This second tab is hidden by default and must be enabled by left clicking on the application logo on top left and selecting “Enable Tamper Check” option from the application menu that will open.



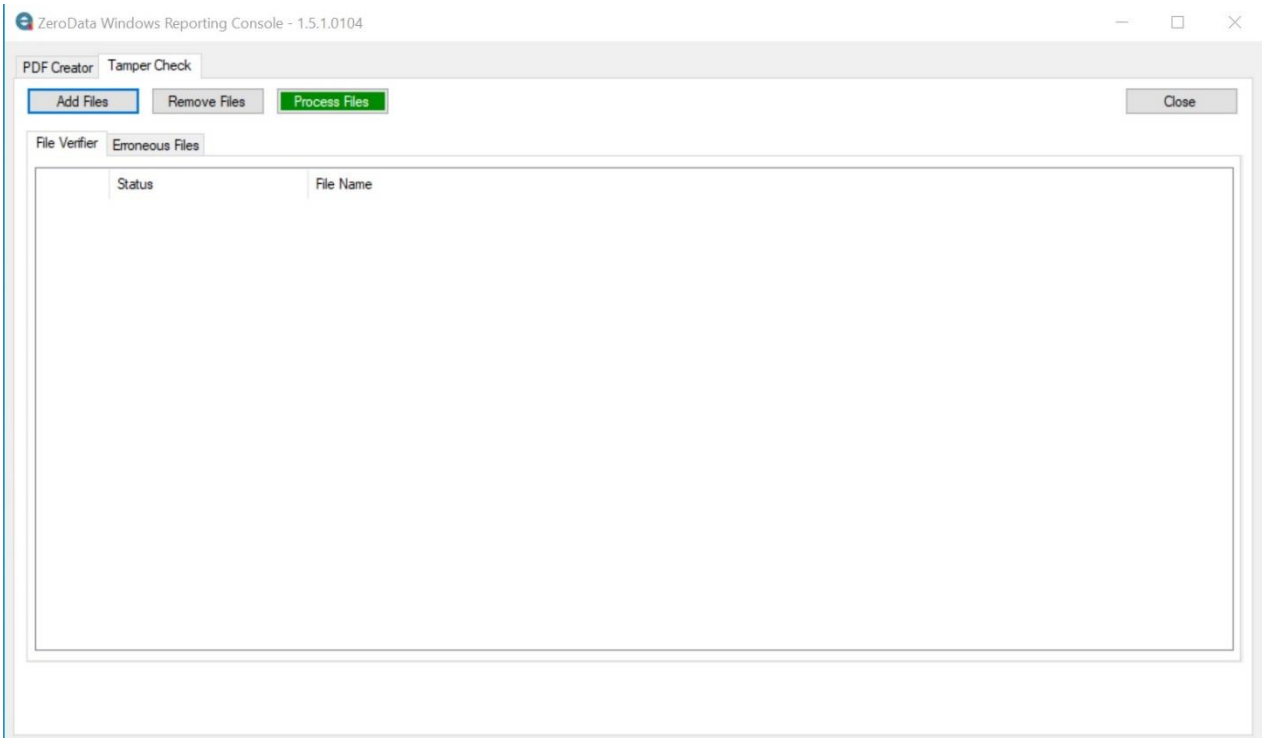
The Tamper Check tab will become visible to the right of PDF Creator tab.

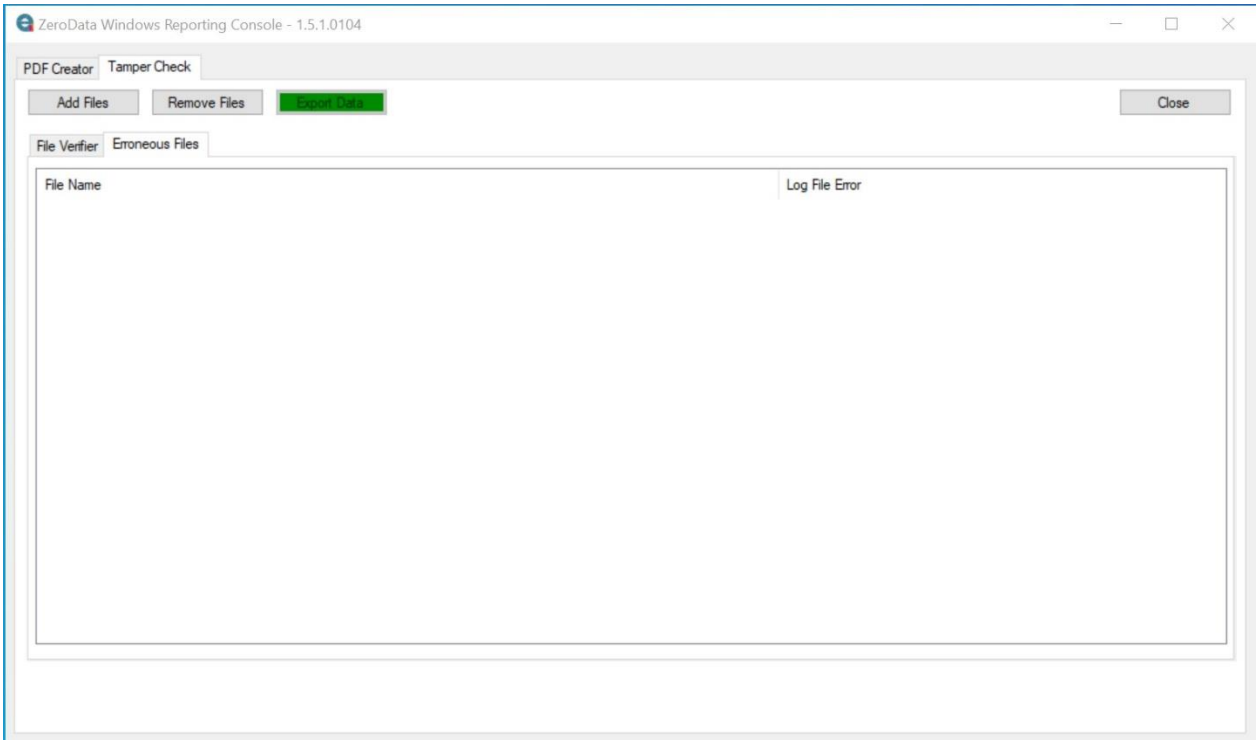


When needed or desired, the Tamper Check tab can be hidden using the same steps described above.

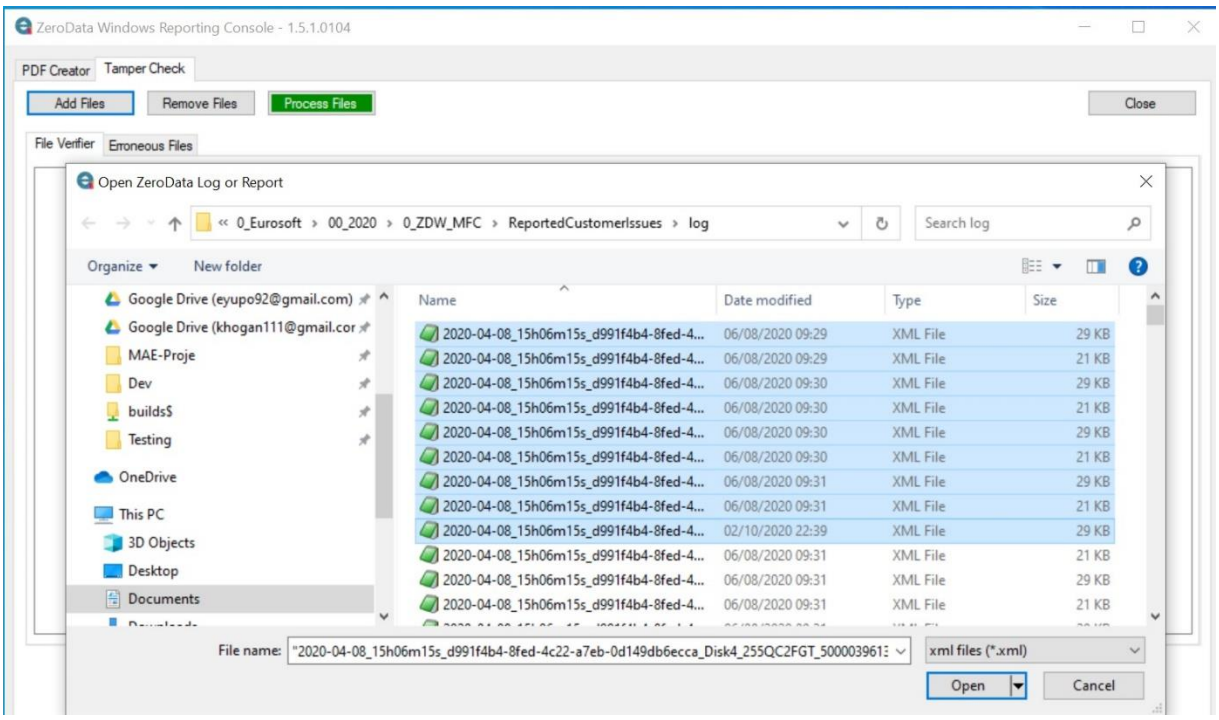
ZeroData Windows uses standard digital signature storage practices for XML files. The PDF standard has an inbuilt digital signature mechanism, but that mechanism is helpful to verify the source of the document, not to verify authenticity of its content. Therefore, ZeroData Windows stores a digital signature string on a PDF file property field, outside of the PDF file content.

To verify authenticity of files, the user must click on Tamper Check tab. The pane will be displayed with the focus set to File Verifier tab, with a second Erroneous Files tab also being available to display any files which were not being able to be processed due file errors.

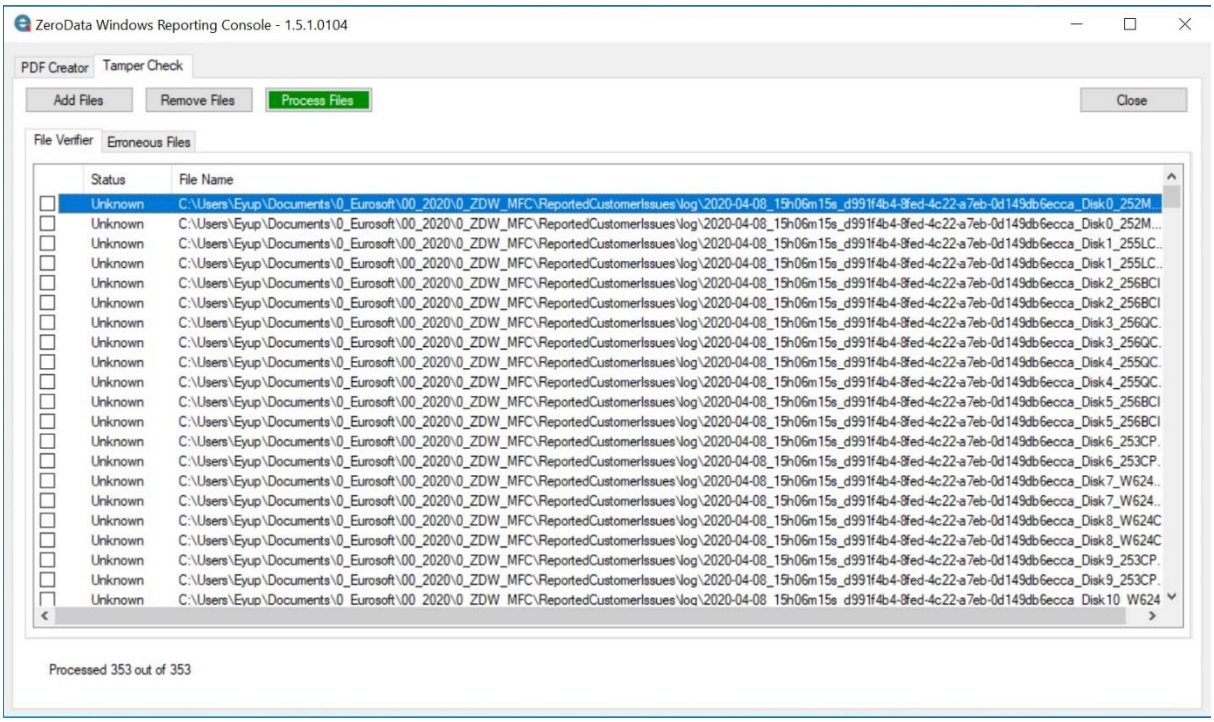




The first step is adding files to check by clicking on Add Files button and selecting files from the File Browser box.



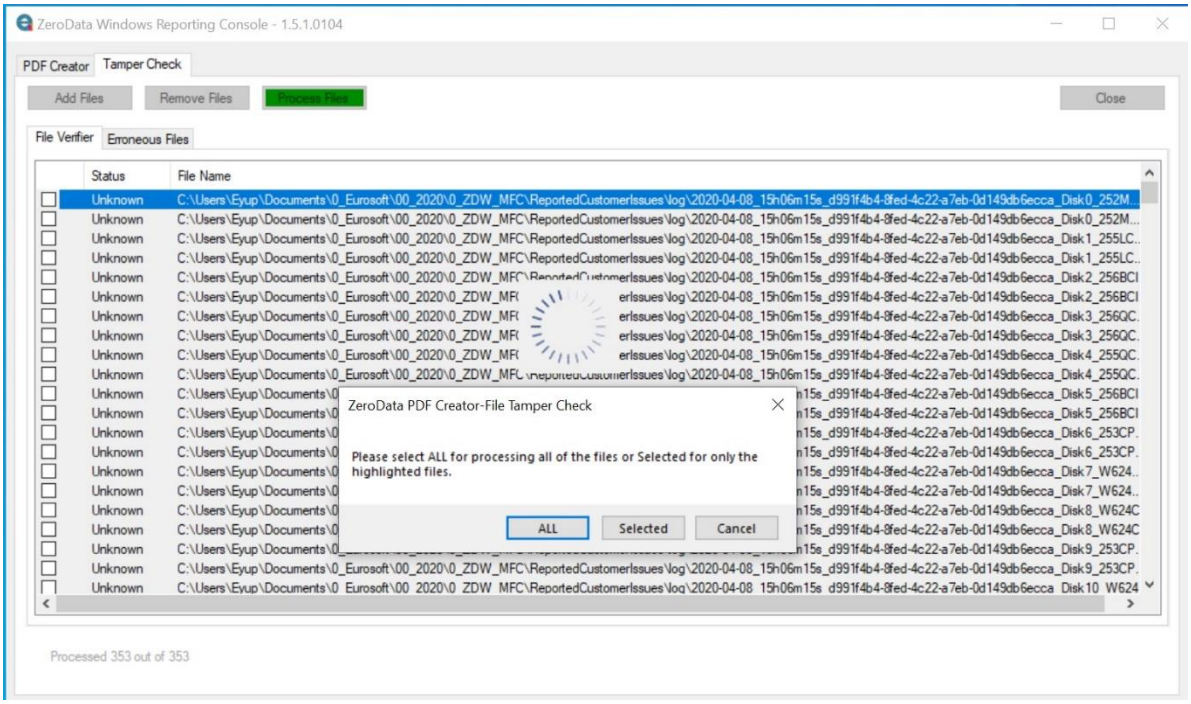
Clicking on “Open” button loads the files for processing.



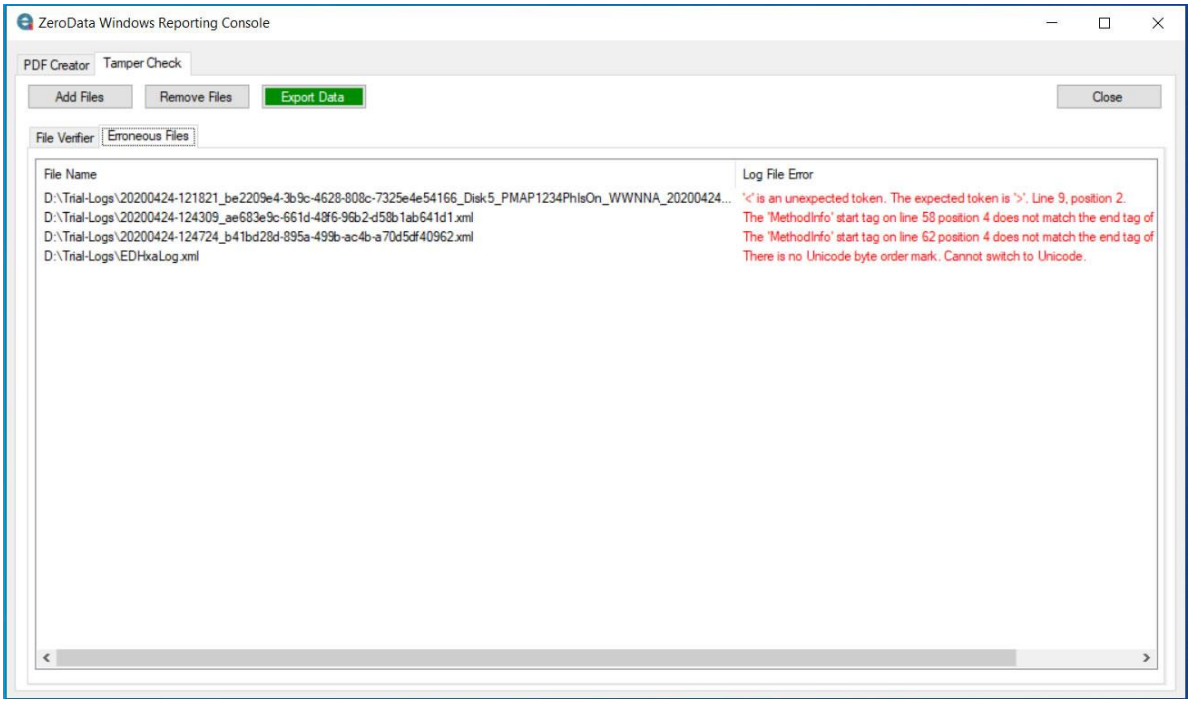
To process loaded files, the user needs to

- either select several files and click on Process Files button and confirm his selection by clicking on “Selected” button,
- or directly click on Process Files button and click on “All” button to process all loaded files,

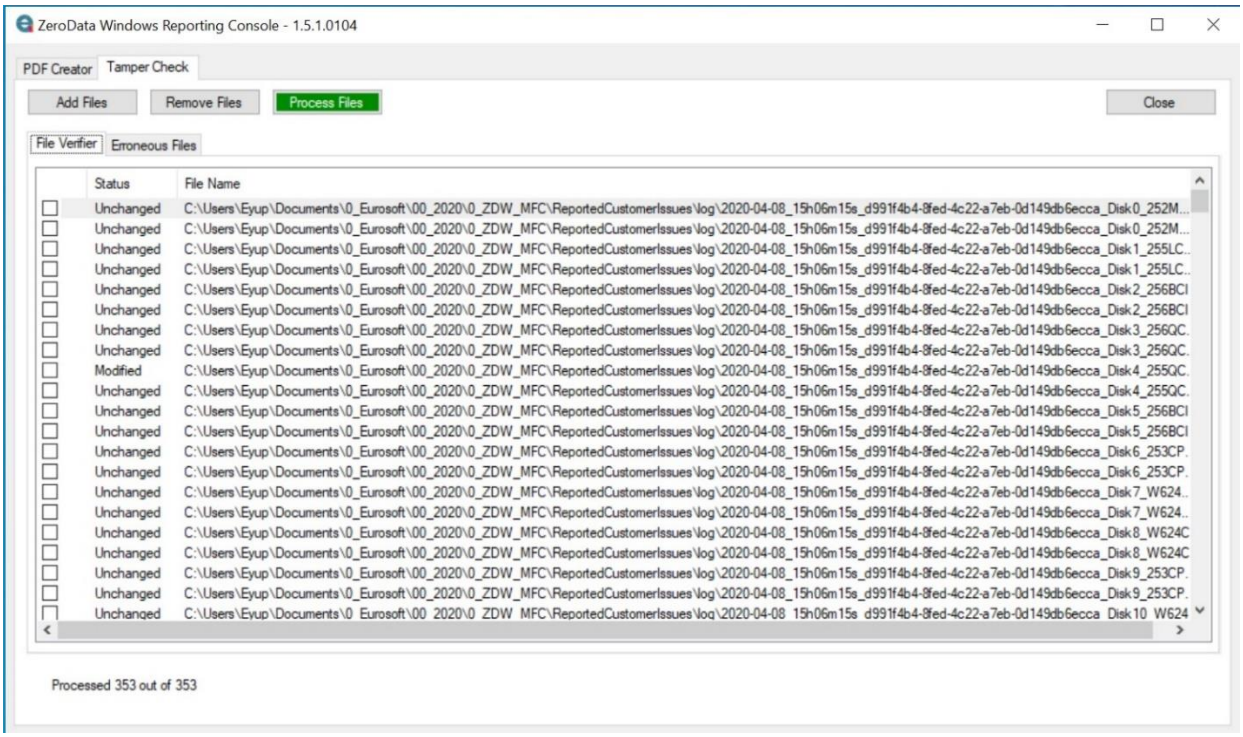
as shown in below screenshot.



After processing ends, the first step should be checking whether there are any invalid XML files that could not be processed from Erroneous Files tab.



File Viewer tab will show the status of processed files, whether they have been modified or tampered after they were created by ZeroData Windows or not. Status of modified files are denoted as “Modified”, and status of unmodified files are denoted as “Unchanged” in green letters.



This functionality allows users to verify the authenticity of file contents they receive through electronic data transmissions.

ZeroData Windows Data Erasure Standards

NIST 800-88 Rev. 1 Methods

These methods implement NIST Special Publication 800-88 Revision 1, Appendix A, Tables A.5 and A.8; optional steps described in standard are discussed in page describing NIEREM parameter.

Due to the complexity of explaining exact steps for each device type, brief details of methods are given below:

Name	Pass	Algorithm
NIST800-88Clear	1	If disk is ATA SSD and Secure Erase or Enhanced Secure Erase is available, apply preliminary verification steps, apply the firmware command, and then verify the erasure. If not ATA SSD or the firmware erasure fails, apply regular overwrite pass(es) specified for device type, like zeroes or “pattern and its complement” passes.
NIST800-88Purge	1	Determine the disk type. Also determine if the firmware-based erasure method(s) specified for the device type are available or not. If available, apply preliminary verification steps, apply firmware commands in sequence until one of them reports a successful completion and then verify the erasure. The sequence for applying firmware command is: 1) TCG Erasure 2) Format NVM in case of NVMe disk 3) SANITIZE Erasure methods that are applicable a. SANITIZE Crypto Erase b. SANITIZE Block Erase c. SANITIZE Overwrite
	2	If none of the above are available: fall back to NIST Clear method specified for device type, like zeroes or “pattern and its complement” passes.

Note that the specification states only two SANITIZE methods to be applied. For SSD’s these are Crypto Scramble and Block Erase, though there are some old disks that support Overwrite they are rare and not addressed in the standard. For HDD’s these are Crypto Scramble and Overwrite as Block Erase is not possible on magnetic platters.

Method specification has one short (default) erasure method and one optional (long) erasure method laid out.

- To execute the short (default) method, specifying erasure method as NIST800-88Purge or NIST800-88Clear on command line or user interface is enough.

- To execute the optional (longer) method, an additional parameter must be given as described in below page describing NIEREM parameter.
    - For command line /NIEREM 0 must be added to the command line making it look like this ***Zerodatawindows.exe /me nist800-88Purge /nierem 0 [other parameters]***

ISO/IEC 27040:2015 Methods

These methods implement methods specified by the document European Standard, Information technology – Security techniques – Storage security (ISO/IEC 27040:2015), Annex A (normative) Media sanitization. Optional steps described in standard are discussed in page describing NIEREM parameter.

Due to the complexity of explaining exact steps for each device type, brief details of methods are given below:

Name	Pass	Algorithm
ISO27040Clear	1	If disk is ATA SSD and Secure Erase or Enhanced Secure Erase is available, apply preliminary verification steps, apply the firmware command, and then verify the erasure. If not ATA SSD or the firmware erasure fails, apply regular overwrite pass(es) specified for device type, like zeroes or “pattern and its complement” passes.
ISO27040Purge	1	Determine the disk type. Also determine if the firmware-based erasure method(s) specified for the device type are available or not. If available, apply preliminary verification steps, apply firmware commands in sequence until one of them reports a successful completion and then verify the erasure. The sequence for applying firmware command is: 1) TCG Erasure 2) Format NVM in case of NVMe disk 3) SANITIZE Erasure methods that are applicable a. SANITIZE Crypto Erase b. SANITIZE Block Erase c. SANITIZE Overwrite
	2	If none of the above are available: fall back to ISO27040 Clear method specified for device type, like zeroes or “pattern and its complement” passes.

Note that the specification states only two SANITIZE methods to be applied. For SSD’s these are Crypto Scramble and Block Erase, though there are some old disks that support Overwrite they are rare and not addressed in the standard. For HDD’s these are Crypto Scramble and Overwrite as Block Erase is not possible on magnetic platters.

Method specification has one short (default) erasure method and one optional (long) erasure method laid out.

- To execute the short (default) method, specifying erasure method as ISO27040Purge or ISO27040Clear on command line or user interface is enough.

- To execute the optional (longer) method, an additional parameter must be given as described in below page describing NIEREM parameter.
    - For command line /NIEREM 0 must be added to the command line making it look like this ***Zerodatawindows.exe /me iso27040 /nierem 0 [other parameters]***

NIEREM parameter use in NIST 800-88 Rev 1 and ISO/IEC 27040 methods

NIST 800-88 Revision 1 standard (nist800-88purge and nist800-88clear erasure methods in ZeroData Windows) and ISO/IEC 27040 standard (iso27040purge and iso27040clear erasure methods in ZeroData Windows) define a data destruction procedure in a clearly stated sequence. On top of these "standard" sequences, there are "optional" sequences of steps that can be applied as well. Based on customer feedback, this functionality has been extended to allow extra sequence of steps with this parameter.

Command line execution of this option is as follows:

zerodatawindows.exe /me nist800-88purge /nierem { 0 | 1 } ...

zerodatawindows.exe /me iso27040purge /nierem { 0 | 1 } ...

where:

/nierem 0 executes the "optional sequence of steps defined in NIST 800-88 Revision 1 and ISO/IEC 27040 standards.

/nierem 1 adds a new sequence of steps NIST 800-88 Revision 1 and ISO/IEC 27040 standards. First the "default" sequence of steps described in standard are applied:

- if the last executed step of data erasure is a **successfully executed and verified firmware command**, then an extra write zeroes pass is applied to the disk and a verification pass is applied.

- If the last executed step of data erasure executed is a **successfully executed and verified regular overwrite pass**, then no extra write zeroes pass is applied to the disk.

NISTISO-Clear and NISTISO-Purge Methods

These methods have the same functionality as NIST 800-88 Rev.1 and ISO 27040 Clear and Purge methods, except they do not implement the fallback portion of specifications and require the erasure operator to specify which erasure method to use as fallback when primary erasure options cannot be executed successfully.

Due to the complexity of explaining exact steps for each device type, brief details of methods are given below:

Name	Pass	Algorithm
NistISO-Clear	1	If disk is ATA SSD and Secure Erase or Enhanced Secure Erase is available, apply preliminary verification steps, apply the firmware command, and then verify the erasure. If not ATA SSD or the firmware erasure fails, apply fallback erasure method specified by erasure operator. This custom fallback method can be any of the other methods like US DoD, HMG IS5 Higher, SSDRandom6 etc. Important: As ATA Secure Erase and Enhanced Secure Erase are only applicable under WinPE and after disks are power cycled, practically this method will only be useful when there are SATA SSD's connected to the system using hot-swap drive cages and they are taken out and reconnected to the system after WinPE boots and before ZeroData Windows is started.
NistISO-Purge	1	Determine the disk type. Also determine if the firmware-based erasure method(s) specified for the device type are available or not. If available, apply preliminary verification steps, apply firmware commands in sequence until one of them reports a successful completion and then verify the erasure. The sequence for applying firmware command is: 1) TCG Erasure 2) Format NVM in case of NVMe disk 3) SANITIZE Erasure methods that are applicable a. SANITIZE Crypto Erase b. SANITIZE Block Erase c. SANITIZE Overwrite
	2	If none of the above are available: apply fallback erasure method specified by erasure operator. This custom fallback method can be any of the other methods like US DoD, HMG IS5 Higher, SSDRandom6 etc.

Note that the specification states only two SANITIZE methods to be applied. For SSD's these are Crypto Scramble and Block Erase, though there are some old disks that support Overwrite they are rare and not addressed in the standard. For HDD's these are Crypto Scramble and Overwrite as Block Erase is not possible on magnetic platters.

Unlike all other erasure methods that accept only one method name as parameter, both methods require two method names as parameter:

- /me { nistiso-clear | nistiso-purge } { fallback erasure method }

The first method name must either be nistiso-clear or nistiso-purge, the second method name can be any other method name.

If first method name is not nistiso-clear or nistiso-purge, then a second parameter is treated as an error.

- For user interface operation, if erasure method is selected either as NistISO-Clear of NistISO-Purge Options; then a new dropdown box is displayed to erasure operator to select the fallback erasure method.

- Sample command line usages:

    - ***/me nistiso-clear usdod***

      Attempt to erase disks using NistISO-Clear method; if that option fails, then attempt US DoD method to erase the disk.

    - ***/me nistiso-purge SSDRandom6***

      Attempt to erase disks using NistISO-Purge method; if that option fails, then attempt SSDRandom6 method to erase the disk.

German SI-2011-VS BSI-GS and BSI-GSE Data Erasure Methods

These methods are based on documents published by German SI-2011-VS based on document BSI-TL 03423 „Anforderungen zum Überschreiben von Datenträgern“ and the firmware erasure step has been extended by Eurosoft to address NVMe SSD disks as well.

Name	Pass	Algorithm
BSI-GS	1	Entire device is wiped with Marsaglia-Zaman random numbers.
	2	Apply firmware method relevant for disk type
		ATA/SATA : perform Enhanced Secure Erase if command is supported, else perform Secure Erase
		SCSI/SAS : perform Format Unit command
		NVMe: perform Format NVM command
	3	If the above methods are not supported or fail, then a Zero pass is performed
	4	Verify the erasure.
BSI-GSE	1 -2	Entire device is wiped with Marsaglia-Zaman random numbers
	3	Apply firmware method relevant for disk type
		ATA/SATA : perform Enhanced Secure Erase if command is supported, else perform Secure Erase
		SCSI/SAS : perform Format Unit command
		NVMe: perform Format NVM command
	4	If the above methods are not supported or fail, then a Zero pass is performed
	5	Verify the erasure.

Command line execution of these methods are as follows:

zerodatawindows.exe /me bsi-gs ...

zerodatawindows.exe /me bsi-gse ...

Extended Firmware Erasure Methods

For additional information about firmware erasure methods please see Appendix C. These methods implement TCG Opal V1.0 and TCG Opal V2.0 Firmware Data Erasure Methods with added verification rounds to overcome any discrepancies due to manufacturer specific implementation issues.

TCG OPAL Firmware Data Erasure Methods

For additional information about firmware erasure methods please see Appendix C. These methods implement TCG Opal V1.0 and TCG Opal V2.0 Firmware Data Erasure Methods with added verification rounds to overcome any discrepancies due to manufacturer specific implementation issues.

Name	Pass	Algorithm
TCG-Erase	1	Determine disk type, determine TCG Opal v1.0 or TCG Opal V2.0 erasure is reported as supported by the disk or not. If supported, apply preliminary verification steps, apply firmware command, apply verification. If not available: fail erasure.

NVMe Firmware Data Erasure Methods

These methods implement NVMe Firmware Data Erasure Methods with added verification rounds to overcome any discrepancies due to manufacturer specific implementation issues.

Name	Pass	Algorithm
NVM-Format	1	Determine disk type, determine NVM Format command is reported as supported by the disk or not. If supported, apply preliminary verification steps, apply firmware command, apply verification. If not available: fail erasure.
NVM-Sanitize	1	Currently no disk implements these commands properly.

SANITIZE Firmware Data Erasure Methods

These methods implement SANITIZE Firmware Data Erasure Methods for ATA/SATA and SCSI/SAS disks with added verification rounds to overcome any discrepancies due to manufacturer specific implementation issues. Each method is specified in a generic manner at command line, and relevant commands are issued to the disks depending on disk type. For additional information about firmware erasure methods please see Appendix C.

Name	Pass	Algorithm
Sanitize-Crypto	1	Determine disk type, determine whether SANITIZE Crypto Scramble command is reported as supported by the disk or not. If supported, apply preliminary verification steps, apply firmware command, apply verification. If not available: fail erasure.
Sanitize-Block	1	Determine disk type, determine whether SANITIZE Block Erase command is reported as supported by the disk or not. If supported, apply preliminary verification steps, apply firmware command, apply verification. If not available: fail erasure.
Sanitize-Overwrite	1	Determine disk type, determine whether SANITIZE Overwrite command is reported as supported by the disk or not. If supported, apply preliminary verification steps, apply firmware command, apply verification. If not available: fail erasure.

ATA Firmware Data Erasure Methods

For additional information about firmware erasure methods please see Appendix C. These methods implement ATA Firmware Data Erasure Methods with added verification rounds to overcome any discrepancies due to manufacturer specific implementation issues.

Name	Pass	Algorithm
ATA-SecureErase	1	Determine disk type, determine ATA SECURE ERASE command is reported as supported by the disk or not. If supported, apply preliminary verification steps, apply firmware command, and verify erasure. If not available: fail the erasure.
ATA-EnhancedSecureErase	1	Determine disk type, determine ATA ENHANCED SECURE ERASE command is reported as supported by the disk or not. If supported, apply preliminary verification steps, apply firmware command, and verify erasure. If not available: fail the erasure.
ATA-Sanitize	1	Determine disk type, determine ATA SANITIZE commands is reported as supported by the disk or not. Apply preliminary verification steps, apply firmware commands and then apply verification. Repeat these steps in the following order until one of the below methods are reported as successful. • SANITIZE Crypto Scramble • SANITIZE Block Erase • SANITIZE Overwrite If all three commands fail: fail the erasure.
ATA-Crypto-BlockErase	1	Determine disk type, determine firmware erasure method(s) specified for device type are available or not. Apply preliminary verification steps, apply firmware commands, and then apply verification. Repeat these steps in the following order until one of the below methods are reported as successful. • SANITIZE Crypto Scramble • SANITIZE Block Erase If all two commands fail: fail erasure.

SCSI/SAS Firmware Data Erasure Methods

For additional information about firmware erasure methods please see Appendix C. These methods implement SCSI Firmware Data Erasure Methods with added verification rounds to overcome any discrepancies due to manufacturer specific implementation issues.

NOTE: SCSI/SAS firmware commands are disabled by default but can be enabled using /DSP parameter.

Almost all existing SAS RAID controllers block firmware erasure commands sent to disk connected to them and pure SAS controller cards that do not block firmware commands are rarely used. Some SAS RAID controllers show an aggressive behavior to maintain RAID volume integrity and regularly check disks attached to them, even if they are not part of any RAID volume. **As these checks break execution of firmware erasure commands and render the disk unusable, ZeroData Windows does not apply firmware erasure commands by default.**

If /DSP is present in command line, this protection is lifted, and firmware erasure commands are passed to the SAS controller.

Name	Pass	Algorithm
SCSI-FormatUnit	1	Determine disk type, determine whether Format Unit command is reported as supported by the disk or not. If supported, apply preliminary verification steps, apply firmware command, apply verification. If not available: the erasure fails.
SCSI-Sanitize	1	Determine disk type, determine whether SANITIZE commands is reported as supported by the disk or not. Apply preliminary verification steps, apply firmware commands, apply verification. Repeat these steps in the following order until one of the below methods are reported as successful. • SANITIZE Crypto Scramble • SANITIZE Block Erase • SANITIZE Overwrite If all three commands fail, the erasure fails.

Overwrite Erasure Methods Synthesized And Extended By Eurosoft

Details of these erasure methods and their implementation of passes in exact order are listed below.

Name	Pass	Algorithm	Pattern
Personal	Eurosoft algorithm		
	1	Entire device is wiped with zeroes.	0x00000000
Professional	Eurosoft algorithm		
	1	Entire device is wiped with Marsaglia-Zaman random numbers.	
Corporate	Eurosoft algorithm		
	1 - 3	Entire device is wiped with Marsaglia-Zaman random numbers.	
Military	Eurosoft algorithm		
	1 - 7	Entire device is wiped with Marsaglia-Zaman random numbers.	
ESFast	Eurosoft algorithm		
	1	Entire device is wiped with Marsaglia-Zaman random numbers.	
	2 - 3	Entire device is wiped with non-linear pass using Marsaglia-Zaman random numbers.	
	4	Entire device is wiped with zeroes.	0x00000000
ESStandard	Eurosoft algorithm		
	1 - 4	Entire device is wiped with Marsaglia-Zaman random numbers.	
	5 - 12	Entire device is wiped with non-linear pass using Marsaglia-Zaman random numbers.	
	13	Entire device is wiped with zeroes.	0x00000000
ESDeep	Eurosoft algorithm		
	1 - 8	Entire device is wiped with Marsaglia-Zaman random numbers.	
	9 - 24	Entire device is wiped with non-linear pass using Marsaglia-Zaman random numbers.	
	25	Entire device is wiped with zeroes.	0x00000000
Initialise	Eurosoft algorithm		
	1	First 0.1% of disk is wiped with zeroes.	0x00000000

Overwrite Erasure Methods Optimized For SSD

For special notes about SSD drive erasure please see appendices A & B.

Details of these erasure methods and their implementation of passes in the exact order are listed below.

Name	Pass	Algorithm	Pattern
SSDStandard	Eurosoft algorithm		
	1 - 2	Entire device is wiped with Marsaglia-Zaman random numbers.	
SSDRandom4	Eurosoft algorithm		
	1 - 4	Entire device is wiped with Marsaglia-Zaman random numbers.	
SSDRandom6	Eurosoft algorithm		
	1 - 6	Entire device is wiped with Marsaglia-Zaman random numbers.	

Most Current Overwrite Erasure Standards

For special notes about SSD drive erasure please see appendix A & B.

Details of these erasure methods and their implementation of passes in exact order are listed below.

Name	Pass	Algorithm	Pattern
HMGIS5Lower	HMG Information Security 5 Lower/Baseline Method		
	1	Entire device is wiped with Marsaglia-Zaman random numbers and write is verified.	
HMGIS5Higher	HMG Information Security 5 Higher/Enhanced Method		
	1	Entire device is wiped with a specified character	0x00000000
	2	Entire device is wiped with a specified character	0xFFFFFFFF
	3	Entire device is wiped with Marsaglia-Zaman random numbers and write is verified.	

Regular Magnetic Disk Erasure Methods

Details of these erasure methods and their implementation of passes in exact order are listed below.

Name	Pass	Pass Details	Pattern
USDoD	United States Department of Defense 5220.22-M method		
	1	Entire device is wiped with a specified character	0x55555555
	2	Entire device is wiped with a specified character	0xAAAAAAAA
	3	Entire device is wiped with Marsaglia-Zaman random numbers and write is verified.	
USDoDMECE	United States Department of Defense 5220.22-M ECE method		
	1	Entire device is wiped with a specified character	0x55555555
	2	Entire device is wiped with a specified character	0xAAAAAAAA
	3	Entire device is wiped with Marsaglia-Zaman random numbers and write is verified	
	4	Entire device is wiped with Marsaglia-Zaman random numbers	
	5	Entire device is wiped with a specified character	0x55555555
	6	Entire device is wiped with a specified character	0xAAAAAAAA
	7	Entire device is wiped with Marsaglia-Zaman random numbers and write is verified.	
GermanVSITR	Verschlusssache IT Richtlinien as originally defined by Bundesamt für Sicherheit in der Informationstechnik		
	1	Entire device is wiped with a specified character	0x00000000
	2	Entire device is wiped with a specified character	0xFFFFFFFF
	3	Entire device is wiped with a specified character	0x00000000
	4	Entire device is wiped with a specified character	0xFFFFFFFF
	5	Entire device is wiped with a specified character	0x00000000
	6	Entire device is wiped with a specified character	0xFFFFFFFF
	7	Entire device is wiped with Marsaglia-Zaman random numbers.	
NAVSO	NAVSO P-5239-26 method as described on NAVSO Publication 5239-26		
	1	Entire device is wiped with a specified character	0x00000000
	2	Entire device is wiped with the complement of the specified character	0xFFFFFFFF
	3	Entire device is wiped with Marsaglia-Zaman random numbers and write is verified.	
OPNAVINST	United States Navy Intelligence Service OPNAVIST 5239.1a method as defined on 1993 document		
	1	Entire device is wiped with a specified character	0xFFFFFFFF
	2	Entire device is wiped with a specified character	0x00000000
	3	Entire device is wiped with Marsaglia-Zaman random numbers and write is verified.	
AirForceSecurity	AFSSI-5020 sanitization method as originally defined in the Air Force System Security Instruction 5020		
	1	Entire device is wiped with a specified character	0x00000000
	2	Entire device is wiped with a specified character	0xFFFFFFFF
	3	Entire device is wiped with Marsaglia-Zaman random numbers and write is verified.	

Details of these erasure methods and their implementation of passes in exact order are listed below.

Name	Pass	Pass Details	Pattern
USArmyAR380	United States Army AR 380-19 sanitization method as defined in Army Regulation 380-19 Appendix F		
	1	Entire device is wiped with Marsaglia-Zaman random numbers	
	2	Entire device is wiped with a specified character	0x00000000
	3	Entire device is wiped with the complement of the specified character and write is verified.	0xFFFFFFFF
NCSC	NCSC-TG-025 as described by National Computer Security Center Forest Green Book		
	1	Entire device is wiped with a specified character and write is verified	0x00000000
	2	Entire device is wiped with complement of a specified character and write is verified	0xFFFFFFFF
	3	Entire device is wiped with Marsaglia-Zaman random numbers and write is verified.	
NSA1301	National Security Agency 130-1 standard		
	1	Entire device is wiped with Marsaglia-Zaman random numbers	
	2	Entire device is wiped with Marsaglia-Zaman random numbers	
	3	Entire device is wiped with 0x00000000 and write is verified.	0x00000000
CSEC	CSEC ITSG-06 sanitization method as defined in Section 2.3.2 of IT Security Guidance 06: Clearing and Declassifying Electronic Data Storage Devices, published by Communication Security Establishment Canada		
	1	Entire device is wiped with a specified character	0xFFFFFFFF
	2	Entire device is wiped with the complement of the specified character	0x00000000
	3	Entire device is wiped with Marsaglia-Zaman random numbers and write is verified	
RCMP	RCMP TSSIT OPS-II sanitization method as originally defined in Appendix Ops-II: Media Sanitation of the Technical Security Standards for Information Technology document, published by the Royal Canadian Mounted Police		
	1	Entire device is wiped with a specified character	0x00000000
	2	Entire device is wiped with a specified character	0xFFFFFFFF
	3	Entire device is wiped with a specified character	0x00000000
	4	Entire device is wiped with a specified character	0xFFFFFFFF
	5	Entire device is wiped with a specified character	0x00000000
	6	Entire device is wiped with a specified character	0xFFFFFFFF
	7	Entire device is wiped with Marsaglia-Zaman random numbers and write is verified	

Academic Proof Of Concept Magnetic Disk Erasure Methods

All methods implement passes in the exact order they are listed above. However, ZeroData Windows' Gutmann implementation follows the method description to the letter, with the first four and last four random write passes are applied as listed in the below sequence but passes 5 to 31 are applied in random order.

Schneier	Bruce Schneier's 7 pass algorithm as described in his 1996 book		
	1	Entire device is wiped with a specified character	0xFFFFFFFF
	2	Entire device is wiped with a specified character	0x00000000
	3-7	Entire device is wiped with Marsaglia-Zaman random numbers.	
Gutmann	Peter Gutmann's 35 pass algorithm as described in 1996 paper		
	1 - 4	Entire device is wiped with Marsaglia-Zaman random numbers	
	5	Entire device is wiped with a specified character	0x55555555
	6	Entire device is wiped with a specified character	0xAAAAAAAA
	7	Entire device is wiped with repeating pattern	0x924924
	8	Entire device is wiped with repeating pattern	0x492492
	9	Entire device is wiped with repeating pattern	0x249249
	10	Entire device is wiped with a specified character	0x00000000
	11	Entire device is wiped with a specified character	0x11111111
	12	Entire device is wiped with a specified character	0x22222222
	13	Entire device is wiped with a specified character	0x33333333
	14	Entire device is wiped with a specified character	0x44444444
	15	Entire device is wiped with a specified character	0x55555555
	16	Entire device is wiped with a specified character	0x66666666
	17	Entire device is wiped with a specified character	0x77777777
	18	Entire device is wiped with a specified character	0x88888888
	19	Entire device is wiped with a specified character	0x99999999
	20	Entire device is wiped with a specified character	0xAAAAAAAA
	21	Entire device is wiped with a specified character	0xBBBBBBBB
	22	Entire device is wiped with a specified character	0xCCCCCCCC
	23	Entire device is wiped with a specified character	0xDDDDDDDD
	24	Entire device is wiped with a specified character	0xEEEEEEEE
	25	Entire device is wiped with a specified character	0xFFFFFFFF
	26	Entire device is wiped with repeating pattern	0x924924
	27	Entire device is wiped with repeating pattern	0x492492
	28	Entire device is wiped with repeating pattern	0x249249
	29	Entire device is wiped with repeating pattern	0x6DB6DB
	30	Entire device is wiped with repeating pattern	0xB6DB6D
	31	Entire device is wiped with repeating pattern	0xDB6DB6
	32-35	Entire device is wiped with Marsaglia-Zaman random numbers.	

Pass Details – Zero, Fixed, Random Data and Verification

An “erasure method” consists of one or more passes where some form of data is written to the disk.

An erasure method is applied to a disk using the following format:

ZeroDataWindows /me method_name {other parameters}

All available method_name values are listed in below table with details of their passes. The method names are not case sensitive and can be written in any combination of small and capital letters; but they must match desired method name exactly.

Some examples are:

ZeroDataWindows /me hmgis5higher

ZeroDataWindows /me Gutmann

ZeroDataWindows /me nist800-88purge

ZeroDataWindows /me NIST800-88Clear

There are four general pass types employed by ZeroData Windows.

Zero pass: this involves writing the hexadecimal value of 0x00000000 to the disk. On some storage controllers, this pattern is compressed, and artificially big performance figures are reported.

Fixed pattern pass: this involves writing a fixed hexadecimal value in the form of 0x KLMNOPRS to the disk. On some storage controllers, some of these patterns is compressed and artificially big performance figures are reported. Most of these patterns have the form of 0xKKKKKKKK where all bytes are the same, but Gutmann method also employs passes that have the form 0xKLMKLM.

Random Data Pass: Whenever random data is mentioned in a method description, ZeroData Windows treats this requirement as a random data stream. Random data streams are using a Marsaglia-Zaman Random Number Generator which produces practically nonrepeating sequence of random data to fill the data buffer.

Non-linear Pass: This pattern is a Eurosoft feature not present in any competing product. The idea is to harden the data erasure process by adding randomness to the overwritten blocks on the disk.

On a regular overwrite pass, the whole disk area is overwritten with a pattern (whether a fixed one or random one).

On the other hand, a non-linear pass moves along disk area and at each block makes a random decision whether to write a random block of data to the location or not. In first non-linear pass, ½ of the whole disk area is written, on second non-linear pass ⅓ of the whole disk area is overwritten, on third pass ¼ of the whole disk is overwritten, on fourth pass 1/5 of the whole disk area is overwritten and so on. At the end of non-linear pass run, there is no way to deduce how many passes of data had been written to a sector. Example: for an erasure with HMG IS 5 Higher method applied to the disk and three additional non-linear passes applied to it, any sector on the disk might have been overwritten 3 times, 4 times, 5 times or 6 times, and it is impossible to know which sector has been overwritten how many times.

In comparison to regular overwrite passes, there is no performance hit on regular magnetic hard disks when non-linear passes are applied. However, solid state disks (SSD’s) become dirty with each overwrite pass, and they become much dirtier when non-linear passes are applied. With each non-linear pass, the SSD becomes

slower and slower, therefore the erasure time gets longer and longer. On high and mid-quality SSD's like Samsung 850 Pro and 850 Evo, the disk recovers from this performance hit when one Zero pass is applied to it; on low quality SSD's like Samsung 750 Evo, it takes multiple Zero passes to recover from this performance hit. Therefore, additional non-linear passes are applied to SSD's as last passes.

Due to these reasons, it is not advised to apply ESStandard and ESDeep methods on SSD's when data erasure time is of concern, however if data erasure quality is of concern these methods will provide very high level of confidence.

Verification Pass: These passes involve not only reading data and but also comparing the data to the pattern that is supposed to be written on the previous write pass.

All passes use a block size of 16 MB while writing to disk.

Patterns written for each pass are listed in method descriptions below.

How To Use ZeroData Windows From Command Line

The first part of this user manual described how your organization should approach Data Sanitization for data stored in disks. The sections after introduced all the features and command line switches available in ZeroData Windows.

Now comes the critical question: how do you combine all this information to match requests of your organization or your customers ?

Any ZeroData Windows erasure run produces two outputs:

- One or more disks which have their original content replaced with some other content as described in definition of chosen erasure method,
- Multiple computer files in text, XML and PDF file formats produced during the erasure run, each recording information on various steps carried out and various reports documenting the erasure run and the final state of erased disks.

Depending on what the requirements of organization are, sanitized disks may be re-used internally or externally, or properly disposed of. Again, depending on the requirements of the organization, some or all of computer files might be safely stored as they are, some of the files might be printed and stored as hard copies, they may be processed and transmitted as they are needed.

Therefore, to carry out a proper ZeroData Windows erasure, ZeroData Windows features must be employed to satisfy needs of target organization.

Learning the target organization's needs is easy; generally asking them what they need to be done on the disks is enough. The answers may range from "we require a three pass overwrite standard with 10% verification for mechanical hard disks" to "I need a quick and cheap erasure method that destroys previous contents of my disk". Generally, the answer to this question does not include what their criteria for risky and/or unusable disks are. Therefore, this point must be brought forward and agreed on in writing before attempting any erasure.

The second step involves what kind of documentation the target organization needs. ZeroData Windows produces very detailed logs in machine readable XML format. However, generally customers do not need that much of detail and are interested in concise reports that document crucial details recorded in these logs which they can use to prove the disks had been properly sanitized in case they are audited for their data sanitization processes. ZeroData Windows processes these XML logs and produces output reports that contain the same information in three different file formats: text, XML and PDF. In addition to these computer files, ZeroData Windows can write a short summary report to the first sectors of erased disks and create a small bootable partition on erased disks to display this short summary report. Reporting Console application can also process XML logs and create the same text, XML and PDF report files; and additionally, it can also create various labels and send them to printers.

In next section, we will look at the digital files created by ZeroData Windows, then we will build up some sample command lines to satisfy data sanitization requirements of some hypothetic customers.

Understanding and Using ZeroData Windows Output

ZeroData Windows produces numerous output files for each disk erasure run. These files can be divided into two broad classes : log files and combined files.

- Log files : The moment ZeroData Windows starts, it produces log files to keep track of information it collects. All log files are produced in XML file format. ZeroData Windows log files are distinguished as follows:

    - [GOF_File_Name]_[GUID].xml : this file is created when ZeroData Windows starts and contains information on ZeroData Windows software, erasure settings, system information for the computer, customer information and a summary of processed disk counts.

      To uniquely identify each ZeroData Windows data sanitization operation, a unique identifier called GUID (or UUID in Microsoft vocabulary) is created and attached to all internally created files to identify all files related to the same data sanitization operation. Details on ZeroData Windows software details, application settings, and hardware details of the system are recorded in this file.

      If no GOF_File_Name is specified using /GOF command line switch, then "[GOF_File_Name]_" part will not be present in the file name, and the file name will be [date – time]_[GUID].xml .

    - [GOF_File_Name]_[GUID]_[date – time]_**LD.xml** : this file contains the "List of Disks" connected to the system and details of these disks.

      Current date and time are added to file name for easier identification as well. The string "_LD.xml" is attached to the end of file name.

      If no GOF_File_Name is specified using /GOF command line switch, then "[GOF_File_Name]_" part will not be present in the file name, and the file name will be [date – time]_[GUID]_[date – time]_**LD.xml**.

      In case the /NUUID command line switch is specified, then GUID and last date-time parts will not be present, and the file name will be [GOF_File_Name]_LD.xml .

    - [GOF_File_Name]_[GUID]_[Disk ID number]_[Disk Serial Number]_[Disk World Wide Number]_[date – time]_**log.xml** : this file contains details for erasure settings and erasure progress for each disk.

      If no GOF_File_Name is specified using /GOF command line switch, then "[GOF_File_Name]_" part will not be present in the file name, and the file name will be [date – time]_GUID]_[Disk ID number]_[Disk Serial Number]_[Disk World Wide Number]_[date – time]_**log.xml**.

      Every operating system assigns a Disk ID number to connected disks to distinguish them from each other, Windows operating system assigns labels like "Disk 0", "Disk 1", "Disk 11" to disks.

      Each disk has a Disk Serial Number assigned by disk manufacturers to identify individual disks for various purposes, in general this serial number is stored in the disk itself and can be

retrieved from the disk, if this serial number cannot be retrieved, the value “NA” (Not Available) is shown instead.

In the same manner, most disks (but not all of them) have a second serial number which is supposed to be unique in the whole world and this serial number is called “Disk World Wide Number”. In general, this serial number is stored in the disk itself and can be retrieved from the disk, if this Disk World Wide Number cannot be retrieved, the value “WWNNA” (World Wide Number Not Available) is shown instead.

In case the /NUUID command line switch is specified, the file name pattern does not change – disk erasure log file names are not affected by /NUUID command switch.

- [GOF_File_Name]_[GUID]_**[Disk ID number]**_[Disk Serial Number]_[Disk World Wide Number]_[date – time]_**ead_log.xml** : this file is only created when the /GDER (Generate Disk Erasure Reports) command line switch is specified in the command line and contains combined details for a specific disk erasure that are extracted from the above XML files. System, disk and erasure settings and erasure progress are combined and presented as a complete description of a disk erasure. This file is used to create reports for individual disk erasures.

  If no GOF_File_Name is specified using /GOF command line switch, then “[GOF_File_Name]_” part will not be present in the file name, and the file name will be [date – time]_[GUID]_**[Disk ID number]**_[Disk Serial Number]_[Disk World Wide Number]_[date – time]_**ead_log.xml**.

  In practice, a single disk that is erased, but the string “ead” is added to file name to denote this file as a combined log file from which individual disk erasure reports can be created.

  In case where /NUUID command switch is specified in the command line, then the file name will be [GOF_File_Name]_[n]_log.xml, where “n” is the ID of the disk.

  For example, if disk ID is 0, then file name will be [GOF_File_Name]_0_log.xml, if disk ID is 6, then file name will be [GOF_File_Name]_6_log.xml .

- [GOF_File_Name]_[GUID]_**ead_log.xml** : this file contains combined details of all disk erasures carried out. System, disk and erasure settings and erasure progress for all disks are combined and presented as a complete description of all disk erasures carried out in erasure session. This file is used to create reports for the erasure session.

  If no GOF_File_Name is specified using /GOF command line switch, then “[GOF_File_Name]_” part will not be present in the file name, and the file name will be [date – time_[GUID]_**ead_log.xml**.

  Regardless of whether there was a single disk that was erased or multiple disks, the string “ead” (Erase All Disks) is added to file name to denote this file as a combined log file from which a system wide disk erasure report can be created.

  In case where /NUUID command switch is specified in the command line, then the file name will be [GOF_File_Name]_log.xml .

- Report files: Reports are created by processing log files. They contain a subset of information present in log files and erasure progress details are summarized to create a concise report.

    - [GOF_File_Name]_[GUID]_**[Disk ID number]**_[Disk Serial Number]_[Disk World Wide Number]_[date – time]_**ead_rep.xml** : this file is only created if /GDER switch is specified in the command line and contains a concise report of a specific disk erasure in XML format.

      If no GOF_File_Name is specified using /GOF command line switch, then "[GOF_File_Name]_" part will not be present in the file name, and the file name will be [date – time]_[GUID]_**[Disk ID number]**_[Disk Serial Number]_[Disk World Wide Number]_[date – time]_**ead_rep.xml** .

      In case where /NUUID command switch is specified in the command line, then the file name will be [GOF_File_Name]_[n]_rep.xml, where "n" is the ID of the disk.

      For example, if disk ID is 0, then file name will be [GOF_File_Name]_0_rep.xml, if disk ID is 6, then file name will be [GOF_File_Name]_6_rep.xml .

    - [GOF_File_Name]_[GUID]_**[Disk ID number]**_[Disk Serial Number]_[Disk World Wide Number]_[date – time]_**ead_rep.txt** : this file is only created if /GDER switch is specified in the command line and contains a concise report of a specific disk erasure in text format.

      If no GOF_File_Name is specified using /GOF command line switch, then "[GOF_File_Name]_" part will not be present in the file name, and the file name will be [date – time]_[GUID]_**[Disk ID number]**_[Disk Serial Number]_[Disk World Wide Number]_[date – time]_**ead_rep.txt** .

      In case where /NUUID command switch is specified in the command line, then the file name will be [GOF_File_Name]_[n]_rep.txt, where "n" is the ID of the disk.

      For example, if disk ID is 0, then file name will be [GOF_File_Name]_0_rep.txt, if disk ID is 6, then file name will be [GOF_File_Name]_6_rep.txt .

    - [GOF_File_Name]_[GUID]_**[Disk ID number]**_[Disk Serial Number]_[Disk World Wide Number]_[date – time]_**ead_rep.pdf** : this file is only created if /GDER switch is specified in the command line and contains a concise report of a specific disk erasure in PDF format.

      If no GOF_File_Name is specified using /GOF command line switch, then "[GOF_File_Name]_" part will not be present in the file name, and the file name will be [date – time]_[GUID]_**[Disk ID number]**_[Disk Serial Number]_[Disk World Wide Number]_[date – time]_**ead_rep.pdf** .

      In case where /NUUID command switch is specified in the command line, then the file name will be [GOF_File_Name]_[n]_rep.pdf, where "n" is the ID of the disk.

      For example, if disk ID is 0, then file name will be [GOF_File_Name]_0_rep.pdf, if disk ID is 6, then file name will be [GOF_File_Name]_6_rep.pdf .

- [GOF_File_Name]_[GUID]_**ead_rep.xml** : this file contains combined report of all disk erasures carried out in XML format in the ZeroData Windows data sanitization operation identified by the GUID.

  If no GOF_File_Name is specified using /GOF command line switch, then "[GOF_File_Name]_" part will not be present in the file name, and the file name will be [date – time_[GUID]_**ead_rep.xml** .

  In case where /NUUID command switch is specified in the command line, then the file name will be [GOF_File_Name]_rep.xml .

- [GOF_File_Name]_[GUID]_**ead_rep.txt** : this file contains combined report of all disk erasures carried out in text format in the ZeroData Windows data sanitization operation identified by the GUID.

  If no GOF_File_Name is specified using /GOF command line switch, then "[GOF_File_Name]_" part will not be present in the file name, and the file name will be [date – time_[GUID]_**ead_rep.txt** .

  In case where /NUUID command switch is specified in the command line, then the file name will be [GOF_File_Name]_rep.txt .

- [GOF_File_Name]_[GUID]_**ead_rep.pdf** : this file contains combined report of all disk erasures carried out in pdf format in the ZeroData Windows data sanitization operation identified by the GUID.

  If no GOF_File_Name is specified using /GOF command line switch, then "[GOF_File_Name]_" part will not be present in the file name, and the file name will be [date – time_[GUID]_**ead_rep.pdf** .

  In case where /NUUID command switch is specified in the command line, then the file name will be [GOF_File_Name]_rep.pdf .

ZeroData Windows XML logs and reports contain a multitude of date and time values, a multitude of GUID values to uniquely identify operation steps and a final digital signature created based on XML file contents. With the number of unique identifiers present, any change to XML file contents will break the digital signature and any tampering will be detected by Reporting Console Tamper Check feature.

PDF file format does not support digital signatures to detect content tampering. To overcome this problem, a digital signature for PDF contents is added to the Subject metadata of PDF file.

Text reports do not support checking for digital signatures and therefore any tampering cannot be detected.

Reporting Console application contains a feature to detect if logs are tampered with or not. Please consult the section named "Verifying Authenticity of XML logs in Reporting Console" of this manual.

Samples for Command Line Option Usage

ZeroDataWindows.exe

- Application will start and display a dialog window asking whether the user wants to supply erasure operator details or not.
- Nothing else will be done, application will wait for user input.

ZeroDataWindows.exe /help

- A help window listing ZeroData Windows command line switches and erasure methods will be displayed.
- Nothing else will be done and the window will be closed when the user clicks on the Close button.

ZeroDataWindows.exe /nc AcceptTheRisk

- Application will start without asking whether the user wants to supply erasure operator details or not.
- Splash screen will be displayed, and startup steps will be carried out.
- The main erasure window will be displayed after all startup steps end.
- Nothing else will be done, application will wait for the user input.

ZeroDataWindows /eadp /gof eadp_default_filenames

- This command line will erase all attached disks in parallel with default methods – Personal method for HDD's and NIST800-88Purge for SSD's in parallel, erasing all disks simultaneously.
- Application will start and display a dialog window asking whether the user wants to supply erasure operator details or not. This dialog window will stay in focus until user input occurs.
- After user input, splash screen will be displayed, and startup steps will be carried out.
- The main erasure window will be displayed after all startup steps end.
- Hidden area removal will be attempted on each disk as it is enabled by default.
- Verification will not be carried out for HDD's as Personal method does not have any default verification steps.
- NIST800-88Purge method has default verification steps and therefore verification will be carried out for SSD's.
- As there are no conditions set for the erasure to stop, erasure will continue until all passes are executed.
- As neither /nuuid nor no report file type is specified, the combined log and report files will be in XML file format and they will be named as:
    - eadp_default_filenames_[GUID]_ead_log.xml
    - eadp_default_filenames_[GUID]_ead_rep.xml
    - Please note that, if the file name specified in /GOF is static, /nuuid switch is applied and all files are created in the same folder, each erasure run will create combined files with the same names. In this case, new files will be written over old files and all combined files except the most recent on will be lost. As a solution, either a dynamic file name can be created as a system variable and supplied to /gof switch as parameter, or /nuuid switch is not used. Please refer to the end of this section on a sample idea for creating unique and dynamic file names.
    - A sample execution of the above command line produced the following files:
        - eadp_default_filenames_d3a19841-2df9-4c72-89ba-71a17ead220a.xml

        - eadp_default_filenames_d3a19841-2df9-4c72-89ba-71a17ead220a_20210301-143459_LD.xml
        - eadp_default_filenames_d3a19841-2df9-4c72-89ba-71a17ead220a_Disk0_50026B723202E09E_50026B723202E09E_20210301-143459_log.xml
        - eadp_default_filenames_d3a19841-2df9-4c72-89ba-71a17ead220a_Disk1_S11DNEAC933755_WWNNA_20210301-143459_log.xml
        - eadp_default_filenames_d3a19841-2df9-4c72-89ba-71a17ead220a_Disk3_PMAP1234_WWNNA_20210301-143459_log.xml
        - eadp_default_filenames_d3a19841-2df9-4c72-89ba-71a17ead220a_ead_log.xml
        - eadp_default_filenames_d3a19841-2df9-4c72-89ba-71a17ead220a_ead_rep.xml

ZeroDataWindows /eadp /gof eadp_default_filenames /nuuid

- Notice that this command line is the same command line as in previous sample command line, but it has the additional /nuuid command switch.
- This command line will erase all attached disks in parallel with default methods – Personal method for HDD's and NIST800-88Purge for SSD's in parallel, erasing all disks simultaneously.
- Application will start and display a dialog window asking whether the user wants to supply erasure operator details or not. This dialog window will stay in focus until user input occurs.
- After user input, splash screen will be displayed, and startup steps will be carried out.
- The main erasure window will be displayed after all startup steps end.
- Hidden area removal will be attempted on each disk as it is enabled by default.
- Verification will not be carried out for HDD's as Personal method does not have any default verification steps.
- NIST800-88Purge method has default verification steps and therefore verification will be carried out for SSD's.
- As there are no conditions set for the erasure to stop, erasure will continue until all passes are executed.
- As /nuuid is specified but no report file type is specified, the combined log and report files will be in XML file format and they will be named as:
    - eadp_default_filenames_log.xml
    - eadp_default_filenames_rep.xml
    - Please note that, if the file name specified in /GOF is static, /nuuid switch is applied and all files are created in the same folder, each erasure run will create combined files with the same names. In this case, new files will be written over old files and all combined files except the most recent on will be lost. As a solution, either a dynamic file name can be created as a system variable and supplied to /gof switch as parameter, or /nuuid switch is not used. Please refer to the end of this section on a sample idea for creating unique and dynamic file names.
    - A sample execution of the above command line produced the following files:
        - eadp_default_filenames_a526dada-429e-4e94-bc0d-7630ffbd58ab.xml
        - eadp_default_filenames_a526dada-429e-4e94-bc0d-7630ffbd58ab_Disk0_50026B723202E09E_50026B723202E09E_20210301-143727_log.xml
        - eadp_default_filenames_a526dada-429e-4e94-bc0d-7630ffbd58ab_Disk1_S11DNEAC933755_WWNNA_20210301-143727_log.xml
        - eadp_default_filenames_a526dada-429e-4e94-bc0d-7630ffbd58ab_Disk3_PMAP1234_WWNNA_20210301-143727_log.xml
        - eadp_default_filenames_LD.xml

- eadp_default_filenames_log.xml
- eadp_default_filenames_rep.xml

ZeroDataWindows /eadp /vp 29 /gof erasealldisks07

- This command line will erase all attached disks with default methods – Personal method for HDD's and NIST800-88Purge for SSD's in parallel, erasing all disks simultaneously.
- Application will start and display a dialog window asking whether the user wants to supply erasure operator details or not. This dialog window will stay in focus until user input occurs.
- After user input, splash screen will be displayed, and startup steps will be carried out.
- The main erasure window will be displayed after all startup steps end.
- Even though 29% verification is specified, this parameter will not be applied. Personal erasure method does not have any verification pass and NIST800-88Purge has a default erasure pass that verifies 10% of the disk.
- As there are no conditions set for the erasure to stop, erasure will continue until all passes are executed. Even if thousands of errors are detected, erasure will not stop.
- As neither /nuuid nor report file type is specified, the combined log and report files will be in XML file format and they will be named as:
    - erasealldisks07_[GUID]_ead_log.xml
    - erasealldisks07_[GUID]_ead _rep.xml
    - Please note that, if the file name specified in /GOF is static, /nuuid switch is applied and all files are created in the same folder, each erasure run will create combined files with the same names. In this case, new files will be written over old files and all combined files except the most recent on will be lost. As a solution, either a dynamic file name can be created as a system variable and supplied to /gof switch as parameter, or /nuuid switch is not used. Please refer to the end of this section on a sample idea for creating unique and dynamic file names.
    - A sample execution of the above command line produced the following files:
        - erasealldisks07_f84a9c4e-492c-4b28-9f37-0e711101a5ee.xml
        - erasealldisks07_f84a9c4e-492c-4b28-9f37-0e711101a5ee_20210301-143948_LD.xml
        - erasealldisks07_f84a9c4e-492c-4b28-9f37-0e711101a5ee_Disk0_50026B723202E09E_50026B723202E09E_20210301-143948_log.xml
        - erasealldisks07_f84a9c4e-492c-4b28-9f37-0e711101a5ee_Disk1_S11DNEAC933755_WWNNA_20210301-143948_log.xml
        - erasealldisks07_f84a9c4e-492c-4b28-9f37-0e711101a5ee_Disk3_PMAP1234_WWNNA_20210301-143948_log.xml
        - erasealldisks07_f84a9c4e-492c-4b28-9f37-0e711101a5ee_ead_log.xml
        - erasealldisks07_f84a9c4e-492c-4b28-9f37-0e711101a5ee_ead_rep.xml

ZeroDataWindows /eads /me hmgis5higher /vp 10 /ec 5 /gof gof20210107-batch1 /nuuid

- This command line will erase all attached disks with HMG IS 5, Higher method.
- Application will start and display a dialog window asking whether the user wants to supply erasure operator details or not. This dialog window will stay in focus until user input occurs.
- After user input, splash screen will be displayed, and startup steps will be carried out.
- The main erasure window will be displayed after all startup steps end.
- Only one disk will be erased at any given time as erasures will be carried out sequentially, when a disk erasure ends, then next disk in the line will start erasure until all disks are erased.

- Verification will be carried out on 10% of disks as HMG IS 5, Higher method has a default erasure pass after the end of third write pass.
- Erasure will continue for each disk until 5 errors are encountered.
    - If number of encountered errors is less than 5, the erasure will be reported as successful. Next disk on the line will start processing.
    - If number of encountered errors reaches 5, the erasure will stop and erasure will be reported as failed. Next disk on the line will start processing.
- As /nuuid is specified but no report type is specified, combined log and report files will be named as:
    - gof20210107-batch1_log.xml
    - gof20210107-batch1_rep.xml
    - Please note that, if the file name specified in /GOF is static, /nuuid switch is applied and all files are created in the same folder, each erasure run will create combined files with the same names. In this case, new files will be written over old files and all combined files except the most recent on will be lost. As a solution, either a dynamic file name can be created as a system variable and supplied to /gof switch as parameter, or /nuuid switch is not used. Please refer to the end of this section on a sample idea for creating unique and dynamic file names.
    - A sample execution of the above command line produced the following files:
        - gof20210107-batch1_c005697b-fa69-4abb-9913-617a34cf9775.xml
        - gof20210107-batch1_c005697b-fa69-4abb-9913-617a34cf9775_Disk0_50026B723202E09E_50026B723202E09E_20210301-144134_log.xml
        - gof20210107-batch1_c005697b-fa69-4abb-9913-617a34cf9775_Disk1_S11DNEAC933755_WWNNA_20210301-144135_log.xml
        - gof20210107-batch1_c005697b-fa69-4abb-9913-617a34cf9775_Disk3_PMAP1234_WWNNA_20210301-144134_log.xml
        - gof20210107-batch1_LD.xml
        - gof20210107-batch1_log.xml
        - gof20210107-batch1_rep.xml

ZeroDataWindows /eads /me hmgis5higher /vp 10 /ec 5 /gof gof20210107-batch1

- Notice that this command line is the same command line as in previous sample command line, but it has the no /nuuid command switch.
- This command line will erase all attached disks with HMG IS 5, Higher method.
- Application will start and display a dialog window asking whether the user wants to supply erasure operator details or not. This dialog window will stay in focus until user input occurs.
- After user input, splash screen will be displayed, and startup steps will be carried out.
- The main erasure window will be displayed after all startup steps end.
- Only one disk will be erased at any given time as erasures will be carried out sequentially, when a disk erasure ends, then next disk in the line will start erasure until all disks are erased.
- Verification will be carried out on 10% of disks as HMG IS 5, Higher method has a default erasure pass after the end of third write pass.
- Erasure will continue for each disk until 5 errors are encountered.
    - If number of encountered errors is less than 5, the erasure will be reported as successful. Next disk on the line will start processing.
    - If number of encountered errors reaches 5, the erasure will stop and erasure will be reported as failed. Next disk on the line will start processing.
- As neither /nuuid nor report type is specified, combined log and report files will be named as:
    - gof20210107-batch1_[GUID]_ead_log.xml
    - gof20210107-batch1_[GUID]_ead_rep.xml

- Please note that, if the file name specified in /GOF is static, /nuuid switch is applied and all files are created in the same folder, each erasure run will create combined files with the same names. In this case, new files will be written over old files and all combined files except the most recent on will be lost. As a solution, either a dynamic file name can be created as a system variable and supplied to /gof switch as parameter, or /nuuid switch is not used. Please refer to the end of this section on a sample idea for creating unique and dynamic file names.
- A sample execution of the above command line produced the following files:
  - gof20210107-batch1_270e5a10-0e92-427e-aa69-9eea62c7adce.xml
  - gof20210107-batch1_270e5a10-0e92-427e-aa69-9eea62c7adce_20210301-145606_LD.xml
  - gof20210107-batch1_270e5a10-0e92-427e-aa69-9eea62c7adce_Disk0_50026B723202E09E_50026B723202E09E_20210301-145606_log.xml
  - gof20210107-batch1_270e5a10-0e92-427e-aa69-9eea62c7adce_Disk1_S11DNEAC933755_WWNNA_20210301-145607_log.xml
  - gof20210107-batch1_270e5a10-0e92-427e-aa69-9eea62c7adce_Disk3_PMAP1234_WWNNA_20210301-145606_log.xml
  - gof20210107-batch1_270e5a10-0e92-427e-aa69-9eea62c7adce_ead_log.xml
  - gof20210107-batch1_270e5a10-0e92-427e-aa69-9eea62c7adce_ead_rep.xml

ZeroDataWindows /eadp /nc AcceptTheRisk /me usdodmece /gof mwrec5-batch3 /rft txt

- This command line will erase all attached disks with US DoD 5220.22-M ECE method in parallel.
- Application will start and without displaying a dialog window asking whether the user wants to supply erasure operator details or not.
- Splash screen will be displayed without waiting for user input, and startup steps will be carried out.
- The main erasure window will be displayed after all startup steps end.
- Erasure will start automatically on all disks simultaneously.
- As there are no conditions set for the erasure to stop, erasure will continue until all passes are executed. Even if thousands of errors are detected, erasure will not stop.
- Verification will be carried out on 1% of disks as HMG IS 5, Higher method has a default erasure pass after the end of third write pass and as no other verification percentage is specified, 1% verification will be carried out as default.
- As the report file type is specified as text, combined log and report files will be named as:
  - mwrec5-batch3_[GUID]_ead_log.xml
  - mwrec5-batch3_[GUID]_ead_rep.txt
  - Please note that, if the file name specified in /GOF is static, /nuuid switch is applied and all files are created in the same folder, each erasure run will create combined files with the same names. In this case, new files will be written over old files and all combined files except the most recent on will be lost. As a solution, either a dynamic file name can be created as a system variable and supplied to /gof switch as parameter, or /nuuid switch is not used. Please refer to the end of this section on a sample idea for creating unique and dynamic file names.
  - A sample execution of the above command line produced the following files:
    - mwrec5-batch3_85cfeb9e-65cb-44dd-8be5-e406f5b9ef3f.xml
    - mwrec5-batch3_85cfeb9e-65cb-44dd-8be5-e406f5b9ef3f_20210301-150645_LD.xml
    - mwrec5-batch3_85cfeb9e-65cb-44dd-8be5-e406f5b9ef3f_Disk0_50026B723202E09E_50026B723202E09E_20210301-150646_log.xml

- mwrec5-batch3_85cfeb9e-65cb-44dd-8be5-e406f5b9ef3f_Disk1_S11DNEAC933755_WWNNA_20210301-150646_log.xml
- mwrec5-batch3_85cfeb9e-65cb-44dd-8be5-e406f5b9ef3f_Disk3_PMAP1234_WWNNA_20210301-150645_log.xml
- mwrec5-batch3_85cfeb9e-65cb-44dd-8be5-e406f5b9ef3f_ead_log.xml
- mwrec5-batch3_85cfeb9e-65cb-44dd-8be5-e406f5b9ef3f_ead_rep.txt

ZeroDataWindows /eadp /me csec /vp 5 /ec 5 /gof id3csec /lfn id3csecmrr25 /rfn myreport /rft xtp /nuuid

- This command line will erase all disks with CSEC method.
- Application will start and display a dialog window asking whether the user wants to supply erasure operator details or not. This dialog window will stay in focus until user input occurs.
- After user input, splash screen will be displayed, and startup steps will be carried out.
- The main erasure window will be displayed after all startup steps end.
- Erasure will start automatically on all disks simultaneously.
- 5% verification will be carried out on third pass of CSEC method.
- Erasure will stop when 5 errors are reached during all write and verification passes.
    - If number of encountered errors is less than 5, the erasure will be reported as successful.
    - If number of encountered errors reaches 5, the erasure will stop and erasure will be reported as failed.
- Combined log file will be named as:
    - id3csecmrr25_log.xml
- As /nuuid is specified and the report file type is specified as XML, text, and PDF, combined report files will be named as:
    - myreport_rep.xml
    - myreport_rep.txt
    - myreport_rep.pdf
    - Please note that, if the file name specified in /GOF is static, /nuuid switch is applied and all files are created in the same folder, each erasure run will create combined files with the same names. In this case, new files will be written over old files and all combined files except the most recent on will be lost. As a solution, either a dynamic file name can be created as a system variable and supplied to /gof switch as parameter, or /nuuid switch is not used. Please refer to the end of this section on a sample idea for creating unique and dynamic file names.
    - A sample execution of the above command line produced the following files:
        - id3csecmrr25_4cb4c5e4-39b2-43f2-8270-ceba3ea0e78b.xml
        - id3csecmrr25_4cb4c5e4-39b2-43f2-8270-ceba3ea0e78b_Disk0_50026B723202E09E_50026B723202E09E_20210301-150830_log.xml
        - id3csecmrr25_4cb4c5e4-39b2-43f2-8270-ceba3ea0e78b_Disk1_S11DNEAC933755_WWNNA_20210301-150830_log.xml
        - id3csecmrr25_4cb4c5e4-39b2-43f2-8270-ceba3ea0e78b_Disk3_PMAP1234_WWNNA_20210301-150829_log.xml
        - id3csecmrr25_log.xml
        - id3csec_LD.xml
        - myreport_rep.pdf
        - myreport_rep.txt
        - myreport_rep.xml

ZeroDataWindows /eadp /me csec /vp 5 /ec 5 /gof id3csec /lfn id3csecmrr25 /rfn myreport /rft xtp /nuuid /gder

- Notice that this command line is the same command line as previous sample command line, but it has additional /gder command switch.
- This command line will erase all disks with CSEC method.
- Application will start and display a dialog window asking whether the user wants to supply erasure operator details or not. This dialog window will stay in focus until user input occurs.
- After user input, splash screen will be displayed, and startup steps will be carried out.
- The main erasure window will be displayed after all startup steps end.
- Erasure will start automatically on all disks simultaneously.
- 5% verification will be carried out on third pass of CSEC method.
- Erasure will stop when 5 errors are reached during all write and verification passes.
    - If number of encountered errors is less than 5, the erasure will be reported as successful.
    - If number of encountered errors reaches 5, the erasure will stop and erasure will be reported as failed.
- Combined log file will be named as:
    - id3csecmrr25_log.xml and combined log files for single disks will be named as id3csecmrr25_0_log.xml and id3csecmrr25_1_log.xml .
- As /nuuid is specified and the report file type is specified as XML, text, and PDF, combined report files will be named as:
    - Combined XML report file for all disks will be named as myreport_rep.xml and combined XML report files for single disks will be named as id3csecmrr25_0_rep.xml and id3csecmrr25_1_rep.xml .
    - Combined text report file for all disks will be named as myreport_rep.txt and combined text report files for single disks will be named as id3csecmrr25_0_rep.txt and id3csecmrr25_1_txt.xml .
    - Combined PDF report file for all disks will be named as myreport_rep.pdf and combined PDF report files for single disks will be named as id3csecmrr25_0_pdf.xml and id3csecmrr25_1_pdf.xml .
    - Please note that, if the file name specified in /GOF is static, /nuuid switch is applied and all files are created in the same folder, each erasure run will create combined files with the same names. In this case, new files will be written over old files and all combined files except the most recent on will be lost. As a solution, either a dynamic file name can be created as a system variable and supplied to /gof switch as parameter, or /nuuid switch is not used. Please refer to the end of this section on a sample idea for creating unique and dynamic file names.
    - A sample execution of the above command line produced the following files:
        - id3csecmrr25_0_log.xml
        - id3csecmrr25_0_rep.pdf
        - id3csecmrr25_0_rep.txt
        - id3csecmrr25_0_rep.xml
        - id3csecmrr25_1_log.xml
        - id3csecmrr25_1_rep.pdf
        - id3csecmrr25_1_rep.txt
        - id3csecmrr25_1_rep.xml
        - id3csecmrr25_7332af1a-824f-426f-a085-76224dd28c67.xml
        - id3csecmrr25_7332af1a-824f-426f-a085-76224dd28c67_Disk0_50026B723202E09E_50026B723202E09E_20210301-192140_log.xml
        - id3csecmrr25_7332af1a-824f-426f-a085-76224dd28c67_Disk1_S11DNEAC933755_WWNNA_20210301-192140_log.xml

- id3csecmrr25_7332af1a-824f-426f-a085-76224dd28c67_Disk3_PMAP1234_WWNNA_20210301-192140_log.xml
- id3csecmrr25_log.xml
- id3csec_LD.xml
- myreport_rep.pdf
- myreport_rep.txt
- myreport_rep.xml

ZeroDataWindows /eadp /me nist800-88Purge /gof nistpurge /rft xp /ec 1 /dni /asd /nc AcceptTheRisk

- This command line will erase all disks with NIST800-88Purge method in parallel.
- 10% verification will be carried out on verification passes as defined in NIST800-88Purge method.
- No data entry will be required as /nc AcceptTheRisk parameter is supplied.
- As /dni switch is specified, no user interaction will be possible on application window. This also means, there is no way to interrupt or stop the erasure once it begins.
- As /asd switch is specified, erasure will stop when all passes are executed, and ZeroData Windows will be shut down automatically.
- Erasure will stop on any disk if error count of 1 is reached and the disk will be reported as failed. If no /EC parameter were specified, then a faulty disk could derail erasure process and the user would not have any control over erasure duration – a very bad disk could lock up the computer and other disks for hours, even for days.
- Combined log file will be named as:
  - nistpurge_log.xml
- As the report file type is specified as XML and PDF, combined report files will be named as:
  - nistpurge_[GUID]_ead_rep.xml
  - nistpurge_[GUID]_ead_rep.pdf
  - Please note that, if the file name specified in /GOF is static, /nuuid switch is applied and all files are created in the same folder, each erasure run will create combined files with the same names. In this case, new files will be written over old files and all combined files except the most recent on will be lost. As a solution, either a dynamic file name can be created as a system variable and supplied to /gof switch as parameter, or /nuuid switch is not used. Please refer to the end of this section on a sample idea for creating unique and dynamic file names.
  - A sample execution of the above command line produced the following files:
    - nistpurge_b5db4d56-5628-42fa-8ca5-ab597463a320.xml
    - nistpurge_b5db4d56-5628-42fa-8ca5-ab597463a320_20210301-151109_LD.xml
    - nistpurge_b5db4d56-5628-42fa-8ca5-ab597463a320_Disk0_50026B723202E09E_50026B723202E09E_20210301-151109_log.xml
    - nistpurge_b5db4d56-5628-42fa-8ca5-ab597463a320_Disk1_S11DNEAC933755_WWNNA_20210301-151109_log.xml
    - nistpurge_b5db4d56-5628-42fa-8ca5-ab597463a320_Disk3_PMAP1234_WWNNA_20210301-151109_log.xml
    - nistpurge_b5db4d56-5628-42fa-8ca5-ab597463a320_ead_log.xml
    - nistpurge_b5db4d56-5628-42fa-8ca5-ab597463a320_ead_rep.pdf
    - nistpurge_b5db4d56-5628-42fa-8ca5-ab597463a320_ead_rep.xml

ZeroDataWindows /eadp /me personal /ssd /me ssdrandom4 /ze 1 /hdd /me usdod /gof nistpurge /vp 1 /ec 1 /dni /asd /nc AcceptTheRisk /nuuid

- This command line will erase all disks with Personal method as /me Personal is specified.
- However, as there is a "/ssd /me /ze" block is present, for disks identified as SSD, SSDRandom4 method will be applied first and one extra zero pass will be applied after SSDRandom4 method ends. A total of 4 random passes and one zero pass will be applied to SSD disks.
- As there is a "/hdd /me" block is present, for disks identified as HDD for disks identified as HDD, US DoD method will be applied, and no extra passes will be applied afterwards.
- The Personal method will be applied all disks that are neither HDD nor SSD, for example, removable disks like USB disks will be erased using Personal method.
- Notice that in this case the file name supplied with /gof parameter is not relevant to erasure methods that are applied to disks, furthermore this name creates unnecessary confusion. In practice, better and relevant file names must be specified.
- No data entry will be required as /nc AcceptTheRisk parameter is supplied.
- As /dni switch is specified, no user interaction will be possible on application window. This also means, there is no way to interrupt or stop the erasure once it begins.
- As /asd switch is specified, erasure will stop when all passes are executed, and ZeroData Windows will be shut down automatically.
- 1% verification will be carried out on verification passes whenever applicable. SSDRandom4 method does not have any default erasure pass, therefore no verification will be applied to SSD disks. However, USDoD method has a verification pass after the third and lass pass, therefore 1% verification will be applied to HDD disks.
- Erasure will stop on any disk if error count of 1 is reached and the disk will be reported as failed. If no /EC parameter were specified, then a faulty disk could derail erasure process and the user would not have any control over erasure duration – a very bad disk could lock up the computer and other disks for hours, even for days.
- As /nuuid is specified but no report file type is specified, combined log and report files will be named as:
  - nistpurge_log.xml
  - nistpurge_rep.xml
  - Please note that, if the file name specified in /GOF is static, /nuuid switch is applied and all files are created in the same folder, each erasure run will create combined files with the same names. In this case, new files will be written over old files and all combined files except the most recent on will be lost. As a solution, either a dynamic file name can be created as a system variable and supplied to /gof switch as parameter, or /nuuid switch is not used. Please refer to the end of this section on a sample idea for creating unique and dynamic file names.
  - A sample execution of the above command line produced the following files:
    - nistpurge_bf9a2249-bf94-48dd-bd11-de63d8214121.xml
    - nistpurge_bf9a2249-bf94-48dd-bd11-de63d8214121_Disk0_50026B723202E09E_50026B723202E09E_20210301-151322_log.xml
    - nistpurge_bf9a2249-bf94-48dd-bd11-de63d8214121_Disk1_S11DNEAC933755_WWNNA_20210301-151322_log.xml
    - nistpurge_bf9a2249-bf94-48dd-bd11-de63d8214121_Disk3_PMAP1234_WWNNA_20210301-151322_log.xml
    - nistpurge_LD.xml
    - nistpurge_log.xml
    - nistpurge_rep.xml

ZeroDataWindows /eadp /me professional /nl 2 /ssd /me ssdrandom4 /ze 1 /hdd /me usdod /nl 1 /rd 2 /gof better_file_name /vp 1 /ec 1 /dni /asd /nc AcceptTheRisk /nuuid

- Notice that this command line is the same command line as previous sample command line, however the file name specified in /gof command switch does not create any unnecessary confusion.
- This command line will erase all disks with Professional method and apply two extra non-linear passes on top of it.
- However, as there is a "/ssd /me /ze" block is present, for disks identified as SSD, SSDRandom4 method and one extra zero pass will be applied.
- However, as there is a "/hdd /me / nl /rd" block is present, for disks identified as HDD, US DoD method, one extra non-linear pass and two extra random passes will be applied.
- No data entry will be required as /nc AcceptTheRisk parameter is supplied.
- As /dni switch is specified, no user interaction will be possible on application window. This also means, there is no way to interrupt or stop the erasure once it begins.
- As /asd switch is specified, erasure will stop when all passes are executed, and ZeroData Windows will be shut down automatically.
- 1% verification will be carried out on verification passes whenever applicable. Professional and SSDRandom4 methods do not have any default erasure passes, therefore no verification will be applied to SSD disks or other disk types except HDD. USDoD method has a verification pass after the third and lass pass, therefore 1% verification will be applied to HDD disks.
- Erasure will stop on any disk if error count of 1 is reached and the disk will be reported as failed. If no /EC parameter were specified, then a faulty disk could derail erasure process and the user would not have any control over erasure duration – a very bad disk could lock up the computer and other disks for hours, even for days.
- As /nuuid is specified but no report file type is specified, combined log and report files will be named as:
    - better_file_name_log.xml
    - better_file_name_rep.xml
    - Please note that, if the file name specified in /GOF is static, /nuuid switch is applied and all files are created in the same folder, each erasure run will create combined files with the same names. In this case, new files will be written over old files and all combined files except the most recent on will be lost. As a solution, either a dynamic file name can be created as a system variable and supplied to /gof switch as parameter, or /nuuid switch is not used. Please refer to the end of this section on a sample idea for creating unique and dynamic file names.
    - A sample execution of the above command line produced the following files:
        - better_file_name_a4056817-b51c-4bae-8165-35087210d38a.xml
        - better_file_name_a4056817-b51c-4bae-8165-35087210d38a_Disk0_50026B723202E09E_50026B723202E09E_20210301-151527_log.xml
        - better_file_name_a4056817-b51c-4bae-8165-35087210d38a_Disk1_S11DNEAC933755_WWNNA_20210301-151527_log.xml
        - better_file_name_a4056817-b51c-4bae-8165-35087210d38a_Disk3_PMAP1234_WWNNA_20210301-151526_log.xml
        - better_file_name_LD.xml
        - better_file_name_log.xml
        - better_file_name_rep.xml

zerodatawindows.exe /eadp /xrd /me nist800-88purge /tff /dndc /ofp "Y:\ZDW_Logs" /gof nist-gder /nuuid /rft xp /wfp /ec 1 /mwr 5.5 /mrr 10 /dhar /nc AcceptTheRisk /dni /asd /edl /lds 1 /gder

- This command line will erase all disks in parallel with nist800-88purge method. A default 10% verification will be applied to all disks as specified in NIST 800-88 Rev. 1 Purge method specification.
- As /xrd switch is present, removable drives will be excluded from erasure and their presence will not be reported in logs and reports.
- As /tff switch is present, for disks that report they have firmware erasure commands, these firmware commands will be tried out before actual erasure to check whether they work or not. If this check passes, NIST verification steps are applied and firmware command is applied; if this check fails, then erasure immediately falls back to 1 pass zero overwrite pass, reducing erasure duration.
- Log and report files will be created in Y:\ZDW_Logs folder. In case this folder is a network folder, a reliable network connection is required, otherwise file write errors might occur and output files might be unusable.
- As /wfp is specified, a bootable fingerprint report will be written to the first sectors of each disk.
- Erasure will stop on any disk if error count of 1 is reached and the disk will be reported as failed. If no /EC parameter were specified, then a faulty disk could derail erasure process and the user would not have any control over erasure duration – a very bad disk could lock up the computer and other disks for hours, even for days.
- As /mwr 5.5 is specified and /ec is 1, if disk write speeds go below 5.5 MB/s for a disk, erasure will stop, and the disk will be reported as failed.
- As /mrr 10 is specified and /ec is 1, if disk read speeds go below 10 MB/s for a disk, erasure will stop, and the disk will be reported as failed.
- As /dhar is specified, hidden area removal feature will be disabled and will not be attempted.
- No data entry will be required as /nc AcceptTheRisk parameter is supplied.
- As /dni switch is specified, no user interaction will be possible on application window. This also means, there is no way to interrupt or stop the erasure once it begins.
- As /asd switch is specified, erasure will stop when all passes are executed, and ZeroData Windows will be shut down automatically.
- As /edl switch is specified, debug logs will be created for this erasure run.
- As /lds 1 is specified, contents of first sector of the disk will be dumped into the logs and reports for each erased disk.
- As /gder is specified, combined logs and combined reports will be created for each individual disk.
- As /nuuid is specified and report file types are specified as XML and PDF, combined log and report files for all disks will be named as:
  - nist-gder_log.xml
  - nist-gder_rep.xml
  - nist-gder_rep.pdf
  - Please note that, if the file name specified in /GOF is static, /nuuid switch is applied and all files are created in the same folder, each erasure run will create combined files with the same names. In this case, new files will be written over old files and all combined files except the most recent on will be lost. As a solution, either a dynamic file name can be created as a system variable and supplied to /gof switch as parameter, or /nuuid switch is not used. Please refer to the end of this section on a sample idea for creating unique and dynamic file names.
  - A sample execution of the above command line produced the following files:
    - Disk1_EDOpLog.txt
    - Disk3_EDOpLog.txt

- EDHxaLog.xml
- EDOpLog.txt
- nist-gder_0_log.xml
- nist-gder_0_rep.pdf
- nist-gder_0_rep.xml
- nist-gder_1_log.xml
- nist-gder_1_rep.pdf
- nist-gder_1_rep.xml
- nist-gder_b6cdb110-7119-4e79-a9f3-3425dfe05112.xml
- nist-gder_b6cdb110-7119-4e79-a9f3-3425dfe05112_Disk0_50026B723202E09E_50026B723202E09E_20210301-153234_log.xml
- nist-gder_b6cdb110-7119-4e79-a9f3-3425dfe05112_Disk1_S11DNEAC933755_WWNNA_20210301-153234_log.xml
- nist-gder_LD.xml
- nist-gder_log.xml
- nist-gder_rep.pdf
- nist-gder_rep.xml

zerodatawindows.exe /EADP /XRD /ME NIST800-88Purge /NC AcceptTheRisk /DNI /ASD /ofp "Y:\ZDW" /gof "CompanyX-Order27" /UTF /RFT XP /EC 50 /PHFBE 80 /PHFAE 80 /FBDSB 10 /FBDSA 10 /FWDSB 5 /FWDSA 5 /PV Last /VP 1 /EDL /DART 120 /DARC 3 /EON "Johnny Appleseed" /ESN "Jason White" /ASI

- This command line will erase all disks in parallel with nist800-88purge method. A default 10% verification will be applied to all disks as specified in NIST 800-88 Rev. 1 Purge method specification.
- As /xrd switch is present, removable drives will be excluded from erasure and their presence will not be reported in logs and reports.
- No data entry will be required as /nc AcceptTheRisk parameter is supplied.
- As /dni switch is specified, no user interaction will be possible on application window. This also means, there is no way to interrupt or stop the erasure once it begins.
- As /asd switch is specified, erasure will stop when all passes are executed, and ZeroData Windows will be shut down automatically.
- Log and report files will be created in Y:\ZDW folder. In case this folder is a network folder, a reliable network connection is required, otherwise file write errors might occur and output files might become unusable.
- As /utf switch is specified, the files will be created in a temporary folder under the folder where zerodatawindows.exe is located, and files will be transferred to Y:\ZDW folder after all file processing is done.
- Erasure will stop on any disk if error count of 50 is reached and the disk will be reported as failed. If no /EC parameter were specified, then a faulty disk could derail erasure process and the user would not have any control over erasure duration – a very bad disk could lock up the computer and other disks for hours, even for days.
- As /phfbe 80 is specified, any disk that has a health score of 80% and less will be reported as failed before erasure and these disks will not be erased.
- As /phfae 80 is specified, any disk that has a health score of 80% and less after erasure will be reported as failed after erasure completes.
- As /fbdsb 10 is specified, any disk that has 10 or more bad sectors before erasure will be reported as failed before erasure and these disks will not be erased.

- As /fbdsa 10 is specified, any disk that has 10 or more bad sectors after erasure will be reported as failed after erasure completes.
- As /fwdsb 5 is specified, any disk that has 5 or more weak sectors before erasure will be reported as failed before erasure and these disks will not be erased.
- As /fwdsa 5 is specified, any disk that has 5 or more bad sectors after erasure will be reported as failed after erasure completes.
- As /PV Last and /VP 1 are specified, verification should be carried out after the last erasure pass and 1% of the disk should be verified. However, NIST 800-88 Rev.1 Purge and Clear methods have a default 10% verification and this verification percentage and how and when it is carried out cannot be changed.
- As /edl switch is specified, debug logs will be created for this erasure run.
- As /dart 120 is specified, a disk access attempt will time out after 120 seconds and will be attempted again.
- As /darc 3 is specified, in case of disk access timeouts three attempts will be made before failing the attempt and logging an error.
- As /eon “Johnny Appleseed” is specified, erasure operator name will be recorded as Johnny Appleseed in logs and reports.
- As /esn “Jason White” is specified, erasure supervisor name will be recorded as Jason White in logs and reports.
- As /asi is specified, if there is a folder named Signature where zerodatawindows.exe resides and if there are two png files named Operator.png and Supervisor.png in that folder, then Operator.png will be output to the PDF report as signature of erasure operator and Supervisor.png will be output to the PDF reports as signature of erasure supervisor.
- No /nuuid switch is specified and report file types are specified as XML and PDF.
    - A sample execution of the above command line produced the following files:
        - CompanyX-Order27_3e344639-e18a-45cd-82d9-e232bef67c21.xml
        - CompanyX-Order27_3e344639-e18a-45cd-82d9-e232bef67c21_20210301-152218_LD.xml
        - CompanyX-Order27_3e344639-e18a-45cd-82d9-e232bef67c21_Disk0_50026B723202E09E_50026B723202E09E_20210301-152220_log.xml
        - CompanyX-Order27_3e344639-e18a-45cd-82d9-e232bef67c21_Disk1_S11DNEAC933755_WWNNA_20210301-152220_log.xml
        - CompanyX-Order27_3e344639-e18a-45cd-82d9-e232bef67c21_ead_log.xml
        - CompanyX-Order27_3e344639-e18a-45cd-82d9-e232bef67c21_ead_rep.pdf
        - CompanyX-Order27_3e344639-e18a-45cd-82d9-e232bef67c21_ead_rep.xml
        - Disk0_EDOpLog.txt
        - Disk1_EDOpLog.txt
        - Disk3_EDOpLog.txt
        - EDHxaLog.xml
        - EDOpLog.txt

zerodatawindows.exe /EADP /XRD /ME NIST800-88Purge /NC AcceptTheRisk /DNI /ASD /ofp "Y:\ZDW" /gof "CompanyX-Order27" /UTF /RFT XP /EC 50 /PHFBE 80 /PHFAE 80 /FBDSB 10 /FBDSA 10 /FWDSB 5 /FWDSA 5 /PV Last /VP 1 /EDL /DART 120 /DARC 3 /EON “Johnny Appleseed” /ESN “Jason White” /ASI /GDER

- Notice that this command line is the same command line as previous sample command line, but it has additional /gder command switch.
- This command line will erase all disks in parallel with nist800-88purge method. A default 10% verification will be applied to all disks as specified in NIST 800-88 Rev. 1 Purge method specification.

- As /xrd switch is present, removable drives will be excluded from erasure and their presence will not be reported in logs and reports.
- No data entry will be required as /nc AcceptTheRisk parameter is supplied.
- As /dni switch is specified, no user interaction will be possible on application window. This also means, there is no way to interrupt or stop the erasure once it begins.
- As /asd switch is specified, erasure will stop when all passes are executed, and ZeroData Windows will be shut down automatically.
- Log and report files will be created in Y:\ZDW folder. In case this folder is a network folder, a reliable network connection is required, otherwise file write errors might occur and output files might become unusable.
- As /utf switch is specified, the files will be created in a temporary folder under the folder where zerodatawindows.exe is located, and files will be transferred to Y:\ZDW folder after all file processing is done.
- Erasure will stop on any disk if error count of 50 is reached and the disk will be reported as failed. If no /EC parameter were specified, then a faulty disk could derail erasure process and the user would not have any control over erasure duration – a very bad disk could lock up the computer and other disks for hours, even for days.
- As /phfbe 80 is specified, any disk that has a health score of 80% and less will be reported as failed before erasure and these disks will not be erased.
- As /phfae 80 is specified, any disk that has a health score of 80% and less after erasure will be reported as failed after erasure completes.
- As /fbdsb 10 is specified, any disk that has 10 or more bad sectors before erasure will be reported as failed before erasure and these disks will not be erased.
- As /fbdsa 10 is specified, any disk that has 10 or more bad sectors after erasure will be reported as failed after erasure completes.
- As /fwdsb 5 is specified, any disk that has 5 or more weak sectors before erasure will be reported as failed before erasure and these disks will not be erased.
- As /fwdsa 5 is specified, any disk that has 5 or more bad sectors after erasure will be reported as failed after erasure completes.
- As /PV Last and /VP 1 are specified, verification should be carried out after the last erasure pass and 1% of the disk should be verified. However, NIST 800-88 Rev.1 Purge and Clear methods have a default 10% verification and this verification percentage and how and when it is carried out cannot be changed.
- As /edl switch is specified, debug logs will be created for this erasure run.
- As /dart 120 is specified, a disk access attempt will time out after 120 seconds and will be attempted again.
- As /darc 3 is specified, in case of disk access timeouts three attempts will be made before failing the attempt and logging an error.
- As /eon “Johnny Appleseed” is specified, erasure operator name will be recorded as Johnny Appleseed in logs and reports.
- As /esn “Jason White” is specified, erasure supervisor name will be recorded as Jason White in logs and reports.
- As /asi is specified, if there is a folder named Signature where zerodatawindows.exe resides and if there are two png files named Operator.png and Supervisor.png in that folder, then Operator.png will be output to the PDF report as signature of erasure operator and Supervisor.png will be output to the PDF reports as signature of erasure supervisor.
- No /nuuid switch is specified and report file types are specified as XML and PDF.
    - A sample execution of the above command line produced the following files:
        - CompanyX-Order27_cbd74bd8-fc7f-4ba4-9b58-965097a99cb5.xml
        - CompanyX-Order27_cbd74bd8-fc7f-4ba4-9b58-965097a99cb5_20210301-155416_LD.xml

- CompanyX-Order27_cbd74bd8-fc7f-4ba4-9b58-965097a99cb5_Disk0_50026B723202E09E_50026B723202E09E_20210301-155418_ead_log.xml
- CompanyX-Order27_cbd74bd8-fc7f-4ba4-9b58-965097a99cb5_Disk0_50026B723202E09E_50026B723202E09E_20210301-155418_ead_rep.pdf
- CompanyX-Order27_cbd74bd8-fc7f-4ba4-9b58-965097a99cb5_Disk0_50026B723202E09E_50026B723202E09E_20210301-155418_ead_rep.xml
- CompanyX-Order27_cbd74bd8-fc7f-4ba4-9b58-965097a99cb5_Disk0_50026B723202E09E_50026B723202E09E_20210301-155418_log.xml
- CompanyX-Order27_cbd74bd8-fc7f-4ba4-9b58-965097a99cb5_Disk1_S11DNEAC933755_WWNNA_20210301-155418_ead_log.xml
- CompanyX-Order27_cbd74bd8-fc7f-4ba4-9b58-965097a99cb5_Disk1_S11DNEAC933755_WWNNA_20210301-155418_ead_rep.pdf
- CompanyX-Order27_cbd74bd8-fc7f-4ba4-9b58-965097a99cb5_Disk1_S11DNEAC933755_WWNNA_20210301-155418_ead_rep.xml
- CompanyX-Order27_cbd74bd8-fc7f-4ba4-9b58-965097a99cb5_Disk1_S11DNEAC933755_WWNNA_20210301-155418_log.xml
- CompanyX-Order27_cbd74bd8-fc7f-4ba4-9b58-965097a99cb5_ead_log.xml
- CompanyX-Order27_cbd74bd8-fc7f-4ba4-9b58-965097a99cb5_ead_rep.pdf
- CompanyX-Order27_cbd74bd8-fc7f-4ba4-9b58-965097a99cb5_ead_rep.xml
- Disk0_EDOpLog.txt
- Disk1_EDOpLog.txt
- Disk3_EDOpLog.txt
- EDHxaLog.xml
- EDOpLog.txt

Using Dynamic File Names for Unique Output Naming in Command Line Usage

Let us go back a bit in this manual and remember which pieces of information is contained in default ZeroData Windows file names:

Default File Name

When ZeroData Windows is executed without specifying a file name,

- a default file name in the form of “date-time + erasure UUID” are used for files,
- however, a default file name in the form of “date-time + erasure UUID + Disk ID + Disk Serial Number + Disk World Wide Number + Date + Time” are assigned automatically to log files,
- notice that date-time occurs at the start of the file name and date + time occurs at the end of file name. The second date + time information is added to distinguish files in cases where a disk is erased multiple times in the same erasure session – which is possible when ZeroData Windows is used to erase disks manually from the user interface,
- If file type is not explicitly specified with /RFT option, then default file type of XML will be applied to all files,

- Report files will be added “_rep”, log files will be added “_log” to their ends.

/GOF < Global Output File Name > *e.g., /GOF GOFile*

This option sets the name for log and report files, extensions for file types like TXT and XML are attached automatically. The file name string can be up to 128 characters. If surrounding “ and “ characters are used, then surrounding “ and “ characters around the file name string will use up 2 characters from the allowed 128 characters.

If this option is specified,

- a default file name in the form of “global output file name + erasure UUID” are used for files,
- the log files name will be in the form of “global output file name + erasure UUID + Disk ID + Disk Serial Number + Disk World Wide Number + Date + Time”,
- If file type is not explicitly specified with /RFT option, then default file type of XML will be applied to all files,
- Report files will be added “_rep”, log files will be added “_log” to their ends.

As you can see from above information, ZeroData Windows file naming convention:

- Groups all files produced in an erasure run together as all files begin with
  - the same global file name (if specified), like “ACMEInc”,
  - and the same ZeroData Windows erasure GUID ID, like “131841_255301e2-e33b-4188-9bf3-9ac16498ecaa”
- And each erased disk is uniquely identified by:
  - the Disk ID, like Disk3
  - serial number of the disk, like “WD-WCC3F1FR4R44”,
  - World Wide Number of the disk, like “50014EE2618DBCDC”,
  - date-time string, like “20210221-151251”.
- For the above example, for each disk a unique log file is created with a name like:
  - ACMEInc _0cfe5e12-76ff-41c4-bb9b-3c8f5966dd37_Disk3_WD-WCC3F1FR4R44_50014EE2618DBCDC_20210221-151251_ead_log.xml
- And for each erasure, combined log and report files are created with names like:
  - ACMEInc _0cfe5e12-76ff-41c4-bb9b-3c8f5966dd37_ead_log.xml
  - ACMEInc _0cfe5e12-76ff-41c4-bb9b-3c8f5966dd37_ead_rep.xml
  - ACMEInc _0cfe5e12-76ff-41c4-bb9b-3c8f5966dd37_ead_rep.txt
  - ACMEInc _0cfe5e12-76ff-41c4-bb9b-3c8f5966dd37_ead_rep.pdf

Therefore, default ZeroData Windows naming structure should meet your needs to group and uniquely identify files containing erasure results. If further automatic processing regarding these output files or information contained in them, it is possible to write a parser script to identify correct file and/or files.

However, in some cases you might find dealing with default file names too complicated or you may not be ready to change your existing command scripts that expect a specific file name convention. In these cases, the /NUUID command switch becomes useful.

Let us remember what /NUUID does:

/NUUID < No Default Values Added To Combined Log and Report Filenames > e*.g., /NUUID*

As ZeroData Windows file names are unique, it is not possible to have an exact file name. In cases where an exact file name is required for combined log and report file names – for example, for the sake of processing logs and reports in scripts that expect a static file name or a file name with a different naming convention - this option can be used.

Important : Windows operating system does not allow multiple files with the same name to be located under a folder, and a new file with the same name will be written over the old file already present in the folder. Therefore, using exact file names without any timestamps or UUID values is not a good idea if the user wants to store all output files in a single folder and batch process them to create reports later. Therefore /NUUID must be used be very carefully.

As using this command switch will strip UUID portion of combined log and report files, only the file name supplied with /GOF command switch will be used to name combined log and report files – meaning it is up to you to supply a unique file name that matches your processing needs as parameter for /GOF switch.

How can this be done ?

Windows operating system offers lots of information within WMI interface and at least two different scripting environments: the old DOS-style command prompt scripting and the newer PowerShell scripting. Both environments support retrieving information from WMI interface and creation of system variables and using them in scripts.

As a sample idea expressed using an illustrative pseudocode notation, let us assume we have the following system variables:

- $SYSTEMSERIAL, which contains the serial number of the system,
- $DATETIME, which contains current system date and time.

Then we can concatenate these variables to create a unique global variable called $GOFILE as follows:

$GOFILE = $SYSTEMSERIAL+"_"+ $DATETIME

Then all we need to do is to supply this $GOFILE system variable as the parameter of /GOF switch in your preferred scripting language.

Let us implement the above pseudocode in a command file.

Step 1: Create a variable called %serial% containing the serial number.

```
rem
rem   get system serial number into variable named serial using what WMI interface provides.
rem
        @echo off
        set torun=wmic bios get serialnumber /format:value
        for /f "tokens=2 delims==" %%a in ('%torun%') do set %serial%=%%a
rem
rem now the variable serial contains system serial number.
rem
```

Step 2: Get the date and time in a usable format, creating a datetime variable called %_date% with a value like 20210226092045 using what WMI interface provides.

```
rem
rem   creating a date-time variable called %_date% with a value like 20210226092045.
rem

        @echo off
        setlocal
        rem
        rem use findstr to strip blank lines from wmic output
        rem
                for /f "usebackq skip=1 tokens=1-6" %%g in (`wmic Path Win32_LocalTime Get
                Day^,Hour^,Minute^,Month^,Second^,Year ^| findstr /r /v "^$"`) do (
                 set _day=00%%g
                 set _hours=00%%h
                 set _minutes=00%%i
                 set _month=00%%j
                 set _seconds=00%%k
                 set _year=%%l
                 )
        rem
        rem pad retrieved values with leading zeros if retrieved values have single digit.
        rem
                set _month=%_month:~-2%
                set _day=%_day:~-2%
                set _hh=%_hours:~-2%
                set _mm=%_minutes:~-2%
                set _ss=%_seconds:~-2%
                set _date=%_year%%_month%%_day%%_hh%%_mm%%_ss%
                echo %_date%
        endlocal
 rem
rem   Now %_date% contains a date-time value like 20210226092045.
rem
```

Step 3: Combine these serial and %_date% to form a unique file name for our ZeroData Windows disk erasure.

```
rem
rem   creating a unique file name variable called %uniqnam1% to uniquely identify a ZeroData Windows erasure
rem   with a value that has serial number first and date-time value coming after that
rem
        set %uniqnam1%= %serial%%_date%
```

```
rem
rem   creating a unique file name variable called %uniqnam2% to uniquely identify a ZeroData Windows erasure
rem   with a value that has date-time  first and serial number value coming after that
rem
            set %uniqnam2%= %_date%%serial%
```

Let us implement the above pseudocode in PowerShell.

Step 1: Create a variable called $SystemSerialNumber containing the serial number.

```
$SystemSerialNumber=(Get-WmiObject -classname win32_bios).SerialNumber
```

Step 2: Create a variable called $FileDateTime containing the serial number.

```
$FileDateTime=(Get-Date).tostring("yyyyMMddHHmm")
```

Step 3: Combine these $SystemSerialNumber and $FileDateTime to form a unique file name for our ZeroData Windows disk erasure.

```
$UniqueFileName1=$SystemSerialNumber+$FileDateTime

$UniqueFileName2 =$FileDateTime+$SystemSerialNumber
```

Let us implement how we can pick up files we need in PowerShell.

Let us assume we have a variable named $files in the following form :

```
$files=$SystemSerialNumber+"_"+$MACADDRESS+"_"+$FileDateTime
```

Let us assume we look for the file named:

- the file resides in a folder path stored in the variable named $logdir
- “x:\logs\123_33-33-33-33-33-33_20210301.xml”,
- or “x:\logs\123_33-33-33-33-33-33_20210301_{wwn}_ead_.xml”,
- but not for a file named “x:\logs\123_33-33-33-33-33-33_20210301disk1232311231_log.xml”

Then the following code snippet would allow us to select the correct file for us:

```
$xml= New-Object System.Xml.XmlDocument

$xmlfile=$logdir+$files+"_log.xml"

if (!(Test-Path $xmlfile))

        {

        $xmlfile=Get-childitem -path ($logdir+"\*_ead_log.xml") | Where-Object { $_.FullName -match $files }

        }
```

Appendices

Appendix A - Secure Data Erasure on Solid State Disks

Solid state disks (SSD) based on flash chips operate differently than hard disks based on magnetic plates.

There are multiple aspects where they differ, but four points are more relevant than others for secure data erase operation.

• Point 1: solid state drives have endurance limits that links them to the "Total Bytes Written" (TBW) to them.

There is a misconception that overwrite operations reduce SSD life which dates to early days of SSD technology and the first disks employing NAND chips. For SSD's that were manufactured in last 3 years and later, this misconception is largely unfounded. An SSD does not stop working when its stated TBW value is reached, rather its warranty runs out, but the drive can still be used.

Manufacturers state different TBW values for different models and sizes depending on the technology used. In general, SSD's with low prices tend to have a lower TBW rating. For current SSD drives on the market, the lowest TBW value corresponds to at least 100 times of its capacity and the maximum TBW corresponds to around 6000 times of disk capacity for special datacenter SSD's designed for write oriented workloads.

Some trial runs on a limited number of consumer SSD's on both low- and high-quality SSD's have found out that even the lowest quality SSD was able to exceed its stated TBW limits by a factor of 10.

However, there are some rare and special SSD models, mostly by Intel, that enter a read-only state when their TBW value is reached – Intel claims this "assert mode" is a feature "to prevent enterprise data loss". If the erased disk has this feature and this value is reached during secure erasure, no data can be overwritten as disk enters read-only state and erasure operation will fail.

If the SSD drive supplies "Total Host Writes" data, ZeroData Windows outputs this data before erasing the disk. After the erasure, ZeroData Windows outputs this data supplied by disk again.

To prevent possible problems, please consult your SSD specification for TBW values before deploying the SSD back into use.

• Point 2: accessing and erasing all areas of SSD drives is more complicated than magnetic hard disks.

Applying firmware commands between erasure passes seems to leave some data behind, so our SSD optimized methods involve a series of random data stream overwriting rounds without any firmware commands between them.

Research suggests that a two pass random data stream to be enough to erase all prior data on SSD drives. Eurosoft SSD Optimized Data Erasure Methods consist of 2, 4 and 6 rounds of overwrite with random data stream.

• Point 3: SSD's have varying levels of sustained write performance profiles.

Most SSD's employ some levels of buffers like RAM, SLC, quasi-SLC areas where write performance is high, but once these buffer sizes are exceeded the disk is limited with the actual speed of flash chips. Almost all SATA SSD disks are advertised with a "up to 5xx MB/s write speed" based on a benchmark run with a limited data size (usually 1 GB), but once the first buffer size is exceeded the speed may decrease to 4xx MB/s, then again decrease to 3xx MB/s and finally settle on 1xx MB/s range.

ZeroData Windows writes data to all available area of the disk, therefore all these buffers are exceeded and write and read operations become bound by the native sustainable speed of flash chips.

Additionally, flash chips become dirtier with each overwriting round and this leads to some write performance decrease with each additional overwrite pass applied (as no TRIM operation is applied between passes and SSD is not given time to recover). On high quality SSD's with high sustained write performance profiles, this performance decrease is almost non-existent; on mid-level disks this performance decrease is observable, but on some low-level disks like "DRAM-less hard disk replacement class SSD's" which are commonly used in OEM devices, the performance decrease may become substantial – some SSDs' settle down at write speeds lower than a magnetic hard disk, some even as low as a USB 2.0 flash disk write speeds.

• Point 4: the use of non-linear passes on SSD's.

Non-linear write passes are ZeroData Windows proprietary way of introducing extra layers of randomness to the data written to disk locations. It is a very effective method against data recovery attempts.

When multiple non-linear passes are applied to SSD's with low sustained write performance profiles, the write speed may become very low.

This may look like a bad thing if erasure duration is taken as measure, but if erasure quality is of concern, then this feature is a good thing. If users want to apply nonlinear passes, then they must be careful to strike a balance between erasure duration and data security.

Appendix B - Special Note on Small Footprint SSD form factors: SATA, PCIe and NVMe Solid State Disks

Our testing has shown that solid state disks employing PCIe and NVMe protocols have much lower raw I/O throughput rates than stated on their specification sheets.

It is a well-known and observed fact that SSD read and write speeds are dependent on “Queue Depth (QD)” and “Number of Threads(T)” which allow an SSD to process multiple requests faster.

Common to disk erasure, ZeroData Windows needs to work outside file system based read and write operations and issues raw I/O commands to overwrite all sectors of a disk. When expressed in above terms, ZeroData Windows workload is a Q1T1 workload, 1 thread working on queue depth of 1.

Some disks - like Samsung SM951 256 GB NVMe SSD - respond differently to file read and write operations when running under an operating system. If the read and write operation is based on Windows File System – meaning the disk must be formatted by Windows and treated like a “Windows Volume”- for example like running a Crystal Disk Benchmark run, read rates can reach 2200 MB/s and write rates can reach 1300 MB/s. However, if the read and write requests are sent as raw I/O operations, write throughput is capped at 400 MB/s, going significantly down below this figure when the NAND cells are dirty.

Comparison testing with commonly available utilities and other “Secure Erase” products, have shown that this situation is not limited to ZeroData Windows. In fact, it is a general problem with other products having worse raw I/O rates than ZeroData Windows on this disk.

On the other hand, the PCIe AHCI version of SM951 256 GB SSD has a write throughput rate above 1100 MB/s on raw I/O operations under same conditions.

Some other disks - like “Lenovo LENSE10512GMSP34MEAT2MA 512 GB NVMe” disk - can push up to 1400 MB/s raw write rates in bursts and on average 1000 MB/s raw write rates under same conditions.

We have observed NVMe disk raw write speeds going as low as 20 MB/s for some generic Asian branded drives under same conditions.

According to our observations **as far as sustained raw write performance is concerned**,

- **if NAND chips are MLC, most NVMe disks have lower performance than SATA SSD disks.**
- **if NAND chips are TLC, almost all NVMe disks have much lower performance than SATA SSD disks, even going below magnetic disk performance.**
- **if NAND chips are QLC, almost all NVMe disks have much lower performance than SATA SSD disks, even going below magnetic disk performance.**

Performance throttling due to heat development is a serious concern for all mSATA and M.2 format SATA, PCIe and NVMe disks. Certain cases have been found where the mSATA and m.2 SATA versions of the same SSD model and same disk size show throttling behavior whereas the standard 2.5” version with the same size does not show throttling.

Hitting thermal throttling limits requires a sustained write for more than 30 - 60 seconds, meaning 15-60 GB of data must be written in a short interval. In client workloads, such extreme cases are very rare and can occur only when large amounts of files are transferred from one small form factor SSD disk to another small form factor SSD disk. However, by definition, secure data erasure is one of these extreme cases where the disk is overwritten multiple times. Consequently, this throttling development will occur when disks are erased using ZeroData Windows.

In addition to raw I/O limitations, these disks tend to perform at a higher write speed until the SSD controller reaches a certain temperature, when that point is crossed performance is scaled back until temperature drops below a level, when that lower limit is reached performance is scaled up again until the thermal limit is reached – and this cycle is repeated until disk writes stop.

As multiple rounds of overwrite passes are employed on almost all methods, even for high performing NVMe disks, the operation times are extended with each new overwrite round due to prolonged heat development. Unless the m.2 disk has a cooling solution, thermal throttling will be observed when these disks are secure erased.

Appendix C - Special Note on Firmware Based Secure Erase Methods

ZeroData Windows employs two different sets of secure data erase methods that issue firmware based secure erase and sanitize commands.

1. NIST 800-88r1 Clear and Purge methods and ISO/IEC 27040:2015 methods are fully compliant with the underlying NIST standards document.
2. Our ATA/SATA, SCSI/SAS, NVMe firmware erasure methods are extensions of mentioned firmware commands with verification passes applied according to NIST 800-88r1 verification rules.

Firmware based methods can be divided into three classes:

- Secure Erase class commands for ATA/SATA, SCSI/SAS and NVMe disks.
- SANITIZE class commands for ATA/SATA, SCSI/SAS disks – currently NVMe SANITIZE implementations are not present.
- TCG Opal class commands for ATA/SATA, SCSI/SAS, NVMe disks.

Issuing these commands is subject to limitations imposed by the operating system, BIOS/UEFI, and supported sleep states by the computer system among other things. These limitations have nothing to do with ZeroData Windows itself.

To illustrate these limitations the following are applicable for SATA disks:

- The disks must be connected to SATA ports of the computer and on the BIOS, these ports must be set to work in AHCI mode, and support for hot plugging must be enabled.
- Full Windows operating system prevents submitting ATA Security and Sanitize class commands to attached disks as a security feature.
- Windows PE supports submitting ATA Security and Sanitize class commands to disks, however does not support Sleep states and therefore is unable to put the system into Sleep state and waking up from Sleep.
- BIOS/UEFI locks any disks that are present at computer boot process: a procedure called Freeze Lock.
- If Freeze Lock is present, no ATA Security and Sanitize class command is executed on specified disk.
- Due to these imposed limitations, any ATA Security or Sanitize command fails on Windows operating system.
- Due to these imposed limitations, any ATA Security command fails on Windows PE operating system unless the disk power is disconnected and reconnected after WinPE boot.
- The only situation for ATA Security commands including Secure Erase is executed:
    - Computer is booted into WinPE.
    - Disks that are to be erased using ATA Secure Erase commands must be:
        - Either connected to the system after WinPE boot is completed,
        - Or the disks must be powered down for 10 seconds by unplugging the power cord of the disks and then plugged back in, a process called “power cycling the disk” in relevant literature.
        - Or the disks must be connected to the system through a hot swap drive cage which makes unplugging and plugging disks very easy compared to the alternatives, and disks must be taken out of the cage and put back in
    - In all other cases, issued ATA Security commands will fail.
- The only situation for ATA SANITIZE commands are executed as
    - Computer is booted into WinPE.
    - In all other cases, issued ATA Security commands will fail.

The other point with issuing ATA Secure Erase, Enhanced Secure Erase, Crypto Scramble, Block Erase and Overwrite commands is the implementation of these commands are manufacturer dependent.

“Manufacturer Dependent” means there is no agreed standard(s) on how long the erasure process will take, how the erase process will report its progress and success status back, what pattern will be contained on the disk after erasure ends, which data structure will contain information on firmware capabilities and so on.

Although ATA/SATA, SCSI/SAS and NVMe disk standards describe standard data structures and commands, the implementation varies from brand to brand, between disk models within a brand, and within the same model it can vary between different disk sizes.

For example, we have observed that in general, ATA Secure Erase returns a disk with all bytes set to 0, however some models write a different pattern. This makes verification of Secure Erase commands very difficult.

We have observed cases where the disk firmware reports conflicting information on its secure erase capabilities. For example, OEM version of SanDisk X400 128 and 256 GB m.2 SSD reports that it supports ATA SANITIZE Block Erase and Overwrite commands, however when these commands are issued, it reports back that these commands are not supported.

As another example, Dell version of Micron 1100 256 GB SSD with firmware revision M0DL003 reports that it supports ATA SANITIZE Block Erase command, however when this command is issued, it hangs at the start of the command execution and stays there for 72 hours or more, without doing anything. However, the same model SSD from Micron itself with firmware revision M0MU031 executes the same command in 6 minutes and 30 seconds without any problems.

Although the disks are supposed to report back progress of firmware command execution in a standard way so that they can be checked and displayed, some disks output “garbage” values that make progress tracking impossible. Example: the above-mentioned Micron 1100 256 GB SSD with firmware version M0MU031 that ends Block Erase command execution in 6 minutes and 30 seconds outputs the following progress values: 9% for the first 20 readings, then 19% for the next 4993 readings and 100% for last reading where erasure stops. On the other hand, Samsung SM841N 128 GB SSD outputs meaningful progress values: starts at 0% for first 5 readings, then it moves up by 1 for next 100 readings, reaches 100% in 100 readings and ends erasure.

As a result of this, if the disk responds with “garbage” values, tracking progress of firmware commands is not possible.

Another factor is the reported Secure Erase duration by disk firmware. Due ATA standard limitations, it is not possible to report a duration less than 2 minutes (this is also the reason why almost all disks report 2 minutes as S.M.A.R.T. Short Self-Test duration), there is no upper limit for this duration.

If the disk is queried for status update before the reported Secure Erase duration, then Secure Erase operation fails, leaving the disk in an unstable or locked state. Therefore, if a disk reports a secure erase duration of 80 minutes, but actual erase ends in 67 minutes there is no safe way to check whether erasure had ended or not. As you can expect, this behaviour also varies depending on the model of the disk. We have seen a case where the SSD reports it supports ATA SANITIZE Block Erase command, accepts the Block Erase command but never returns any information on its progress where it should return; making it impossible to determine if the erasure has ended or not.

To overcome these practical difficulties, ZeroData Windows does not stop at implementing pure firmware methods which just issue firmware disk erasure commands. Instead, these methods are implemented just like NIST 800-88 rev.1 Clear and Purge compliant methods and as extended standalone methods - the firmware commands are sandwiched within verification passes.

NIST 800-88 rev.1 Clear and Purge data sanitization methods have a multi layered structure with different fall-back methods following each other. For example, for SSD's the NIST 800-88 rev.1 Clear method states:

1. Overwrite media by using organizationally approved and tested overwriting technologies/methods/tools. The Clear procedure should consist of at least one pass of writes with a fixed data value, such as all zeros. Multiple passes or more complex values may alternatively be used.

2. Use the ATA Security feature set's SECURITY ERASE UNIT command, if supported. "

ZeroData Windows implements this requirement in the following manner:

1. Issue ATA SECURITY ERASE UNIT command, if it passes, report successful erasure.
2. If ATA SECURITY ERASE UNIT command fails, use overwrite one pass with zeroes.

A similar fall-back method is applied for Purge method:

1. Issue TCG Opal v1.0 / v2.0 command, if it passes, report successful erasure.
2. Issue ATA SANITIZE CRYPTO SCRAMBLE command, if it passes, report successful erasure.
3. Issue ATA SANITIZE BLOCK ERASE command, if it passes, report successful erasure.
4. Issue ATA SANITIZE OVERWRITE command, if it passes, report successful erasure.
5. If all the above steps fail, fall back to NIST 800-88 rev.1 Clear method.

This fall-back methodology allows the disk to be securely erased whether the ATA Security and Sanitize firmware commands are available or not – therefore is a safer way than simply issuing firmware commands.

As far as our testing is concerned, we have encountered very few SATA magnetic hard disks or solid-state disks that do not support ATA Secure Erase command. However, the multi-layer freeze lock mechanism imposed by BIOS/UEFI, Option ROM's, storage controller firmware and driver, disk controller firmware and Windows operating system complicates the issue and makes impossible to execute this command without human interaction.

Due to the factors mentioned above, it is not possible to successfully execute ATA Secure Erase command as part of NIST 800-88 rev.1 method without human interaction as waking up the system from Sleep or power cycling the disks require presence of a human operator. In case completely unattended execution is desired, all supported firmware erasure commands by the disk will be attempted in the fall-back sequence specified by standard documentation, and in the worst case, the overwrite pass specified in the document will be executed on the disk.

TCG Opal and ATA Sanitize commands are supported only on some portion of Self Encrypting Drives (SED) disks, practically meaning NIST 800-88 rev.1 Purge method can be run on only a portion of SED disks. If a disk does not report supporting TCG or ATA Sanitize commands, there is no point of executing NIST 800-88 rev.1 Purge method; however, as it will fall back to other methods, it can be used as a default method if desired.

As can be expected, this is also manufacturer dependent, there are some self-encrypting disks (notably Samsung 850 series SSD's) that internally support self-encryption and comply to TCG Opal standard, but do not implement any ATA Sanitize method, just implementing Secure Erase command. Some new class of magnetic hard disks like Seagate Barracuda Compute series have labels containing a PSID that is part of TCG Opal protocol, but do not have any SED capabilities.

Some research projects have found out that the Secure Erase command is not correctly implemented on a big percentage of disks that were tested in the investigation. In some cases, the implementation was simply not doing anything at all or was not able to erase but reported successful erasure.

ZeroData Windows implements verification passes for methods that require verification as part of the method. For methods that do not have a verification requirement, it is possibly to execute optional verification rounds. As for NIST 800-88 rev.1 Clear and Purge methods, ZeroData Windows has additional safeguarding steps to verify that the disk has really been erased with the applied firmware command.

For most solid-state disks, the Secure Erase duration is less than 2 minutes. On magnetic hard disks, we have seen reported ATA firmware secure erase durations ranging from 52 minutes to 720 minutes.

Appendix D - Understanding Disk Wipe Durations

Secure data erasure or disk wipe operation is a time-consuming activity and the time it takes to wipe a disk fully depends on sustained disk write speed of the disk being processed.

Generally, disk specifications do not include this sustained disk write speeds, rather the maximum speed scored on the benchmark that reports highest number is reported with a clause “up to X MB/s”. These “up to” figures are meaningless in any context other than that specific benchmark and do not translate into real world performance.

ZeroData Windows uses specially tuned disk write operations to achieve maximum sustained write performance. Comparative trial runs with different software using comparable disk write operations show that ZeroData Windows is one of the best performers.

As a guideline, ZeroData Windows sustained disk write throughput is on par with the Sequential Write throughput reported by freely available Crystal Disk Benchmark software when it is run for maximum test size (currently this is 32 GB) at 1 Thread and Queue Depth of 1. This guideline holds true for all SATA hard disks and solid-state disks.

Earlier in this manual, we have discussed the throttling effect for smaller card sized SATA, PCIe and NVMe solid state disks. Our testing shows that ZeroData Windows throughput rate is on par with Crystal Disk Mark Sequential Write rate until throttling starts to affect the disk.

If a quick estimation is needed, executing Crystal Disk Mark with 32 GB size, and observing the sequential write speed will help. Comparing that throughput rate with below given table for a disk with a size of 500,000 MB will allow you to have a close estimate for one disk wipe pass will take to finish. The duration obtained by the table must be multiplied by the number of passes present in the selected erasure method and by the factor of actual disk size relative to 500,000 MB.

The below table contains some “magic sustained write speed” numbers for a 500 GB disk:

- 230 MB/s is the throughput for the fastest magnetic hard disk currently on the market
- 230 MB/s is the throughput for a mid-level TLC consumer / OEM SATA SSD
- 400 MB/s is the throughput for high end MLC consumer / OEM SATA SSD
- 500 MB/s is the throughput for the best prosumer SATA SSD on the market (Samsung 850/860 Pro)
- 700 MB/s is the throughput for most of the 120 GB / 256 GB PCIe / NVMe TLC SSD
- 1000 MB/s is the throughput for most 480/512 GB NVMe MLC SSD
- 1200 MB/s is the throughput for 512 GB Lenovo Opal compliant NVMe SSD
- 1600 MB/s is the advertised throughput for 512 GB / 1 TB Samsung NVMe TLC SSDs
- 2000 MB/s is the advertised throughput for 2 TB Samsung NVMe MLC SSD

Disk Size (MB)	Average Disk Write Speed (MB/s)	Time for one overwrite round (seconds)	Time for one overwrite round (minutes)	Time for one overwrite (hours)
500,000	20	25,000.00	416.67	6.94
500,000	30	16,666.67	277.78	4.63
500,000	40	12,500.00	208.33	3.47
500,000	50	10,000.00	166.67	2.78
500,000	60	8,333.33	138.89	2.31
500,000	70	7,142.86	119.05	1.98
500,000	80	6,250.00	104.17	1.74
500,000	90	5,555.56	92.59	1.54
500,000	100	5,000.00	83.33	1.39
500,000	110	4,545.45	75.76	1.26
500,000	120	4,166.67	69.44	1.16
500,000	130	3,846.15	64.10	1.07
500,000	140	3,571.43	59.52	0.99
500,000	150	3,333.33	55.56	0.93
500,000	160	3,125.00	52.08	0.87
500,000	170	2,941.18	49.02	0.82
500,000	180	2,777.78	46.30	0.77
500,000	190	2,631.58	43.86	0.73
500,000	200	2,500.00	41.67	0.69
500,000	210	2,380.95	39.68	0.66
500,000	220	2,272.73	37.88	0.63
500,000	230	2,173.91	36.23	0.60
500,000	250	2,000.00	33.33	0.56
500,000	280	1,785.71	29.76	0.50
500,000	300	1,666.67	27.78	0.46
500,000	320	1,562.50	26.04	0.43
500,000	340	1,470.59	24.51	0.41
500,000	360	1,388.89	23.15	0.39
500,000	380	1,315.79	21.93	0.37
500,000	400	1,250.00	20.83	0.35
500,000	420	1,190.48	19.84	0.33
500,000	440	1,136.36	18.94	0.32
500,000	460	1,086.96	18.12	0.30
500,000	480	1,041.67	17.36	0.29
500,000	500	1,000.00	16.67	0.28
500,000	520	961.54	16.03	0.27
500,000	540	925.93	15.43	0.26
500,000	600	833.33	13.89	0.23
500,000	700	714.29	11.90	0.20
500,000	800	625.00	10.42	0.17
500,000	900	555.56	9.26	0.15
500,000	1000	500.00	8.33	0.14
500,000	1100	454.55	7.58	0.13
500,000	1200	416.67	6.94	0.12
500,000	1300	384.62	6.41	0.11
500,000	1400	357.14	5.95	0.10
500,000	1500	333.33	5.56	0.09
500,000	1600	312.50	5.21	0.09
500,000	2000	250.00	4.17	0.07

When comparing ZeroData Windows sustained write throughput performance, please check the sequential write performance of the disk to be erased and compare it against the table above.

Running the following command

ZeroDataWindows

before executing any erasure, will produce an XML log that end with "…_ld.xml" , which contains lots of identifying information on all connected disks.

This information includes the ATA Secure Erase and ATA Enhanced Secure Erase durations embedded into disk firmware. These durations will give you an idea on how long an erasure pass should take to complete. Before attempting NIST Clear and Purge methods, please make sure the ATA Secure Erase durations are acceptable for your purposes.

We have seen reported ATA Secure Erase durations from 2 minutes to 1440 minutes (12 hours) . In some cases, regular one pass overwrite like Personal or Professional methods were faster than reported ATA Secure Erase durations.

Appendix E – Using Health Check Before and After Erasure For Disks With Low Composite Health Scores

In ZeroData Windows, we first introduced a feature to calculate a health score percentage for all disks both before and after erasure. We base our calculation on a few well documented values we receive from the disk firmware when we inquiry them about S.M.A.R.T. values that have proved to be useful in predicting disk failures.

Although S.M.A.R.T. reporting feature has been introduced to SATA and SAS disks for years now, determining which S.M.A.R.T. values are useful in predicting disk failures is more art than science, as the S.M.A.R.T. feature is implemented as the manufacturers decide on what to report, how to report and what "conveniently" not to report for each disk model. Magnetic disks and solid-state disks have different indicators being reported, and a S.M.A.R.T. feature was not available for NVMe SSD disks until a very recent NVMe disk specification.

As disk manufacturers treat the disks returned to them as trade secret, there are very few data sets available and these sets are based on a specific customer organizations' internal tracking of disk usage. Most of them are based on data center disks which are not present in consumer disks that have vey different characteristics.

In our implementation, we are using number of bad sectors, number of weak sectors, amount of disk writes, wear level reported, and in some cases health status reported by the disk itself, then calculate a composite health score percentage. A score of 100% means perfect health, anything below means the disk has deteriorated to some extent.

After releasing this health calculation feature as part of ZeroData Windows and tracking whether it was useful by examining logs supplied to us by customers who reported issues, we decided to implement a feature to use this composite health score to determine if the disk is worth erasing or not.

We have introduced two specific parameters for ZeroData Windows: one parameter to fail a disk based on calculated composite heath score before erasing a disk, and one failing a disk after erasure based on calculated composite health score.

The feature works like this:

1) The customer decides on a composite health score that is the minimum acceptable health level for classifying disks into "worth attempting erasure" and "not worth attempting erasure",
2) After deciding on the composite health score, the customer has multiple options:
    a) Check for composite health score before erasure:
        i) Do not attempt to erase the disks below set composite health level and scrap those disks,
        ii) Attempt to erase the disks below set composite health level knowing it will not be usable and the erasure times might be much longer but try to sanitize as much data as possible before giving up.
    b) Check for composite health score after the erasure:
        i) Attempt to erase all disks regardless of composite health level knowing the erasure times might be much longer but try to sanitize as much data as possible before giving up. Then scrap the disks that have a composite health level below specified level – whether data sanitization was successful or not.
    c) Check for composite health score both before and after the erasure:
        i) Combine both approaches described above.
        ii) Do not attempt to erase the disks below set composite health level and scrap those disks,
        iii) Attempt to erase remaining disks regardless of composite health level knowing the erasure times might be much longer but try to sanitize as much data as possible before giving up. Then scrap

the disks that have a composite health level below specified level – whether data sanitization was successful or not.

We have introduced reporting for these features into our logs and reports, and most importantly to our bulk log processing utility: ZeroData Windows Reporting Console.

Customers making use of these two features can not only save energy costs at their processing stage, but also can reduce their rate of returns and associated operation costs, and reduce the frictions arising from redeploying disks with low composite health levels.

Appendix F – List of Return Codes

The return codes returned by ZeroData Windows are given below. These codes can be used to determine status of erasure results in batch files and to determine on how the workflow should proceed.

Code	Number	Description
ZDEC_ALL_ERASABLE_DISK_ERASED	0	All erasable disks were successfully erased
ZDEC_APP_START	1	Application started, no status yet
ZDEC_NO_ERASABLE_DISK	2	No erasable disk was found
ZDEC_NO_ERASURES_STARTED	3	No erasures started
ZDEC_ERASURES_FAILED_OR_CANCELLED	4	Some erasures failed or cancelled
ZDEC_SELECTED_ERASURES_SUCCESSFUL	5	Erasures selected were successful
ZDEC_SOME_ERASURES_FAILED_HS	6	Some Erasures failed due to hidden sectors
ZDEC_ERASURE_FAILED_ONE_BAD	7	One Erasure failed due to bad sectors
ZDEC_ERASURE_FAILED_ONE_WEAK	8	Erasure failed due to weak sectors
ZDEC_ERASURE_FAILED_ONE_BAD_WEAK	9	Erasure failed due to bad and weak sectors
ZDEC_ERASURES_FAILED_MULTI_BAD	10	Some Erasures failed due to bad sectors
ZDEC_ERASURES_FAILED_MULTI_WEAK	11	Some Erasures failed due to weak sectors
ZDEC_ERASURES_FAILED_MULTI_BAD_WEAK	12	Some Erasures failed due to bad and weak sectors
ZDEC_ERASURES_FAILED_IN_RAID	13	Some disks are connected in RAID mode
ZDEC_ERASURES_FAILED_MULTI_UN_HEALTHY	14	Multiple disks have failed health status
ZDEC_ERASURE_FAILED_ONE_UN_HEALTHY	15	1 disk failed health status
ZDEC_APP_ERROR	20	Application generated some errors
ZDEC_APP_ERROR_NO_WIPE_METHODS	21	Error in building wipe method list
ZDEC_APP_ERROR_LOGFILE	22	Error creating log file
ZDEC_APP_ERROR_NOTADMIN	23	Not running with administrative privileges
ZDEC_APP_ERROR_BUFFERALLOC	24	Failed to allocate a buffer
ZDEC_APP_ERROR_RNDM_NUM_BUFFERALLOC	25	Failed to allocate a Random number buffer
ZDEC_APP_ERROR_NO_OPERATOR_SUPERVISOR	26	Error when Operator/Supervisor name is not mentioned.
ZDEC_APP_ERROR_NO_DISK_CONTROLLER	27	No disk controller found
ZDEC_APP_ERROR_NO_HXA	28	HXA.dll not found
ZDEC_APP_WARNING_NC_ERASURE	29	Warning if /NC is set, and auto erasure is started.
ZDEC_APP_ERROR_INITIALISING_STRINGS	30	Error occurred while loading the
ZDEC_APP_ERROR_NO_MIC	31	MICommandsDLL.dll not found
ZDEC_APP_ALREADY_RUNNING	32	Another instance of the app is already running
ZDEC_APP_INVALID_COMMAND	33	Invalid command has been encountered
ZDEC_APP_LICENSE_OTHER_ERR	40	Error other than below
ZDEC_APP_LICENSE_FAILURE	41	License file is not present
ZDEC_APP_LICENSE_NOT_EXIT	42	License file is not present
ZDEC_APP_LICENSE_INIT_FAIL	43	Error occurred while Initializing License file.
ZDEC_APP_LICENSE_VESION_MISMATCH	44	Version mismatch for License file
ZDEC_APP_LICENSE_WRONG_PRODUCT	45	Wrong Product for License file
ZDEC_APP_LICENSE_DEMO_EXPIRE	46	Demo version is expired for License file
ZDEC_APP_LICENSE_NO_PLUG	47	USB Plug not found
ZDEC_APP_LICENSE_EXPIRE	48	License has expired
ZDEC_APP_LICENSE_ERR_PLUG	49	A license plug is missing security data or serial number.
ZDEC_APP_LICENSE_PLUG_SERIAL	50	License plug was found but with incorrect serial numbers.

.

Appendix G – List of Error Codes

Internal error codes returned by ZeroData Windows are given below. These codes are for reference only, they can't be used as return codes for batch processing and to decide on application status returned by ZeroData Windows.

Condition	Number	Description
RC_SUCCESS	0	Success
RC_LOGFILE	1	Error creating log file
RC_NOTADMIN	2	Not running with administrative privileges
RC_INVALID	3	An attempt was made to erase a restricted disk
RC_UNAVAILABLE	4	The requested Disk is unavailable for erasure
RC_OPERATORABORT	5	The operator cancelled the task
RC_BUFFERALLOC	6	Failed to allocate a buffer
RC_OPENFAIL	7	Physical device failed to open.
RC_WRITEFAIL	8	Physical device write failure.
RC_READFAIL	9	Physical device read failure
RC_DATAVERIFYFAIL	10	Physical device data verification after a Pass has failed
RC_CLICKFAIL	11	User cancelled
RC_INVALIDDEVTYPE	12	If the selected device type is other than FILE_DEVICE_DISK
RC_MINWRITERATEFAIL	13	Minimum write rate fail
RC_SHARING_VIOLATION	14	Sharing violation if disk is in use.
RC_ACCESS_DENIED	15	Access denied error.
RC_MINREADRATEFAIL	16	Minimum read rate fail
RC_OSDISK	17	Requested Disk contains OS on it.
RC_MFCFAIL	18	Could not initialize MFC
RC_SALFAIL	19	Could not initialize SAL
RC_MPFAIL	20	Error indicating error for the parameters of the command /MP
RC_HS_FAIL	21	Could not remove hidden sectors
RC_HS_SUCCESS	22	HS check successful
RC_HS_SUCCESS_REBOOT	23	HS found and removed. Reboot required
RC_EXIT_HA_FOUND	39	HA found and /EHAF is set.
Licensing Errors		
RC_LICENSE_FAILURE	24	License file is not present.
RC_LICENSE_NOT_EXIT	25	License file is not present.
RC_LICENSE_INIT_FAIL	26	Error occurred while Initialising License file.
RC_LICENSE_VESION_MISMATCH	27	Version mismatch for License file.
RC_LICENSE_WRONG_PRODUCT	28	Wrong Product for License file.
RC_LICENSE_DEMO_EXPIRE	29	Demo version is expired for License file.
RC_LICENSE_OTHER_ERR	30	Error other than above
RC_LIC_USRNAME_LOC_ERR	37	Error while getting Username/Location from License file.
Random Data Stream Buffer Error		
RC_RNDM_NUM_BUFFERALLOC	31	Failed to allocate a Random number buffer
GUID Generation Error		
RC_GUID_GENERATE_ERROR	32	Failed to generate GUID.
Errors Related To Disks Excluded From Erasure		

RC_REMOVABLE_DISK_ERR	33	Error for Removable disks when the flag /DRDE is set
RC_PREVENT_REMOVABLE_DISK_ERR	34	Error for Removable disks when the flag /DRDE is set
RC_XVN_DISK_ERROR	38	Disk erasure failed due /XVN parameter
RC_EUROSOFT_TEST_DEV	35	Error for Eurosoft Test Device USB
Missing Operator and Supervisor Data		
RC_NO_OPERATOR_SUPERVISOR	36	Error when Operator/Supervisor name is not mentioned.
Command Line Validation Error		
RC_CMD_LINE_PARAM_ERR	40	Error occurred while validating command line parameters
Firmware Command Errors		
RC_ATA_READ_IDENTITY_ERROR	60	Could not read ATA identify device data.
RC_DRIVE_FROZEN	61	Drive is frozen
RC_DEVICE_LOCKED	62	Failed to disable security.
RC_DEVICE_CANNOT_UNLOCK	63	Cannot unlock device
RC_DEVICE_PASSWORD_PROTECTED	64	Failed to remove password
RC_DEVICE_CANNOT_DISABLE_SECURITY	65	Cannot disable device security
RC_PASSWORD_COUNT_EXCEEDED	66	Password attempts exceeded. Please reboot and try again
RC_MP_NOT_ALLOWED	67	Security set to MAX. Master password not allowed. Use a user password
RC_DEVICE_INFO_FAIL	68	Failed during device information collection
RC_ATA_COMMAND_ERROR	69	ATA Command failed
RC_WRITE_STATE_FAILED	70	Write state failure
RC_NO_ERASABLE_DISK	71	No erasable disk was found
RC_ALL_ERASABLE_DISK_ERASED	72	All erasable disk were successfully erased
RC_NO_ERASURES_STARTED	73	No erasures
RC_ERASURES_FAILED_OR_CANCELLED	74	Some erasures failed or cancelled
RC_SELECTED_ERASABLE_DISK_ERASED	75	Disk selected were successfully erased
RC_SANITIZE_NOT_SUPPORTED	76	Disk Sanitize not supported
RC_NO_WIPE_METHODS	77	Error in building wipe method list
RC_MAX_ERROR_COUNT_REACHED	78	Max Error Count Reached
RC_MIN_WRITE_RATE_ERROR_COUNT_REACHED	79	Minimum Write Rate Error Count Reached
RC_MIN_READ_RATE_ERROR_COUNT_REACHED	80	Minimum Read Rate Error Count Reached
RC_NO_STORAGE_CONTROLLER	81	Storage controller not found
RC_SECURE_ERASE_NOT_SUPPORTED	82	Secure erase not supported
RC_GET_ERROR	83	Could not get disk attributes
RC_SET_ERROR	84	Could not set disk attributes
RC_UPDATE_ERROR	85	Could not update disk attributes
RC_NVMEWRITEFAIL	86	NVME Format failure
RC_TCGERASEFAIL	87	TCG Erase failure
RC_BAD_WEAK_REALLOC_SECTORS	88	Failed due to the number of bad and weak reallocated sector count
RC_BAD_REALLOC_SECTORS	89	Failed due to the number of bad reallocated sector count
RC_WEAK_REALLOC_SECTORS	90	Failed due to the number of weak reallocated sector count
RC_HEALTH_FAILED	91	Failed due to the set health percentage value
RC_IN_RAID	92	Some disks connected in RAID mode
RC_UNKNOWN	98	An unknown error occurred
RC_SYNTAX	99	Command line error or help request

Appendix H – PXE Boot Images

A PXE Boot image can be built using the Eurosoft WinPE image creation tool. This program has a separate manual so in this appendix we will only deal with the configuration of the Startnet.cmd file. The Startnet.cmd file is the file that is executed at startup when using the Windows PE environment. The commands in this file are all standard windows batch file commands, therefore it is a simple task to create a fully automated process for networked operation.

The Eurosoft Windows Image creator will create a standard file that has all the commands to boot the system and then execute ZeroData Windows using the interactive UI.

Basic Startnet.cmd file as created using the Image creation tool :

If you just want to execute ZeroData Windows from the user interface, then no changes are required to this file. The functions performed by this file and the likely changes are described below.

This first section initializes the environment and sets the machine to maximum power.

@ECHO OFF color 1f wpeutil initializenetwork Wpeutil WaitForRemovableStorage Wpeutil UpdateBootInfo wpeutil disablefirewall wpeinit /unattend:x:\unattend.xml powercfg /s 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c set SOURCEDRIVE= set PEBOOTTYPE=

The next section determines the media that the system is booted from and the architecture of the machine.

set PEBootType=%%a echo %PEBootType%

if %PEBootType%==Opt goto OptSourceDrive if %PEBootType%==SourceI goto USBSourceDrive if %PEBootType%==Remote goto PXESourceDrive if %PEBootType%==" " goto None :None Echo No Boot Device Found goto Error

:OptSourceDrive FOR /f "tokens=3 delims==\:" %%b in ('reg query "HKLM\SYSTEM\MountedDevices"^|find "5C003F00" 2^>Nul') DO set SourceDrive=%%b: goto CheckDrive

:USBSourceDrive REM Get Boot Drive from WinPE Registry for /f "tokens=3,*" %%b in ('reg query HKLM\system\currentcontrolset\control /v PEBootRamDiskSourceDrive ^| find /i "PEBootRamDiskSourceDrive"') do set SourceDrive=%%b goto CheckDrive

:PXESourceDrive SET SourceDrive=X: goto CheckDrive

:CheckDrive

Echo %SourceDrive% :Error Echo %SourceDrive%>Error.txt echo "Drive is not set">Error.txt

Now that the environment and the architecture have been determined we can call the correct version of ZeroData Windows.

CD /D %SOURCEDRIVE%\MyApplications\ZeroData\%arch%\ CLS CALL "ZeroDataWindows.exe"

:end Echo Run Complete, ready to shut down. pause wpeutil shutdown

If you are creating a fully automated script, then you can change the line where ZeroDataWindows.exe is called to include any of the command line switches and parameters described earlier in this manual.

The most important point to remember is that when you are operating using a PXE boot image, all the operations and log files will be stored in the RAM drive. This drive is destroyed each time the system is shutdown, so it is advisable to map a logical drive to a shared location on a file server for the log files and reports.

The easiest way to do this is to add a command to map a drive

Net Use {Drive Letter:} \\ServerName\Share {Password} /User:{Username}

Then you can copy all the output files to the server share

Set the copy command to overwrite existing files without confirmation.

SET COPYCMD=/Y

Then

Copy %SOURCEDRIVE%\MyApplications\ZeroData\%arch%*_LD.* {Server Share} Copy %SOURCEDRIVE%\MyApplications\ZeroData\%arch%*_Rep.* {Server Share} Copy %SOURCEDRIVE%\MyApplications\ZeroData\%arch%*_Log.* {Server Share}

This will copy all the outputs to a server location.

This is a sample basic configuration, other commands and scripts can also be added using the Windows Image Creation tool.

Appendix I – Applying Suggested Registry Setting Changes

As discussed earlier, ZeroData Windows distribution includes 3 registry keys to solve two issues that will likely be encountered while working with log and report files.

These keys are present in the folder named “ZDW_UTILITIES”, in subfolder named “RegistrySettings”.

- On some systems accessing files on a network share requires setting a registry key on the computer where Reporting Console is running, otherwise the network folders might not be visible in File Explorer windows. This issue arises from Windows UAC and security settings. The registry key named “EnableLinkedConnections.Reg” that will help you to fix this issue through registry change. For more information on this issue, you might refer to this Microsoft document: Mapped drives are not available - Windows Client | Microsoft Docs

- On most Windows computers, there is a 260-character limit on file paths. To overcome this limit, there is a registry key named “Remove260CharacterPathLimit.reg” that will help you to remove this limit through registry change.

- In case you need to restore the 260-character limit on file paths, there is a registry key named “Restore260CharacterPathLimit(Default).reg” that will help you to restore back this limit through registry change.

Please follow below sequence of steps to apply these registry changes.

1. You must have administrative rights to perform a registry change.

2. Copy the registry key files you need from ZeroData Windows distribution into a folder on the computer the changes will be made.

3. Right click on the registry key file.

4. A context aware pop-up menu will appear. In most cases, the first item in this menu will be named “Merge”, however in some cases “Merge” option may be in a different line. Select “Merge”.

5. A Registry Editor dialog window will open and ask you if you trust the source and if you are sure to continue. Click on “Yes” button.

6. The registry change will be performed.

7. After applying the registry change, you must restart the computer for the changes to take effect.