WipeDrive Enterprise User Guide

Table of Contents

IMPORTANT! PLEASE READ CAREFULLY:

Thank you for choosing WipeDrive Enterprise. Before running WipeDrive, please make sure that any files, folders, and any other information you wish to preserve is backed up on another media device (CD/DVD/EXT HD). WipeDrive will securely delete all information on the hard drive(s); the information will NOT be recoverable by any means including forensic recovery tools.

When wiping NAS/SAN devices, it is important to keep in mind that some of these devices store their firmware/OS on the drives. When WipeDrive wipes those drives, the firmware/OS is removed, making it so that the drives will no longer 'boot'.

General Information

- WipeDrive Enterprise will not be able to access the drive's previously allocated drive letter (c: d: etc.). Details such as the drive size, serial number and manufacturer will be displayed in the drive selection menu to help identify individual drives.
- While wiping a hard drive on a laptop it is recommended that it remain plugged-in to a power source as the wiping process can take an extended amount of time and may lock the hard drive if the laptop loses power. (Factors such as hard drive size and wiping methods determine this amount of time.)

Security Considerations

ADMINISTRATORS

- A WipeDrive administrator is entrusted with the ability to permanently delete data from hard drives and other media, and so should be trustworthy, careful and knowledgeable of how to use the program.

STORAGE

- The WipeDrive ISO, cloud code accounts, dongles, and any device with the ISO installed on it, should be stored in a secure location.

UPDATES

- Administrators should periodically check for updates of WipeDrive, to ensure that the latest version is being used.

DATE/TIME

- Administrators should make sure that a valid date/time is on the system before running WipeDrive.

WipeDrive Enterprise

OVERVIEW

When a Windows or Linux system saves a file, it does two things: it creates an entry for the file in the Master File Table, which functions as a sort of 'table of contents' for the drive, and it saves the file data itself onto sectors of the hard drive. If a file is deleted using the Recycle Bin, the file is not actually deleted. The file's entry in the Master File Table is deleted, but the data itself still remains intact on the hard drive, while the space that it occupies is marked for use, letting the system know that the space is available for new files to be written to. Unless new data is written to the space held by the deleted file, the original file still exists on the drive in its original state.

Any number of file recovery programs can easily look through the drive and find remnants of the file's entry in the Master File Table and put the file back together, making it as if it was never deleted in the first place. The only way to truly delete a file is to overwrite it with other information.

The primary purpose of WipeDrive is to securely overwrite all data to make any type of data recovery impossible and document the process to comply with all applicable corporate and government regulations.

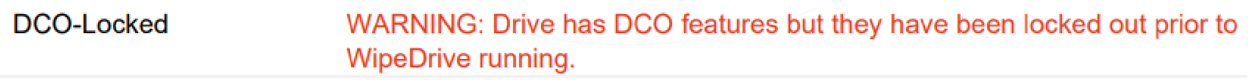
Key Features

SECURE REMOVAL OF HPA, DCO AND ACCESSIBLE MAX ADDRESS

A Host Protected Area (HPA), sometimes referred to as Hidden Protected Area, is an area of a hard drive that is not normally visible to an operating system. A Device Configuration Overlay (DCO) is a hidden area on many of today's Hard Disk Drives (HDDs) and Solid State Drives (SSDs). Accessible Max Address is a way of limiting the number of drive sectors accessible to the system. Usually when information is stored in either the DCO, HPA, or beyond the Accessible Max Address, it is not accessible by the BIOS, OS, or the user.

As part of the wipe process, WipeDrive securely removes and overwrites all data contained in HPAs, DCOs, and beyond the Accessible Max Address.

If the DCO is locked, WipeDrive will not be able to detect the DCO. The machine should warn you before the wipe and put itself to sleep for a short time in order to remove the lock. If it is unable to remove the lock, you will see the following message in the audit file:



```
DCO-Locked          WARNING: Drive has DCO features but they have been locked out prior to
                    WipeDrive running.
```

In order to bypass this, you will need to power-cycle the drive by unplugging the drive while WipeDrive is running (but before a wipe) and then attaching the drive again.

SECURE ERASE AND SANITIZE OPTIONS

A modern hard drive comes with many spare sectors. When a sector is found to be bad by the firmware of a disk controller, the disk controller remaps the logical sector to a different physical sector.

The ANSI T-13 committee which oversees the Advanced Technology Attachment (ATA) (also known as IDE) interface specification and the ANSI T-10 committee which governs the Small Computer System Interface (SCSI) specification have incorporated into their standards a command feature known as Secure Erase (SE) and Sanitize. These completely erase all reallocated disk sectors (sectors that the drive no longer uses because they have hard errors in them).

If supported by the drive, WipeDrive uses the SE and Sanitize commands as part of its NIST 800-88 Revision 1 wipe and United States Department of Defense 5220.22-M compliant (DoD 5220.22-M) wipe processes, to ensure the erasure of remapped sectors.

DETAILED AUDIT LOGGING

Documenting the secure data destruction process is requirement for most Government agencies, companies involved in health care and the financial sector.

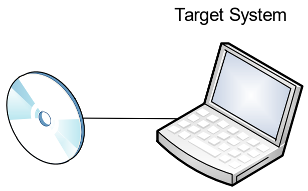
WipeDrive creates an audit log documenting every necessary detail to comply with all major regulations including DoD 5220.22-M, HIPAA, SOX and others.

Running WipeDrive Enterprise

Because organizations can be large or small, centralized or with thousands of locations WipeDrive Enterprise has multiple implementation options. Each option has its strengths; all are available to you under your license agreement. WipeDrive Enterprise can be implemented and run in three different ways. For specific instructions and details please see the corresponding section. The three options are:

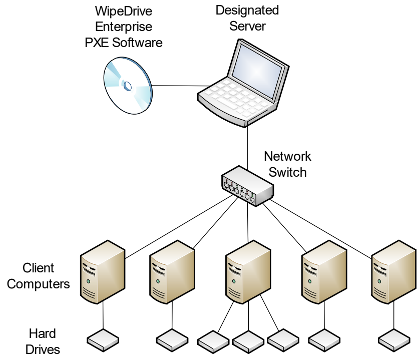
Booting from the CD or USB (see page 13)

Normally the best method when wiping a small number of systems.



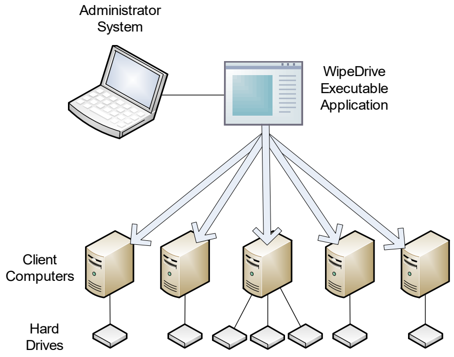
Via PXE network booting (see page 20)

Normally the best method when many computers are brought to a central location.



Via .EXE (see page 25)

Normally the best method when many computers are on the same network. This option allows systems to be wiped remotely.



Wiping Remote Computers Via WipeDrive .EXE

OVERVIEW

This method is best if wanting to securely wipe a computer not readily accessible. Using the WipeDrive application you can wipe a computer remotely one of two ways; through Remote Desktop Connection or through PsExec. This walkthrough will cover both. Before proceeding with this option please note the required criteria necessary for this to work.

REQUIRED FOR REMOTE DESKTOP CONNECTION:

- Computer Name
- User
- User Password (a password MUST exist)

Microsoft provides a thorough FAQ sheet about using this program at the following location:

http://windows.microsoft.com/en-US/windows-vista/Remote-Desktop-Connection-frequently-asked-questions

REQUIRED FOR PSEXEC:

- PsExec: http://technet.microsoft.com/en-us/sysinternals/bb897553.aspx
- Grant permissions through Regedit (See PSExec setup page 10)
- Computer Name
- User
- User Password (a password MUST exist)

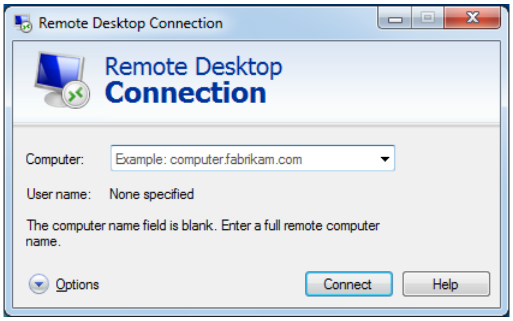
REMOTE DESKTOP CONNECTION WALKTHROUGH

Before using this option make sure the client computer either already has the WipeDrive executable program or has access to it via a download or network. If you are unable to place the WipeDrive wizard from your location onto the client computer refer to the PsExec remote wiping option.

Step 1:

The Remote Desktop Connection program is included with Windows so no install is necessary. It can be found under 'Start' - 'All Programs' - 'Accessories'. Running the program will reveal the following window.

Note: On Windows 10 it can be found under 'Start' – 'All Apps' – 'Windows Accessories'.



Remote Desktop Connection

Remote Desktop **Connection**

Computer: Example: computer.fabrikam.com

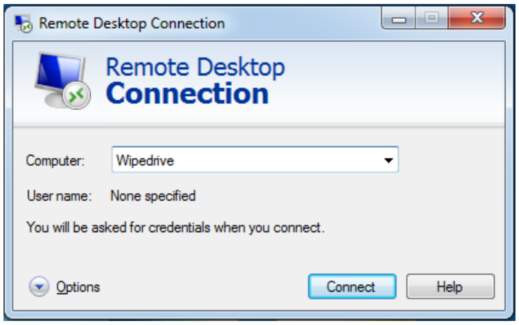
User name: None specified

The computer name field is blank. Enter a full remote computer name.

Step 2:

Next enter the Computer name of the machine you wish to access as well as the user.

If it doesn't ask for a user at this point just enter the Computer name and click '**Connect**.'



Remote Desktop Connection

Remote Desktop **Connection**

Computer: Wipedrive

User name: None specified

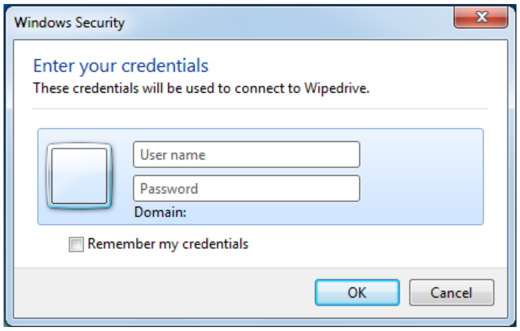
You will be asked for credentials when you connect.

Step 3:

Once the program connects to the machine it will require you enter the login credentials.

This will not work if the computer you are attempting to access isn't password protected, there must be a password.

Once the User name and Password are entered click '**OK**.'



Windows Security

Enter your credentials

These credentials will be used to connect to Wipedrive.

User name

Password

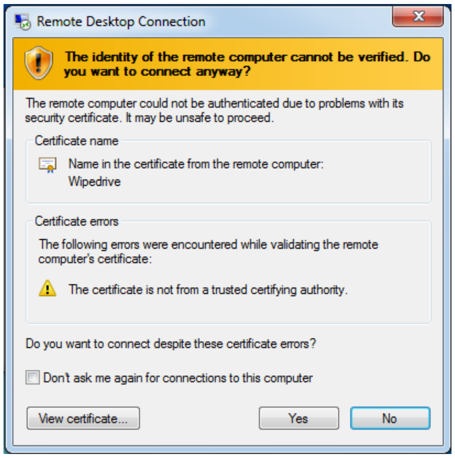
Domain:

□ Remember my credentials

Step 4:

You may see this authentication required window appear. This warning is just a precaution in the event you are logging into a malicious computer.

To access the remote computer click '**Yes**' to authorize a connection.



Remote Desktop Connection

The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
Wipedrive

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

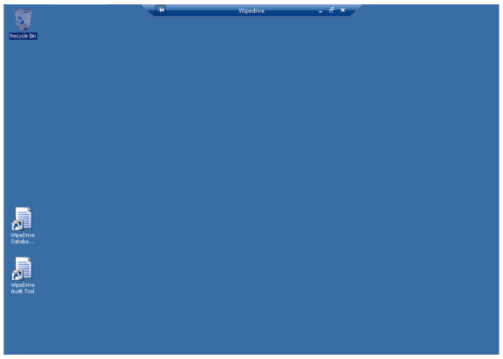
□ Don't ask me again for connections to this computer

Step 5:

After authorizing a connection your screen will change to the desktop of the client computer.

From here you can manipulate the computer and run the WipeDrive Wizard.

Navigate to the location of WipeDrive and launch the wizard. See page 24 for a walkthrough on using the WipeDrive executable.



Remote wiping via PsExec Walkthrough

Before beginning this process understand the options for this method are limited at this time. The wipe pattern utilized by the software is customizable through the “`wipe-level`” option.

By default, WipeDrive runs with the following settings:

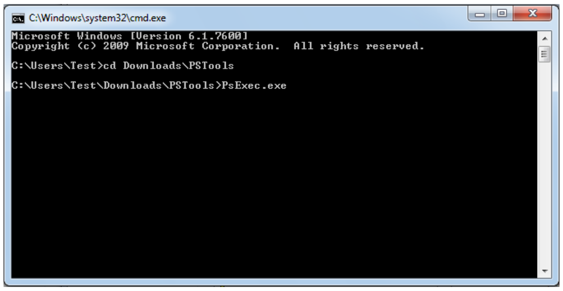
Wipe **ALL** drives | Wipe method “NIST 800-88 Revision 1”.

There are a few things that must happen prior to using this software for your remote wiping needs.

- Download and extract PsExec from the following location: http://technet.microsoft.com/en-us/sysinternals/bb897553.aspx
- Extract the files to a known location.
- PsExec needs permissions to access the client computer and make changes. This will require that you edit the Regedit on the **client** computer.
- Access client computer and open Regedit.
- Navigate to the following location: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System
- Once in this folder add the following by right clicking, selecting ‘New’ and then choosing DWORD (32-bit) Value
- Give it the name ‘LocalAccountTokenFilterPolicy’
- Right click ‘LocalAccountTokenFilterPolicy’ and select Modify to set the value to 1. Click ‘**OK**’
- Close Regedit.
- Upload the WipeDrive wizard onto the client machine unless you plan to copy the file over from the host computer to the client using PsExec.

Once these steps are complete you can begin using PsExec, the following walkthrough will demonstrate how to do this.

Step 1:



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Test>cd Downloads\PSTools

C:\Users\Test\Downloads\PSTools>PsExec.exe
```

Run the command prompt on the host machine. Do this by clicking ‘**Start**’ and typing ‘cmd’ into the Search programs and files field then press **‘Enter**.’

To run the program navigate to where the PsExec files are located.

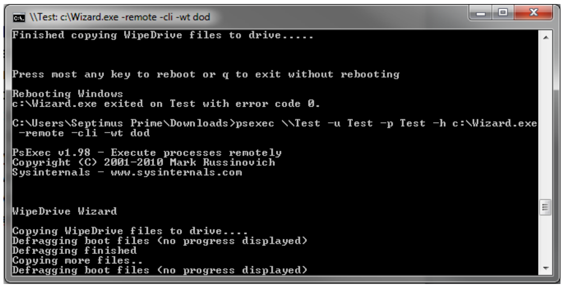
In this screen shot the PsExec files are downloaded and extracted within the ‘Downloads’ folder.

Press **‘Enter’** to start

Step 2:

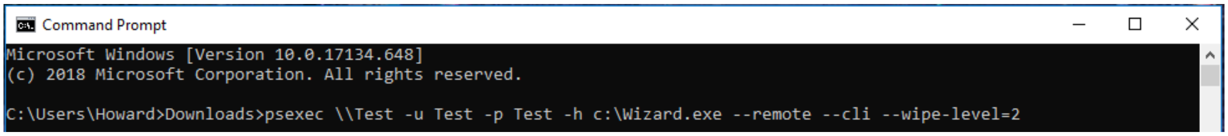
This step is split into two parts: running WipeDrive from the WipeDrive application already on the client computer and using PsExec to copy the WipeDrive executable to the client machine and then running it.

Part 1: Running WipeDrive from the executable already located on the client.



```
Finished copying WipeDrive files to drive.....


Press most any key to reboot or q to exit without rebooting

Rebooting Windows
c:\Wizard.exe exited on Test with error code 0.

C:\Users\Septimus Prime\Downloads>psexec \\Test -u Test -p Test -h c:\Wizard.exe
 -remote -cli -wt dod

PsExec v1.98 - Execute processes remotely
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com



WipeDrive Wizard

Copying WipeDrive files to drive....
Defragging boot files (no progress displayed)
Defragging finished
Copying more files..
Defragging boot files (no progress displayed)
```

- This screen shot shows an example of how to use PsExec to run WipeDrive from an executable that already exists on the client.



```
Microsoft Windows [Version 10.0.17134.648]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Howard>Downloads>psexec \\Test -u Test -p Test -h c:\Wizard.exe --remote --cli --wipe-level=2
```

The following is an explanation of each command being passed to PsExec, as well as a few suggested commands:

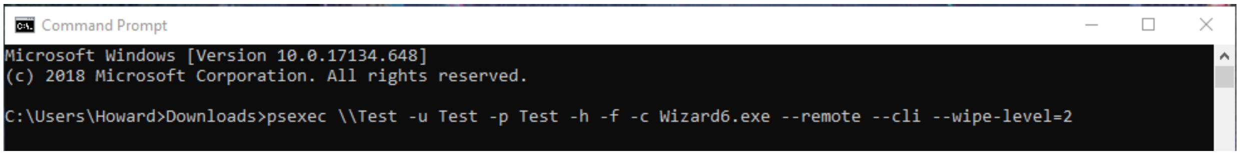
- Psexec: runs the program
- \\Test: This is the name of the client machine
- –u: Username of account on client computer
- –p: Password of user account on client computer
- –h: This command is required for clients running Windows Vista or higher
- C:\WipeDriveWizard.exe : This is the location of the WipeDrive executable. In this example the program is located on the root of the C drive.
- --remote: Allows you to remotely start the program (Be sure to use double dashes)
- --cli: must have so program knows to run in console form (Be sure to use double dashes)
- --wipe-level=2: Sets the wipe level. The 2 signifies the DoD 5220.22-M pattern
- --cloud-act-code=XXXX-XXXX-XXXX-XXXX: Inputs your Cloud Activation Code
- --disk=-1: Automatically selects all hard drives for wiping
- --number-of-confirmations=0: Skips all confirmation screens, making the software more automated
- --auto-restart: Automatically restarts the machine so that the software can run

If all parameters are valid and PsExec can find the location of WipeDrive, the WipeDrive Wizard will begin installing the necessary tools to remotely run the software.

At this point the client machine will reboot into WipeDrive and begin wiping **ALL** drives using the “NIST 800-88 Revision 1” wipe method.

Part 2: Using PsExec to copy and run WipeDrive onto client computer.

- First, place a copy of the WipeDrive wizard into the same folder where psexec.exe is located. This is critical in order for the program to find and copy the application.
- Here is a screen shot of how to properly setup the parameters in order to copy the WipeDrive wizard from the host machine to the client.

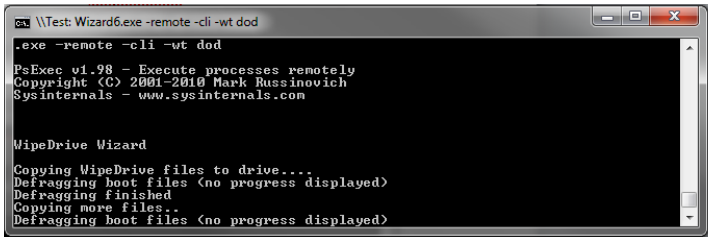


```
Microsoft Windows [Version 10.0.17134.648]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Howard>Downloads>psexec \\Test -u Test -p Test -h -f -c Wizard6.exe --remote --cli --wipe-level=2
```

Just as before, here is an explanation of the parameters required to copy the WipeDrive application to the client computer and then run it, as well as a few suggested commands:

- Psexec: Run following parameters through PsExec
- \\Test: Name of client computer
- –u: Username of account on client computer
- –p: Password of user account on client computer
- –h: This command is required for clients running Windows Vista or higher
- –c WipeDriveWizard.exe: The copy command followed by the file to be copied and ran on the client machine. (Only works if file is found in same location as PsExec)
- --remote: Allows you to remotely start the program (Be sure to use double dashes)
- --cli: must have so program knows to run in console form (Be sure to use double dashes) --wipe-level=2: Sets the wipe level. The 2 signifies the DoD 5220.22-M pattern
- --cloud-act-code=XXXX-XXXX-XXXX-XXXX: Inputs your Cloud Activation Code
- --disk=-1: Automatically selects all hard drives for wiping
- --number-of-confirmations=0: Skips all confirmation screens, making the software more automated
- --auto-restart: Automatically restarts the machine so that the software can run

If all parameters are valid and PsExec can find the location of WipeDrive the following screen will appear:



```
.exe -remote -cli -wt dod

PsExec v1.98 - Execute processes remotely
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com



WipeDrive Wizard

Copying WipeDrive files to drive....
Defragging boot files (no progress displayed)
Defragging finished
Copying more files..
Defragging boot files (no progress displayed)
```

As you can see PsExec copied the WipeDrive Wizard and began installing the necessary tools to remotely run the software.

At this point the client machine will reboot into WipeDrive and begin wiping **ALL** drives using the “NIST 800-88 Revision 1” wipe method.

WipeDrive Boot Via CD or USB

OVERVIEW

Running WipeDrive via CD or USB is normally a good choice when the number of computers to be wiped are small as the CD/USB must be inserted and booted on each system.

SYSTEM REQUIREMENTS

- All versions of DOS, Windows 3.x, 9x, NT, 2000, XP, Vista, 7, OS/2, PC-based, 8, 8.1, and 10, Linux, Unix and Intel-based Mac systems.
- Any type of hard drive (IDE, SCSI, SATA, SSD).
- CD-ROM Drive or USB port
- 1 GB RAM

BIOS SETTINGS

To run WipeDrive Enterprise via CD/USB insert the media into the computer and check that the BIOS is set to first boot from the CD or USB drive. To change the boot sequence, access the BIOS of the computer during the initial start-up of the system. When the computer first turns on/restarts a screen will flash with options to enter either 'Setup' or 'Boot,' as well as a key to press for each corresponding option. See table below for known BIOS keys based on system manufacturer. The key must be pressed quickly, otherwise the computer will continue with its usual booting routine.

Manufacturer	BIOS Key
Acer®	F1, F2, CTRL+ALT+ESC
Compaq®	F10
Dell®	F2, DEL
eMachine®	DEL, F2
Gateway®	F1, F2
HP®	F1, F2, ESC
IBM®	F1
Lenovo®	F1, F2
Apple®	Hold down Option
Micron®	F1, F2, or DEL
Sony®	F2, F3
Toshiba®	ESC, F1

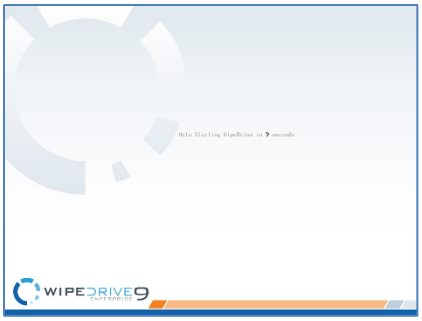
NOTE: If your particular computer or manufacturer is not displayed, the BIOS keys are normally either DEL or F2.

Wipe Process via CD or USB

Step 1

Insert WipeDrive into the CD-ROM drive or USB port and restart the computer.

WipeDrive will now load the necessary drivers.



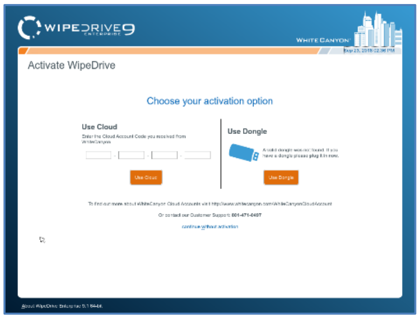
Auto Starting WipeDrive in 7 seconds

Step 2

WipeDrive will now ask for your Cloud Activation Code.

If you have a Cloud Activation Code, enter it in the 4 boxes now then press ‘**Use Cloud’**. Your code can be found in the email with your download links.

If you have a dongle, please insert the dongle now and press ‘**Use Dongle’**.



Activate WipeDrive

Choose your activation option

Use Cloud
Enter the Cloud Account Code you received from WhiteCanyon

Use Dongle
A valid dongle was not found. If you have a dongle please plug it in now.

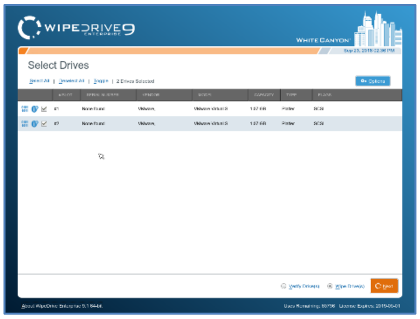
To find out more about WhiteCanyon Cloud Accounts visit http://www.whitecanyon.com/WhiteCanyonCloudAccount

Or contact our Customer Support: 801-471-0497

Step 3

WipeDrive will now display all attached hard drives. Please select the drives you wish to securely erase.

Select ‘**Next’** to continue.



Select Drives

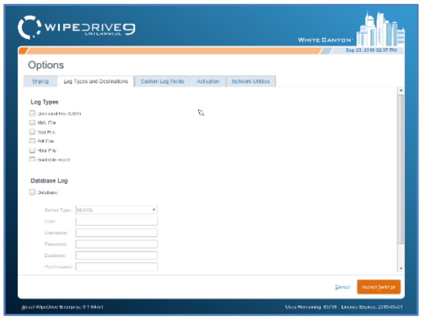
Select All | Deselect All | Toggle | 2 Drives Selected

	[illegible]	SERIAL NUMBER	VENDOR	MODEL	CAPACITY	TYPE	[illegible]
☑	#1	None found	VMware,	VMware Virtual S	1.07 GB	Platter	SCSI
☑	#2	None found	VMware,	VMware Virtual S	1.07 GB	Platter	SCSI

Step 4

If you wish to change the log format or destination; please select ‘**Options**’.

From here you can also set Custom Log Fields, enter your activation code or dongle credentials, or view Network Utilities.



Options

Wiping | Log Types and Destinations | Custom Log Fields | Activation | Network Utilities

Log Types

- ☐ Delimited File (CSV)
- ☐ XML File
- ☐ Text File
- ☐ Pdf File
- ☐ Html File
- ☐ Bootable report

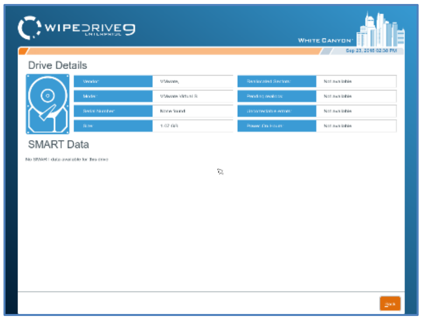
Database Log

- ☐ Database

Server Type: MySQL
Host:
Username:
Password:
Database:
Port/Instance:

Step 5

By selecting the info icon next to the drive serial number, you can view the Drive Details.



Drive Details

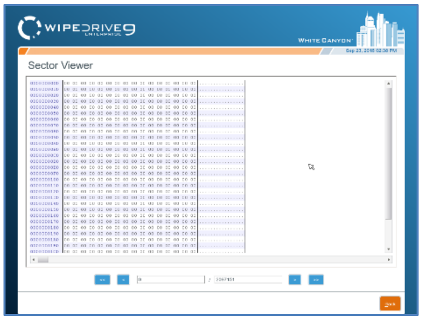
Vendor:	VMware,	Reallocated Sectors:	Not available
Model:	VMware Virtual S	Pending sectors:	Not available
Serial Number:	None found	Uncorrectable errors:	Not available
Size:	1.07 GB	Power On Hours:	Not available

SMART Data

No SMART data available for this drive

Step 6

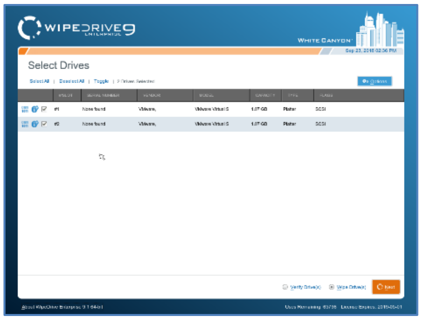
By selecting the Sector icon next to the drive serial number you can see the Sector Viewer.



Step 7

In the bottom right hand corner of the Drive Selection screen, you can select **'Wipe Drives'** or **'Verify Drives'.**

Select **'Next'** to continue.



Select Drives

Select All | Deselect All | Toggle | 2 Drives Selected

	SLOT	SERIAL NUMBER	VENDOR	MODEL	CAPACITY	TYPE	FLAGS
☑	#1	None found	VMware,	VMware Virtual S	1.07 GB	Platter	SCSI
☑	#2	None found	VMware,	VMware Virtual S	1.07 GB	Platter	SCSI

○ Verify Drive(s) ● Wipe Drive(s)

About WipeDrive Enterprise 9.1 64-bit

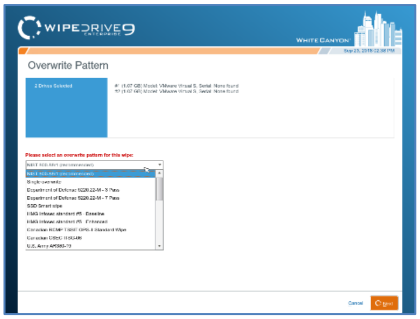
Uses Remaining: 63799 License Expires: 2019-05-01

Step 8

The overwrite pattern can be changed on this screen. WhiteCanyon recommends either the Standard Overwrite or the "NIST 800-88 Revision 1" overwrite Pattern.

Please see page 32 for more details on wipe patterns.

Select '**Next'** to continue.



Overwrite Pattern

2 Drives Selected

#1 (1.07 GB) Model: VMware Virtual S, Serial: None found
#2 (1.07 GB) Model: VMware Virtual S, Serial: None found

Please select an overwrite pattern for this wipe:

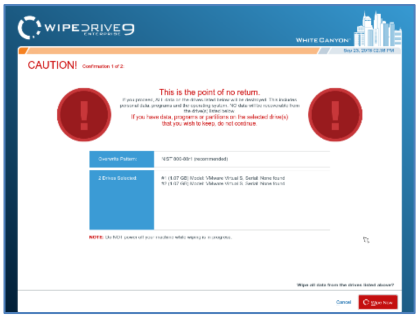
NIST 800-88r1 (recommended)

- NIST 800-88r1 (recommended)
- Single overwrite
- Department of Defense 5220.22-M - 3 Pass
- Department of Defense 5220.22-M - 7 Pass
- SSD Smart wipe
- HMG Infosec standard #5 - Baseline
- HMG Infosec standard #5 - Enhanced
- Canadian RCMP TSSIT OPS-II Standard Wipe
- Canadian CSEC ITSG-06
- U.S. Army AR380-19

Step 9

WipeDrive will warn that this process is irreversible. Select **'Wipe Now'** to continue.

Warning: selecting "Wipe Now" will permanently delete ALL data from hard drives and other media. Personal data, programs, and the operating system will all be removed. No data will be recoverable from the drives after WipeDrive has deleted the data.



CAUTION! Confirmation 1 of 2:

This is the point of no return.

If you proceed, ALL data on the drives listed below will be destroyed. This includes personal data, programs and the operating system. NO data will be recoverable from the drive(s) listed below.

If you have data, programs or partitions on the selected drive(s) that you wish to keep, do not continue.

Overwrite Pattern:	NIST 800-88r1 (recommended)
2 Drives Selected:	#1 (1.07 GB) Model: VMware Virtual S, Serial: None found #2 (1.07 GB) Model: VMware Virtual S, Serial: None found

NOTE: Do NOT power off your machine while wiping is in progress.

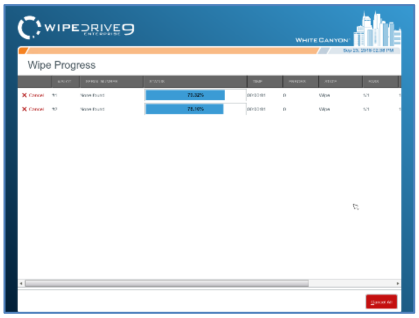
Wipe all data from the drives listed above?

Step 10

WipeDrive will now begin wiping the hard drive.

Warning: If you cancel the wipe before completion there may still be recoverable data left on the drive.

Warning: Do not power off the system while a firmware-based wipe (e.g. Secure Erase, Sanitize Device, etc.) is taking place. Doing so may put the drive in a bad state.

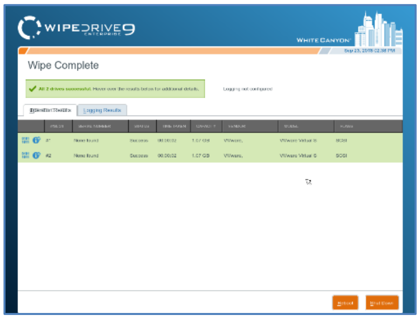


Wipe Progress

	SLOT	SERIAL NUMBER	STATUS	TIME	ERRORS	STAGE	PASS
✕ Cancel	#1	None found	75.32%	00:00:01	0	Wipe	1/1
✕ Cancel	#2	None found	75.10%	00:00:01	0	Wipe	1/1

Step 11

When the process is completed WipeDrive will display the Wiping Complete screen and save the log file if applicable.



Wipe Complete

✓ All 2 drives successful. Hover over the results below for additional details.

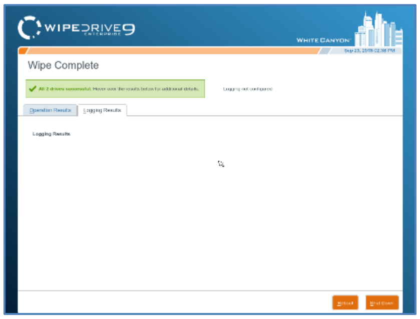
Logging not configured

	SLOT	SERIAL NUMBER	STATUS	TIME TAKEN	CAPACITY	VENDOR	MODEL	FLAGS
	#1	None found	Success	00:00:02	1.07 GB	VMware,	VMware Virtual S	SCSI
	#2	None found	Success	00:00:02	1.07 GB	VMware,	VMware Virtual S	SCSI

Step 12

Select **'Log Results'** to view the logging details.

Click Reboot or Shut Down to exit WipeDrive.



Wipe Complete

✓ All 2 drives successful. Hover over the results below for additional details.

Logging not configured

Logging Results

Configuration Settings

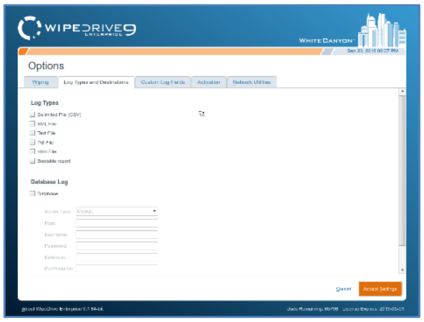
Log Types

WipeDrive offers a variety of different log type formats. Within the Options menu, under the Log Types and Destinations tab, simply select in which format(s) you would like the logs to be created.*

*The Database format requires additional information in order to properly create the file.

These details include:

- Server Type (MySQL or MS SQL)
- Host
- Username
- Password
- Database credentials
- Port/Instance



Log Types

☐ Delimited File (CSV)
☐ XML File
☐ Text File
☐ Pdf File
☐ Html File
☐ Bootable report

Database Log

☐ Database

Server Type: MySQL
Host:
Username:
Password:
Database:
Port/Instance:

Log Destination

For user convenience, WipeDrive has multiple methods in which a log file may be saved. Please reference the following instructions on how to take advantage of these options. All authentication data to external servers is sent in plain text. WipeDrive should be used in a trusted internal network if protecting the authentication data to the third-party servers is a priority.

Windows Share

This feature allows the user to save the log file to a shared network of files. The following information is required:

- Host
- Username
- Password
- Domain
- Path (optional)

FTP

The FTP option allows the user to save the log file to an FTP server. This requires the following information:

- Host
- Username
- Password
- Path (optional)

Removable

By default, WipeDrive will try to log to a removable USB drive. In order to ensure the logging process is a success, make sure a USB drive is plugged into the computer running WipeDrive.

Email

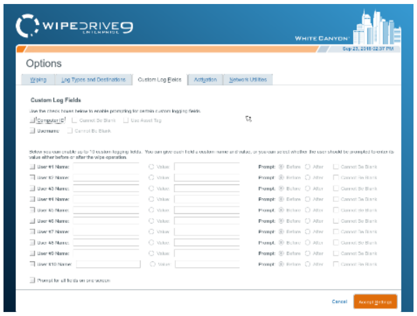
WipeDrive also allows the user to send the log file to a specific email. **Note**: The sending party will be labeled as root. The user must enter the following information:

- Host
- Username
- Password

- From (sending email)
- To (receiving email)
- CC
- Subject

Custom Log Fields

The Custom Log Fields tab under Settings allows the user to put additional information to the log file. Information such as the Computer ID, a Username, as well as any other custom information the user wishes include in the file.



Custom Log Fields

Use the check boxes below to enable prompting for certain custom logging fields.

□ Computer ID □ Cannot Be Blank □ Use Asset Tag

□ Username □ Cannot Be Blank

Below you can enable up to 10 custom logging fields. You can give each field a custom name and value, or you can select whether the user should be prompted to enter its value either before or after the wipe operation.

□ User #1 Name: ○ Value: Prompt: ● Before ○ After □ Cannot Be Blank

□ User #2 Name: ○ Value: Prompt: ● Before ○ After □ Cannot Be Blank

□ User #3 Name: ○ Value: Prompt: ● Before ○ After □ Cannot Be Blank

□ User #4 Name: ○ Value: Prompt: ● Before ○ After □ Cannot Be Blank

□ User #5 Name: ○ Value: Prompt: ● Before ○ After □ Cannot Be Blank

□ User #6 Name: ○ Value: Prompt: ● Before ○ After □ Cannot Be Blank

□ User #7 Name: ○ Value: Prompt: ● Before ○ After □ Cannot Be Blank

□ User #8 Name: ○ Value: Prompt: ● Before ○ After □ Cannot Be Blank

□ User #9 Name: ○ Value: Prompt: ● Before ○ After □ Cannot Be Blank

□ User #10 Name: ○ Value: Prompt: ● Before ○ After □ Cannot Be Blank

□ Prompt for all fields on one screen

Computer ID

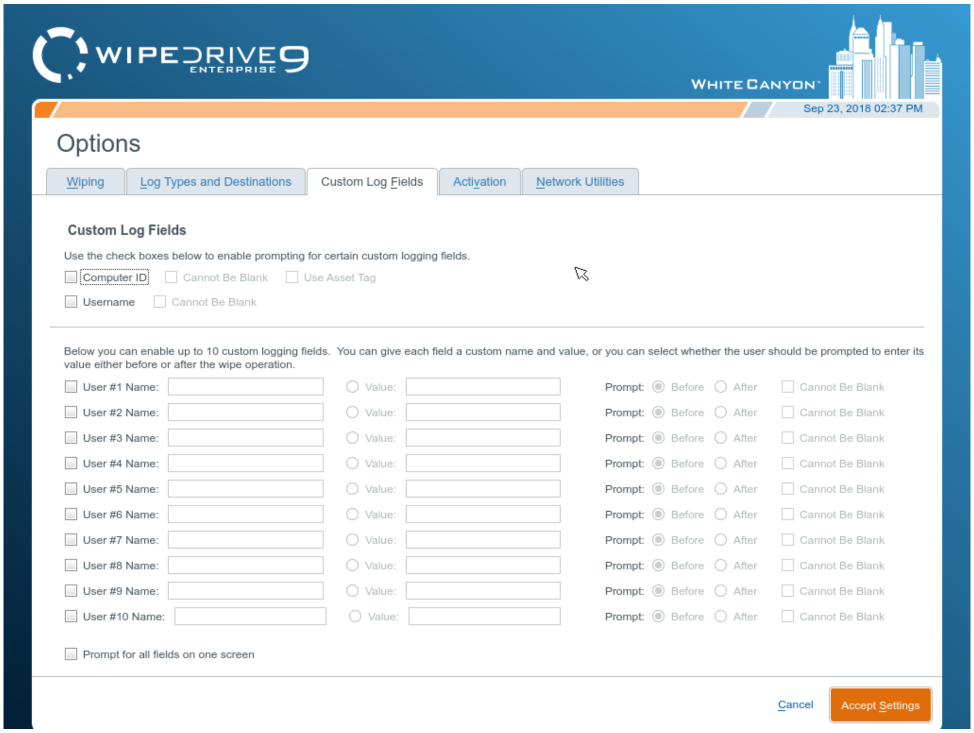
This feature allows the user to give the computer being wiped a specific identification label. WipeDrive will prompt the user to enter the Computer ID after the warning page prior to the initiation of the wiping process.

Username

The username feature works the same way as the Computer ID. The user will be prompted to enter a username prior to the wiping process.

Custom Fields

A user can add up to 10 custom log fields. Each field can be selected to prompt the User either before or after the wiping process to enter a value or enter the default value at this screen.



Options

Custom Log Fields

Use the check boxes below to enable prompting for certain custom logging fields.

□ Computer ID □ Cannot Be Blank □ Use Asset Tag

□ Username □ Cannot Be Blank

Below you can enable up to 10 custom logging fields. You can give each field a custom name and value, or you can select whether the user should be prompted to enter its value either before or after the wipe operation.

□ User #1 Name:		○ Value:		Prompt: ● Before	○ After	□ Cannot Be Blank
□ User #2 Name:		○ Value:		Prompt: ● Before	○ After	□ Cannot Be Blank
□ User #3 Name:		○ Value:		Prompt: ● Before	○ After	□ Cannot Be Blank
□ User #4 Name:		○ Value:		Prompt: ● Before	○ After	□ Cannot Be Blank
□ User #5 Name:		○ Value:		Prompt: ● Before	○ After	□ Cannot Be Blank
□ User #6 Name:		○ Value:		Prompt: ● Before	○ After	□ Cannot Be Blank
□ User #7 Name:		○ Value:		Prompt: ● Before	○ After	□ Cannot Be Blank
□ User #8 Name:		○ Value:		Prompt: ● Before	○ After	□ Cannot Be Blank
□ User #9 Name:		○ Value:		Prompt: ● Before	○ After	□ Cannot Be Blank
□ User #10 Name:		○ Value:		Prompt: ● Before	○ After	□ Cannot Be Blank

□ Prompt for all fields on one screen

WipeDrive Boot Via PXE

Overview

Running WipeDrive via PXE is normally a good choice when the number of computers to be wiped is large.

Because the server controls the process, it is not necessary to attach monitors, mice or keyboards to workstations. The progress for each individual system is displayed on the server, the only requirement is that the boot priority for the system be set to ‘Network Boot’.

Depending on the hardware used WipeDrive can support hundreds of systems simultaneously.

System Requirements

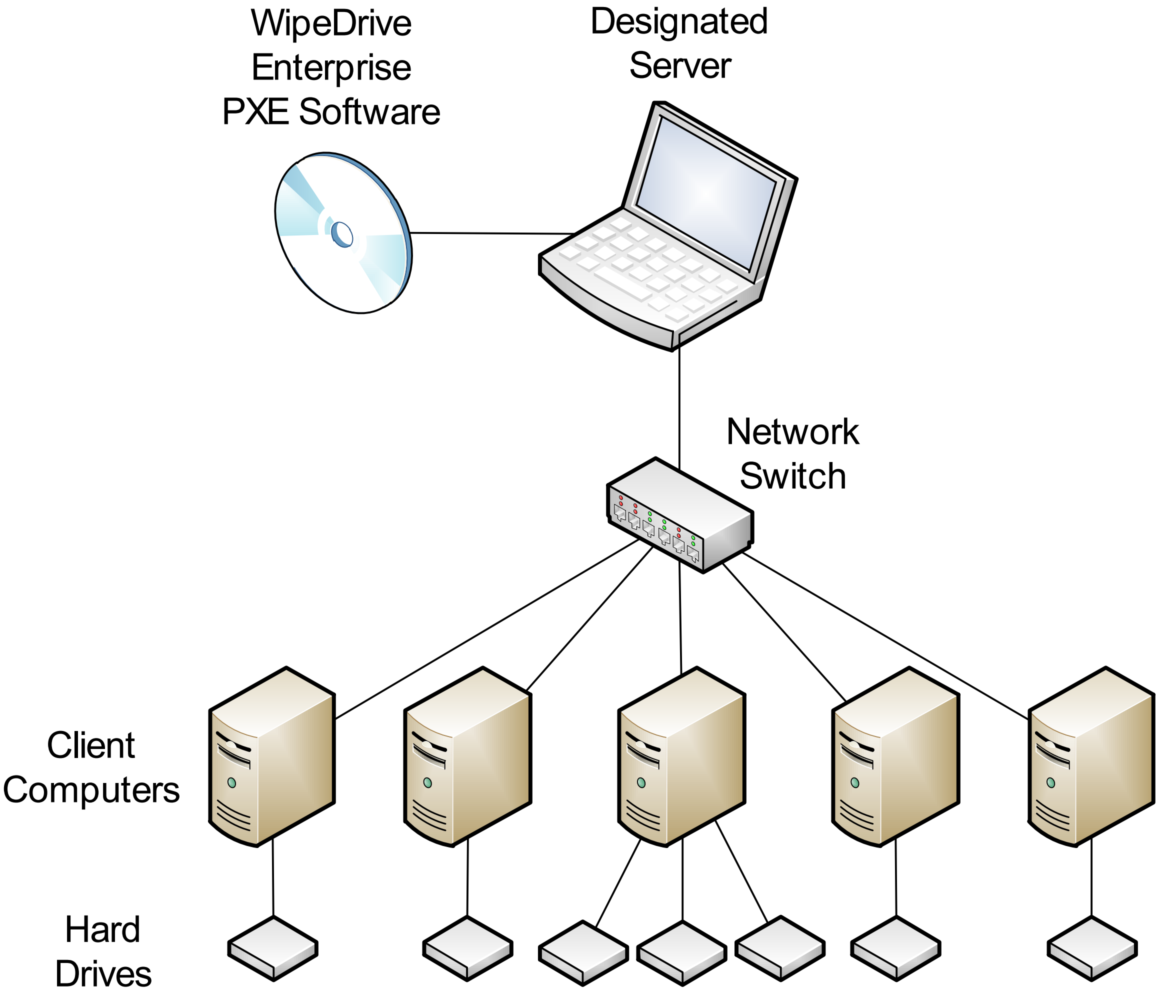
Computer designated to be the server (will not be wiped) with at least the following hardware:

- Core 2 Duo or better / Intel-based Mac OSX v10.6 or better
- 1 GB RAM
- CD-ROM drive or USB port
- Network card
  - If using Cloud activation or logging outside the PXE network a second network card is required.

One or more machines, referred to as the ‘clients’, with at least the following hardware:

- Core 2 Duo or better / Intel-based Mac OSX v10.6 or better
- 1 GB RAM
- Network card
- Network switches and cabling to configure all of the machines (server and clients) to be in the same network.

SETUP DIAGRAM



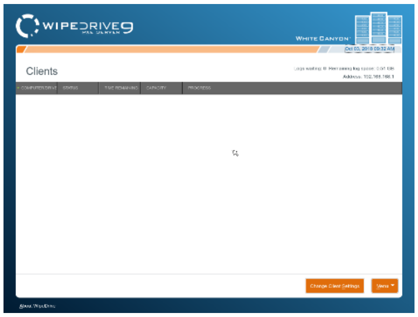
Wipe Process Via PXE

Step 1

Insert the WipeDrive PXE CD into the CD-ROM drive (or insert the WipeDrive PXE USB) and restart the Server.

Please Note: The Server must have at least 1 GB of RAM.

The computer will then display the WipeDrive Client Screen. To edit the type of wipe, please select '**Change Client Settings**'.



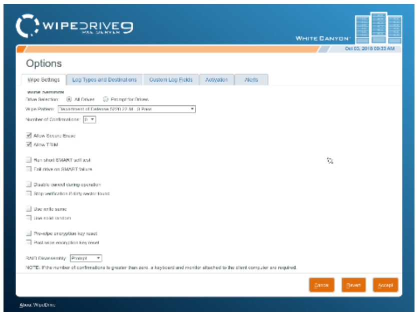
Clients

Logs waiting: 0 Remaining log space: 0.01 GB
Address: 192.168.168.1

COMPUTER/DRIVE	STATUS	TIME REMAINING	CAPACITY	PROGRESS

Step 2

WipeDrive will now list the Wipe Settings that can be adjusted. Please select the necessary options then select the '**Log Types and Destinations**' tab.



Options

Wipe Settings

Drive Selection: ● All Drives ○ Prompt for Drives
Wipe Pattern: Department of Defense 5220.22-M - 3 Pass
Number of Confirmations: 0

☑ Allow Secure Erase
☑ Allow TRIM

□ Run short SMART self test
□ Fail drive on SMART failure

□ Disable cancel during operation
□ Stop verification if dirty sector found

□ Use write same
□ Use solid random

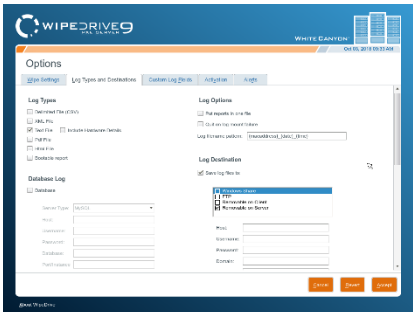
□ Pre-wipe encryption key reset
□ Post-wipe encryption key reset

RAID Disassembly: Prompt

NOTE: If the number of confirmations is greater than zero, a keyboard and monitor attached to the client computer are required.

Step 3

The Log Types and Log Destinations menu will allow the User to adjust these settings. Select the necessary options and select the '**Custom Log Fields**' tab.



Options

Log Types

□ Delimited File (CSV)
□ XML File
☑ Text File □ Include Hardware Details
□ Pdf File
□ Html File
□ Bootable report

Database Log

□ Database

Server Type: MySQL
Host:
Username:
Password:
Database:
Port/Instance:

Log Options

□ Put reports in one file
□ Quit on log mount failure
Log filename pattern: {macaddress}_{date}_{time}

Log Destination

☑ Save log files to:

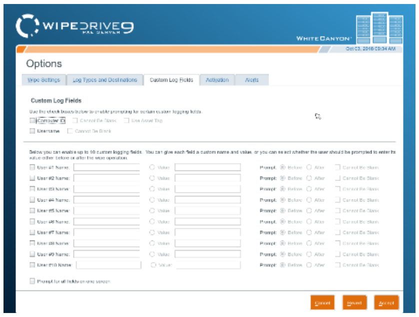
□ Windows Share
□ FTP
□ Removable on Client
☑ Removable on Server

Host:
Username:
Password:
Domain:

Step 4

The Custom Log Fields menu will allow the User to include specific fields in the Log File. WipeDrive will prompt for these fields prior to running the deletion.

Please select the '**Activate'** tab.



Options

Custom Log Fields

Use the check boxes below to enable prompting for certain custom logging fields.

□ Computer ID □ Cannot Be Blank □ Use Asset Tag
□ Username □ Cannot Be Blank

Below you can enable up to 10 custom logging fields. You can give each field a custom name and value, or you can select whether the user should be prompted to enter its value either before or after the wipe operation.

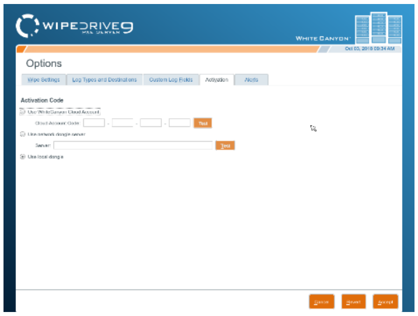
□ User #1 Name: ○ Value: Prompt: ● Before ○ After □ Cannot Be Blank
□ User #2 Name: ○ Value: Prompt: ● Before ○ After □ Cannot Be Blank
□ User #3 Name: ○ Value: Prompt: ● Before ○ After □ Cannot Be Blank
□ User #4 Name: ○ Value: Prompt: ● Before ○ After □ Cannot Be Blank
□ User #5 Name: ○ Value: Prompt: ● Before ○ After □ Cannot Be Blank
□ User #6 Name: ○ Value: Prompt: ● Before ○ After □ Cannot Be Blank
□ User #7 Name: ○ Value: Prompt: ● Before ○ After □ Cannot Be Blank
□ User #8 Name: ○ Value: Prompt: ● Before ○ After □ Cannot Be Blank
□ User #9 Name: ○ Value: Prompt: ● Before ○ After □ Cannot Be Blank
□ User #10 Name: ○ Value: Prompt: ● Before ○ After □ Cannot Be Blank

□ Prompt for all fields on one screen

Step 5

The Activation menu allows the user to select activation options. These options include Cloud Account activation, using an activation dongle on the PXE server, and/or using the activation dongle on the client machines.

Next click the '**Alerts**' tab.



Options

Activation Code

○ Use WhiteCanyon Cloud Account

Cloud Account Code: ___ - ___ - ___ - ___

○ Use network dongle server

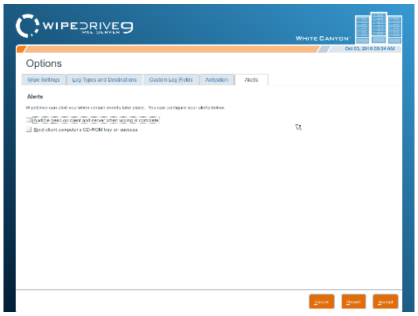
Server:

● Use local dongle

Step 6

The Alerts menu allows the User to select alert methods for when the wipe completes on the Client machines.

Click '**Accept**' to save the options.



Options

Alerts

WipeDrive can alert you when certain events take place. You can configure your alerts below.

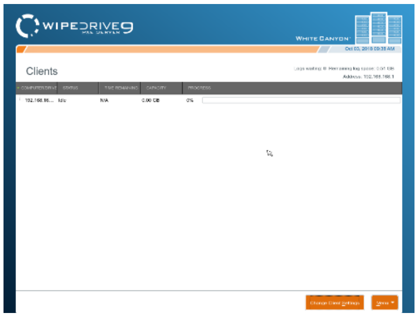
□ Audible beep on client and server when wiping is complete

□ Eject client computer's CD-ROM tray on success

Step 7

Restart each Client machine. The Client machines will boot into WipeDrive over the Network and begin the wipe.

The Server will display the wipe progress on each Client machine.



Clients

Logs waiting: 0 Remaining log space: 0.01 GB

Address: 192.168.168.1

COMPUTER/DRIVE	STATUS	TIME REMAINING	CAPACITY	PROGRESS
192.168.16...	Idle	N/A	0.00 GB	0%

Install the PXE Server

OVERVIEW

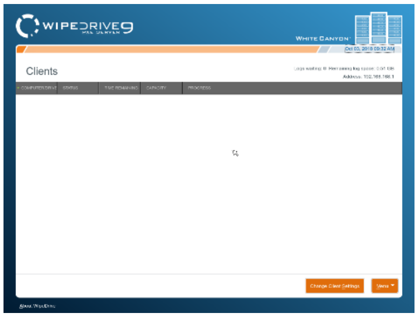
If you prefer not to boot from any bootable media each time you run the PXE server, it is possible to install PXE to the server instead. It does not make any difference on how the software runs however, and is solely based on preference.

Step 1

Insert the WipeDrive PXE CD into the CD-ROM drive (or the WipeDrive PXE USB into the USB port) and restart the Server.

Please Note: The Server must have at least 1 GB of RAM.

The computer will then display the WipeDrive Client Screen.



Step 2

Type ‘exit’ anywhere on the screen and select yes to go to the command prompt.

From here, type the following without quotations and press enter: “cd /hard_drive_install”

Now type the following without quotations and press enter to install to the hard drive: “./hdinstall.sh”

Step 3

PXE is now installed on the machine. You can now eject the CD and restart the computer to continue PXE as normal.

WipeDrive Boot Via .EXE

OVERVIEW

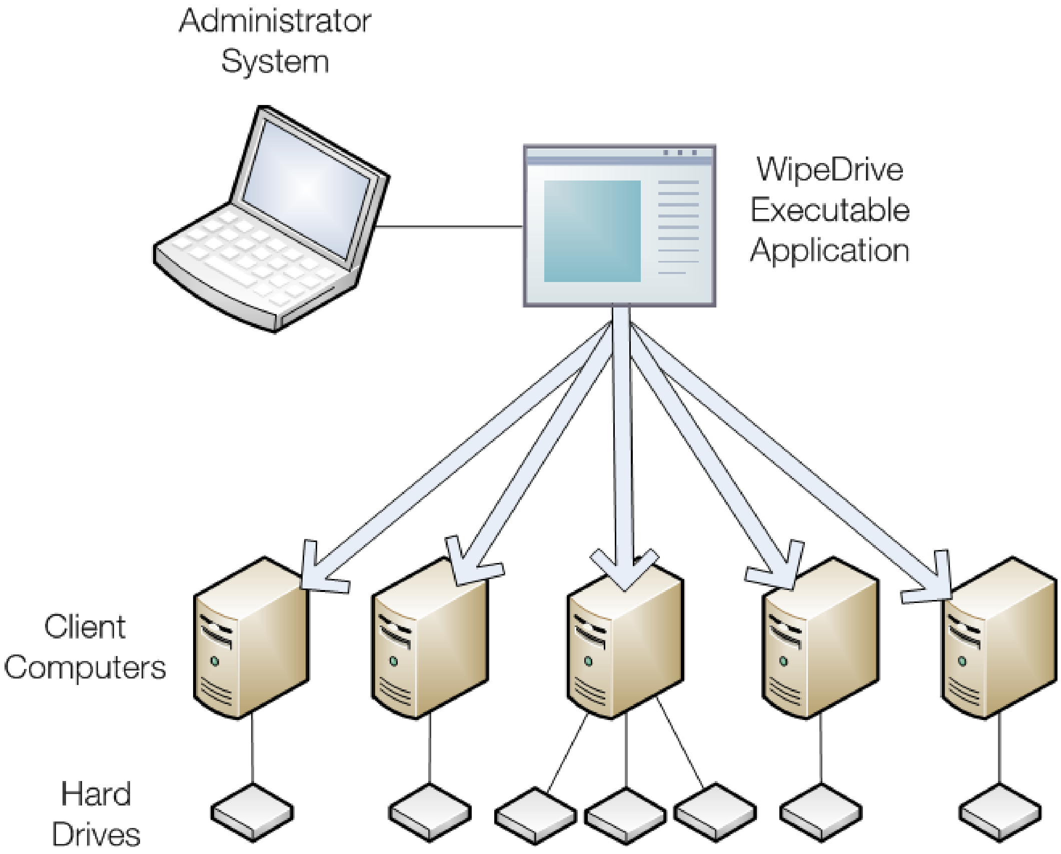
Running WipeDrive via EXE is normally a good choice when then number of computers to be wiped is large and the systems are spread out over multiple locations.

The .EXE build is a scripted build of WipeDrive that can be run over a network on any x86 system to which you have administrative rights. The system will wipe remotely and send a log file for confirmation when the process is complete.

SYSTEM REQUIREMENTS

- Computer running Windows 98, NT, 2000, 2003, XP, Vista and 7. 8, 8.1 and 10 with disabled UEFI
- 256 MB Free Hard Drive Space
- 1 GB RAM

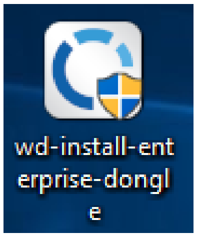
SETUP DIAGRAM



Wipe Process Via .EXE

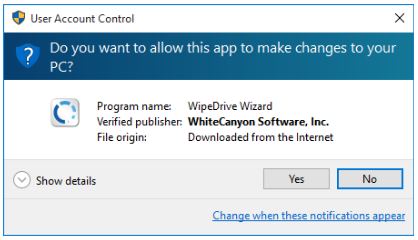
Step 1

Place WipeDrive on to the Client’s desktop then double click to run WipeDrive.



Step 2

Windows will now ask if you would like to run this program. Please select ‘**Yes**’.



User Account Control

Do you want to allow this app to make changes to your PC?

Program name: WipeDrive Wizard
Verified publisher: **WhiteCanyon Software, Inc.**
File origin: Downloaded from the Internet

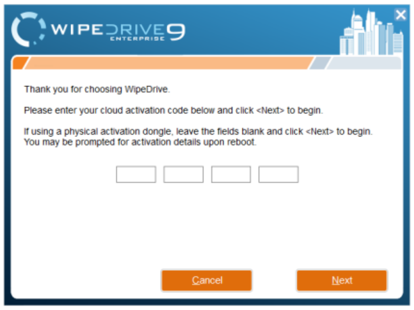
Step 3

WipeDrive may ask for an activation code, please enter the provided code given to you once the purchase was made.

Many Enterprise licenses will skip this step if using a Dongle or a custom build.

In order to move forward, a valid activation code is required. After the code is entered the ‘Next’ button will activate.

Click ‘**Next’** to proceed to the next screen.



Thank you for choosing WipeDrive.

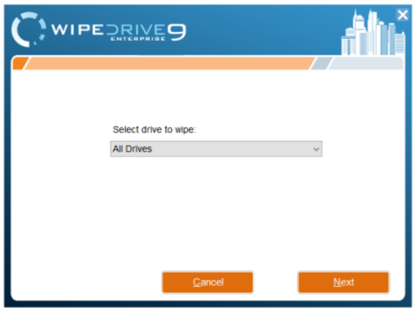
Please enter your cloud activation code below and click <Next> to begin.

If using a physical activation dongle, leave the fields blank and click <Next> to begin.
You may be prompted for activation details upon reboot.

Step 4

Click on the drop-down list to select which drive to wipe. There are only two options when selecting hard drives to be wiped, ‘All Drives’ or a single individual drive.

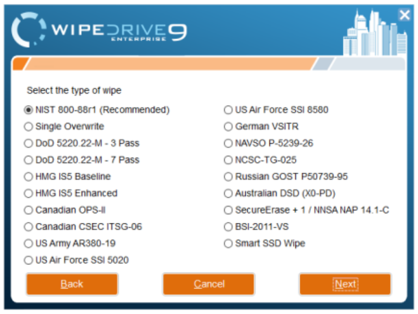
After selecting a drive click ‘Next’ to continue.



Select drive to wipe:
All Drives

Step 5

At the Wipe Selection menu, select the required wipe and select ‘**Next**’.

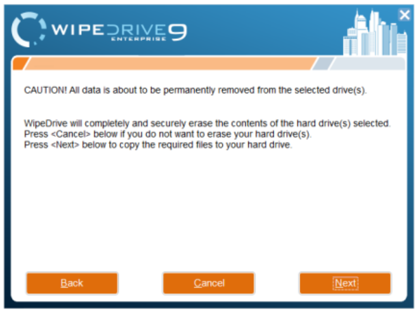


Select the type of wipe

● NIST 800-88r1 (Recommended)
○ Single Overwrite
○ DoD 5220.22-M - 3 Pass
○ DoD 5220.22-M - 7 Pass
○ HMG IS5 Baseline
○ HMG IS5 Enhanced
○ Canadian OPS-II
○ Canadian CSEC ITSG-06
○ US Army AR380-19
○ US Air Force SSI 5020
○ US Air Force SSI 8580
○ German VSITR
○ NAVSO P-5239-26
○ NCSC-TG-025
○ Russian GOST P50739-95
○ Australian DSD (X0-PD)
○ SecureErase + 1 / NNSA NAP 14.1-C
○ BSI-2011-VS
○ Smart SSD Wipe

Step 6

WipeDrive will now verify that you wish to securely overwrite the hard drive(s). Select ‘**Next’** to continue.

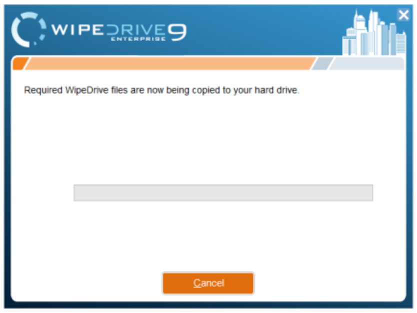


CAUTION! All data is about to be permanently removed from the selected drive(s).

WipeDrive will completely and securely erase the contents of the hard drive(s) selected.
Press <Cancel> below if you do not want to erase your hard drive(s).
Press <Next> below to copy the required files to your hard drive.

Step 7

Before beginning the wiping process WipeDrive will first install the required files.

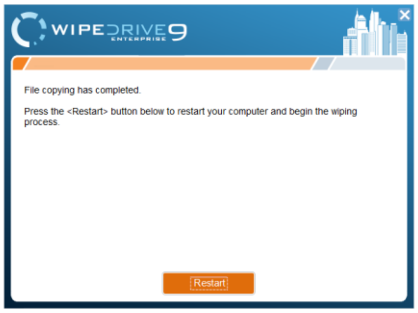


Required WipeDrive files are now being copied to your hard drive.

Step 8

In order to overwrite the entire hard drive, WipeDrive runs outside of Windows within a Linux kernel. For this to happen the computer must restart and boot into the WipeDrive program.

Click ‘**Restart**’ to begin this process.



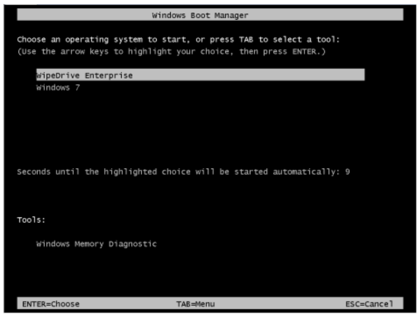
File copying has completed.

Press the <Restart> button below to restart your computer and begin the wiping process.

Step 9

Once the computer restarts you will see a ‘Boot Manager’ window. Make sure to select WipeDrive Enterprise otherwise the computer will boot back into Windows.

Press **‘Enter’** to continue.

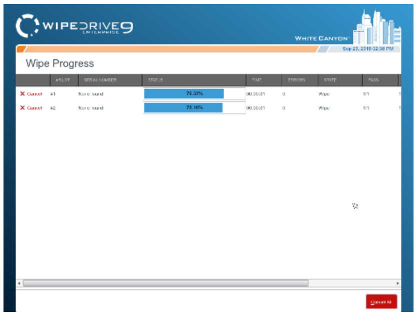


```
                         Windows Boot Manager

Choose an operating system to start, or press TAB to select a tool:
(Use the arrow keys to highlight your choice, then press ENTER.)

    WipeDrive Enterprise
    Windows 7



Seconds until the highlighted choice will be started automatically: 9


Tools:

    Windows Memory Diagnostic


 ENTER=Choose                TAB=Menu                        ESC=Cancel
```

Step 10

At this point WipeDrive will immediately begin wiping the drive(s) selected during setup.

This screen will provide some useful information such as 'Time Remaining' and if any disk errors are detected.



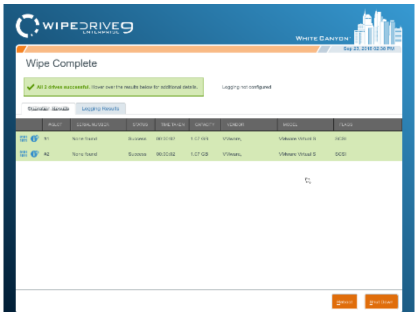
Wipe Progress

	#SLOT	SERIAL NUMBER	STATUS	TIME	ERRORS	STATE	PASS
✕ Cancel	#1	None found	79.32%	00:00:01	0	Wipe	1/1
✕ Cancel	#2	None found	78.10%	00:00:01	0	Wipe	1/1

Step 11

After WipeDrive finishes it will display a screen stating whether or not the hard drive was successfully overwritten as well as logging results.

This concludes the WipeDrive process, you can now click either '**Reboot**' to restart the computer and reinstall an operating system. Or choose '**Shut Down**' to turn the computer off.



Wipe Complete

✓ All 2 drives successful. Hover over the results below for additional details.

Logging not configured

	#SLOT	SERIAL NUMBER	STATUS	TIME TAKEN	CAPACITY	VENDOR	MODEL	FLAGS
	#1	None found	Success	00:00:02	1.07 GB	VMware,	VMware Virtual S	SCSI
	#2	None found	Success	00:00:02	1.07 GB	VMware,	VMware Virtual S	SCSI

Overwrite Patterns

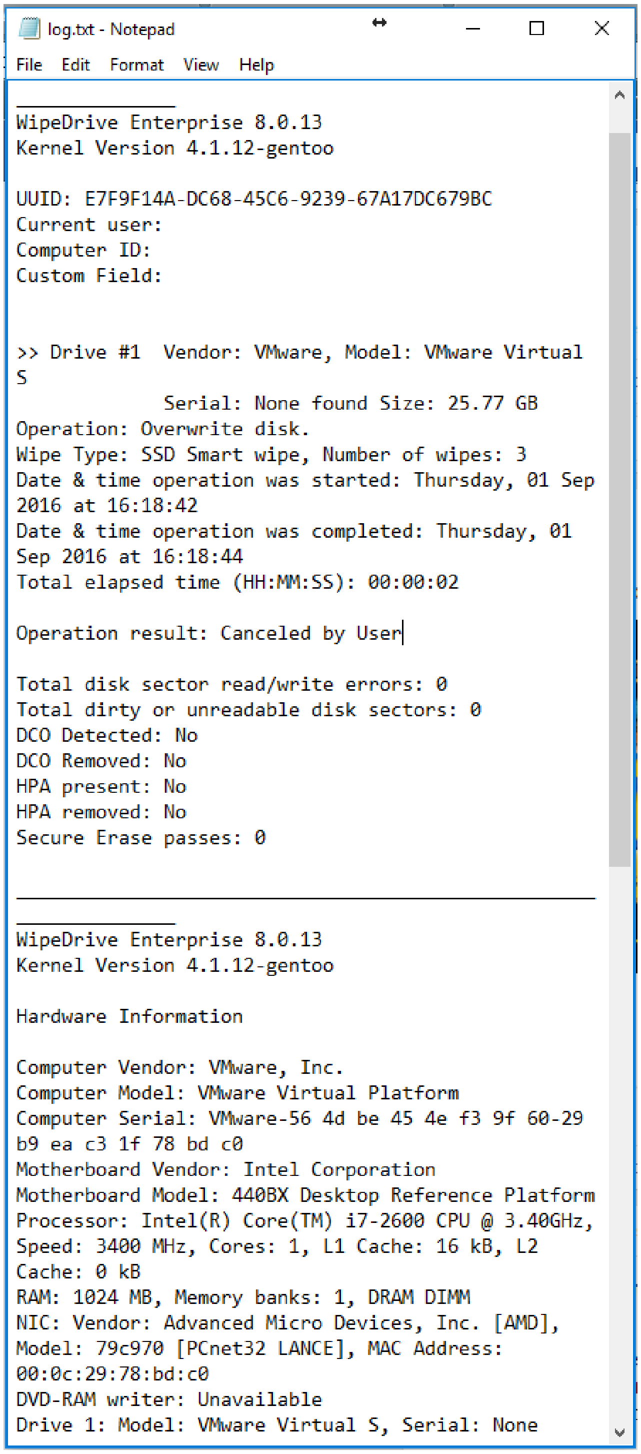
WipeDrive Enterprise provides specific overwrite patterns in compliance with various government agencies. The supported overwrite patterns are listed and described in detail below:

- Standard Single Pass - One overwrite (0's)
- SSD Smarter Wipe – Three overwrites. (0's, specialized pattern designed for SSD's, 0's)
- DoD 5220.22-M - Three overwrites with one verification. (0's, 1's, Random)
- DoD 5220.22-M - Seven overwrites. (0's, 1's, Random)
- HMG IS5 Baseline - One overwrite with verification. (0's)
- HMG IS5 Enhanced - Three overwrites with verification. (0's, 1's, Random)
- Canadian OPS-II - Seven overwrites with verification. (0's, 1's, Random)
- Canadian CSEC ITSG-06 – Three overwrites with single end verification.
- US Army AR380-19 – Three overwrites with single end verification.
- US AFSSI 5020 – Three overwrites with single end verification.
- US AFSSI 8580 – Eighteen overwrites.
- German VSITR - Seven overwrites.
- NAVSO P-5239-26 - Three overwrites with verification.
- NCSC-TG-025 - Three overwrites with verification.
- Russian GOST P50739-95 version 2 – One overwrite.
- Australian DSD ACSI-33 (XO-PD) - Three overwrites with two verifications.
- SecureErase + 1 overwrite with verify or NNSA NAP 15.1-C – Two overwrites with single end verification. (0's and 1's)
- BSI-2011-VS – Two overwrites with two verifications.
- NIST 800-88 – Meets NIST requirements and changes depending on the hardware.
- Custom Overwrite - User defined overwrite pattern.

Log Format Types

PLAIN TEXT LOG FILE OPTION

WipeDrive by default uses a plain text file format which can be saved to any destination option. A sample plain text log file is shown below:



```
______________
WipeDrive Enterprise 8.0.13
Kernel Version 4.1.12-gentoo

UUID: E7F9F14A-DC68-45C6-9239-67A17DC679BC
Current user:
Computer ID:
Custom Field:


>> Drive #1  Vendor: VMware, Model: VMware Virtual
S
             Serial: None found Size: 25.77 GB
Operation: Overwrite disk.
Wipe Type: SSD Smart wipe, Number of wipes: 3
Date & time operation was started: Thursday, 01 Sep
2016 at 16:18:42
Date & time operation was completed: Thursday, 01
Sep 2016 at 16:18:44
Total elapsed time (HH:MM:SS): 00:00:02

Operation result: Canceled by User

Total disk sector read/write errors: 0
Total dirty or unreadable disk sectors: 0
DCO Detected: No
DCO Removed: No
HPA present: No
HPA removed: No
Secure Erase passes: 0


___________________________________________________
______________
WipeDrive Enterprise 8.0.13
Kernel Version 4.1.12-gentoo

Hardware Information

Computer Vendor: VMware, Inc.
Computer Model: VMware Virtual Platform
Computer Serial: VMware-56 4d be 45 4e f3 9f 60-29
b9 ea c3 1f 78 bd c0
Motherboard Vendor: Intel Corporation
Motherboard Model: 440BX Desktop Reference Platform
Processor: Intel(R) Core(TM) i7-2600 CPU @ 3.40GHz,
Speed: 3400 MHz, Cores: 1, L1 Cache: 16 kB, L2
Cache: 0 kB
RAM: 1024 MB, Memory banks: 1, DRAM DIMM
NIC: Vendor: Advanced Micro Devices, Inc. [AMD],
Model: 79c970 [PCnet32 LANCE], MAC Address:
00:0c:29:78:bd:c0
DVD-RAM writer: Unavailable
Drive 1: Model: VMware Virtual S, Serial: None
```

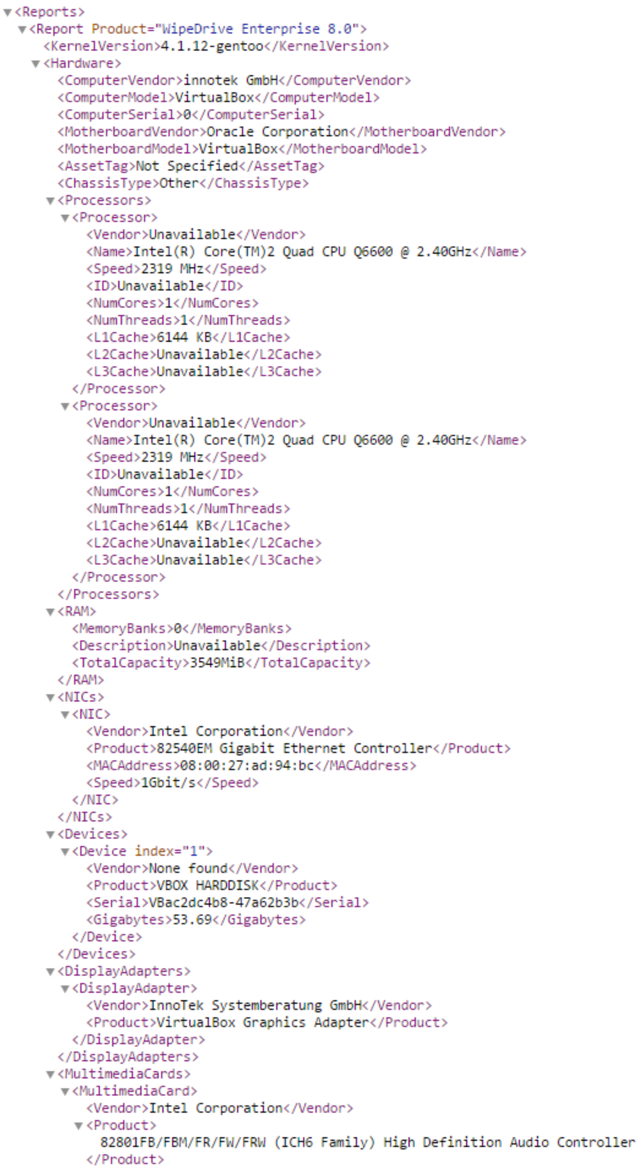
The text file records the following:

- Drive information
  - VENDOR
  - MODEL
  - SERIAL NUMBER
  - DRIVE SIZE
- Settings
  - User (Only applies when username prompting is selected in 'Settings')
  - Computer ID (Only applies when Computer ID prompting is selected in 'Settings')
  - Custom Field (Only applied when custom fields are created in 'Settings')
- Wiping Method
  - Operation (Either overwrite or verify)
  - Wipe Type
  - Number of wipes
- Dates and Time
  - Date & Time operation started
  - Date & Time operation finished
  - Total elapsed time
  - Result of operation
- Hard Drive Results
  - Total disk sector read/write errors
  - Total dirty/unreadable disk sectors
  - DCO Detected (Yes or No)
  - DCO Removed
  - HPA Present (Yes or No)
  - HPA Removed
  - AMAX Detected (Yes or No)
  - AMAX Removed
  - Secure Erase Utilized
  - NIST Method Type (Purge, Clear, or Unknown)

EXTENSIBLE MARKUP LANGUAGE (XML) LOG FILE OPTION

WipeDrive Enterprise can create an XML log file, which is a one page certificate detailing the system hardware and wipe process. The log file type can be changed under 'Settings.'

A sample XML file is shown below:



```
▼<Reports>
  ▼<Report Product="WipeDrive Enterprise 8.0">
     <KernelVersion>4.1.12-gentoo</KernelVersion>
   ▼<Hardware>
       <ComputerVendor>innotek GmbH</ComputerVendor>
       <ComputerModel>VirtualBox</ComputerModel>
       <ComputerSerial>0</ComputerSerial>
       <MotherboardVendor>Oracle Corporation</MotherboardVendor>
       <MotherboardModel>VirtualBox</MotherboardModel>
       <AssetTag>Not Specified</AssetTag>
       <ChassisType>Other</ChassisType>
     ▼<Processors>
       ▼<Processor>
           <Vendor>Unavailable</Vendor>
           <Name>Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GHz</Name>
           <Speed>2319 MHz</Speed>
           <ID>Unavailable</ID>
           <NumCores>1</NumCores>
           <NumThreads>1</NumThreads>
           <L1Cache>6144 KB</L1Cache>
           <L2Cache>Unavailable</L2Cache>
           <L3Cache>Unavailable</L3Cache>
         </Processor>
       ▼<Processor>
           <Vendor>Unavailable</Vendor>
           <Name>Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GHz</Name>
           <Speed>2319 MHz</Speed>
           <ID>Unavailable</ID>
           <NumCores>1</NumCores>
           <NumThreads>1</NumThreads>
           <L1Cache>6144 KB</L1Cache>
           <L2Cache>Unavailable</L2Cache>
           <L3Cache>Unavailable</L3Cache>
         </Processor>
       </Processors>
     ▼<RAM>
         <MemoryBanks>0</MemoryBanks>
         <Description>Unavailable</Description>
         <TotalCapacity>3549MiB</TotalCapacity>
       </RAM>
     ▼<NICs>
       ▼<NIC>
           <Vendor>Intel Corporation</Vendor>
           <Product>82540EM Gigabit Ethernet Controller</Product>
           <MACAddress>08:00:27:ad:94:bc</MACAddress>
           <Speed>1Gbit/s</Speed>
         </NIC>
       </NICs>
     ▼<Devices>
       ▼<Device index="1">
           <Vendor>None found</Vendor>
           <Product>VBOX HARDDISK</Product>
           <Serial>VBac2dc4b8-47a62b3b</Serial>
           <Gigabytes>53.69</Gigabytes>
         </Device>
       </Devices>
     ▼<DisplayAdapters>
       ▼<DisplayAdapter>
           <Vendor>InnoTek Systemberatung GmbH</Vendor>
           <Product>VirtualBox Graphics Adapter</Product>
         </DisplayAdapter>
       </DisplayAdapters>
     ▼<MultimediaCards>
       ▼<MultimediaCard>
           <Vendor>Intel Corporation</Vendor>
         ▼<Product>
             82801FB/FBM/FR/FW/FRW (ICH6 Family) High Definition Audio Controller
           </Product>
```

The XML log file contains the following information if applicable:

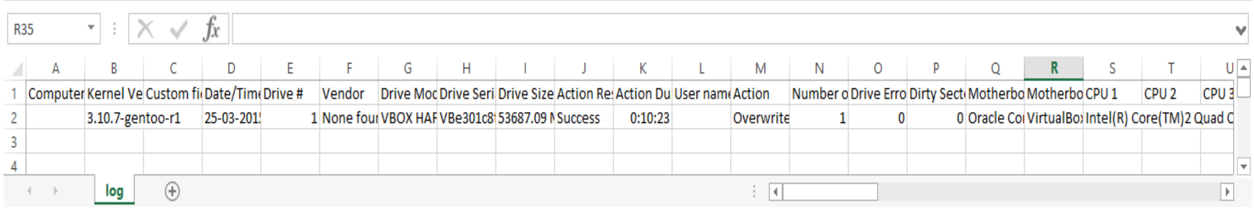
- Hardware Information
  - Computer Vendor
  - Computer Model
  - Computer Serial Number
  - Motherboard Vendor

  - Motherboard Model
  - Asset Tag
  - Chassis Type
  - Processor
  - RAM
  - NIC
  - Hard Drive
  - Display Adapter
  - Storage Controller
  - Number of USB, USB2, and USB3 ports
  - Number of Firewire Ports
  - Number of Thunderbolt, Thunderbolt2, and Thunderbolt3 Ports
- Wipe Information
  - Target Drive Index
  - Username (Only applies if Username prompt is selected under ‘Settings.’)
  - Computer ID (Only applies if Computer ID prompt is selected under ‘Settings.’)
  - Custom Field (Only applied if custom fields are created under ‘Settings.’)
  - Wipe Method
  - Wipe Method Value
  - Start Time
  - Wipe Duration
  - Time Operation Began
  - Result of Operation
  - Dirty Sectors
  - Drive Errors Detected
  - DCO Locked (Yes or No)
  - DCO Found (Yes or No)
  - DCO Removed
  - HPA Found (Yes or No)
  - HPA Removed
  - Accessible Max Address (AMAX) Found (Yes or No)
  - AMAX Removed
  - Security Locked
  - Security Frozen
  - Wipe Passes
  - Number of Secure Erase Passes
  - Number of Passes Sanitize Device—Crypto Erase

  - Number of Passes Sanitize Device—Block Erase
  - Number of Passes Sanitize Device—Overwrite
  - Number of passes Opal Crypto Erase
  - Sectors Overwritten
  - Sectors Not Overwritten
  - Sectors Verified
  - NIST Method Type
  - NIST Required Type
  - NIST Reason for Method Type
  - Manufacturer of Hard Drive
  - Drive Model
  - Drive Serial Number
  - Hard Drive Size
  - Is drive SSD
  - Drive Media Type
  - Pre-wipe SMART Status
  - Post-wipe SMART Status

COMMA DELIMITED (CSV) LOG FILE OPTION

A sample CSV file is shown below:



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
1	Computer	Kernel Ve	Custom fi	Date/Time	Drive #	Vendor	Drive Moc	Drive Seri	Drive Size	Action Re:	Action Du	User name	Action	Number o	Drive Erro	Dirty Secti	Motherbo	Motherbo	CPU 1	CPU 2	CPU 3
2		3.10.7-gentoo-r1		25-03-201!	1	None four	VBOX HAF	VBe301c8!	53687.09 N	Success	0:10:23		Overwrite	1	0	0	Oracle Coı	VirtualBo:	Intel(R) Core(TM)2 Quad C		
3																					
4																					

The purpose of the .csv file is to allow logs created by WipeDrive Enterprise to be easily imported into a database or spreadsheet. The following are details about the operation included in the comma delimited file:

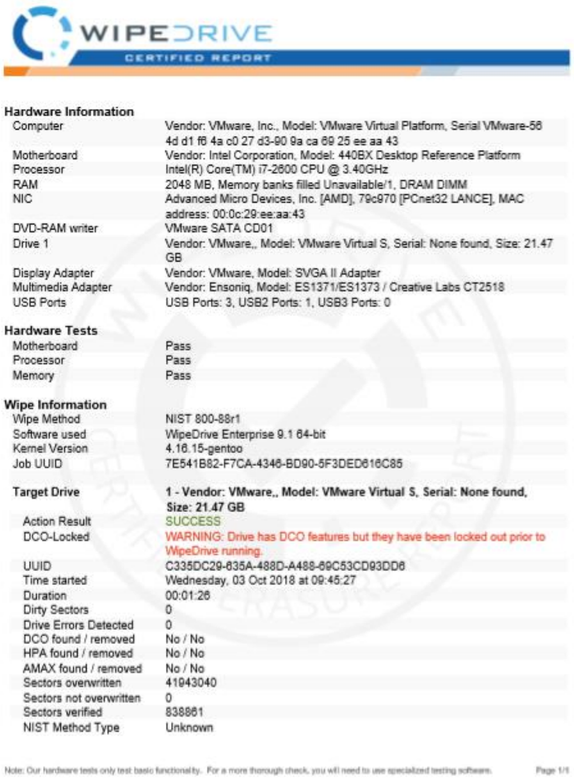
- Hard Drive Information
  - Computer ID
  - Date & Time
  - Drive Number
  - Drive Model
  - Drive Serial

  - Drive Size
- Operation Results
  - Action Result
  - Action Duration
  - Action Start Time
  - Action End Time
  - Username
  - Action
  - Number of Wipes
  - Detected Drive Errors
  - Dirty Sectors
  - Sectors Overwritten
  - Sectors Not Overwritten
  - Sectors Verified
  - Secure Erase Passes
  - Secure Erase Enhanced Passes
  - Sanitize Crypto Erase Passes
  - Sanitize Block Erase Passes
  - Sanitize Overwrite Passes
  - NIST Method Type
  - Opal Crypto Erase Passes
- Hardware Information
  - Motherboard Vendor
  - Motherboard Product
  - CPU (Will include all CPUs present)
  - RAM
  - NIC
  - Optical Drive
  - Hard Drive(s)
  - Video Card
  - Multimedia Card
  - Number of USB, USB2 and USB3 ports
- Computer Information
  - Computer Vendor
  - Computer Model
  - Computer Serial

- Hard Drive Security Features
    - HPA Detected
    - HPA Removed
    - DCO-Locked
    - DCO Detected
    - DCO Removed
    - AMAX Detected
    - AMAX Removed
    - User Number
    - Username

PDF LOG FILE OPTION

WipeDrive includes the option to log a report in PDF format which can be saved to any destination option. An example can be seen below:



WIPEDRIVE
CERTIFIED REPORT

Hardware Information

Computer	Vendor: VMware, Inc., Model: VMware Virtual Platform, Serial VMware-56 4d d1 f6 4a c0 27 d3-90 9a ca 69 25 ee aa 43
Motherboard	Vendor: Intel Corporation, Model: 440BX Desktop Reference Platform
Processor	Intel(R) Core(TM) i7-2600 CPU @ 3.40GHz
RAM	2048 MB, Memory banks filled Unavailable/1, DRAM DIMM
NIC	Advanced Micro Devices, Inc. [AMD], 79c970 [PCnet32 LANCE], MAC address: 00:0c:29:ee:aa:43
DVD-RAM writer	VMware SATA CD01
Drive 1	Vendor: VMware,, Model: VMware Virtual S, Serial: None found, Size: 21.47 GB
Display Adapter	Vendor: VMware, Model: SVGA II Adapter
Multimedia Adapter	Vendor: Ensoniq, Model: ES1371/ES1373 / Creative Labs CT2518
USB Ports	USB Ports: 3, USB2 Ports: 1, USB3 Ports: 0

Hardware Tests

Motherboard	Pass
Processor	Pass
Memory	Pass

Wipe Information

Wipe Method	NIST 800-88r1
Software used	WipeDrive Enterprise 9.1 64-bit
Kernel Version	4.16.15-gentoo
Job UUID	7E541B82-F7CA-4346-BD90-5F3DED616C85
Target Drive	**1 - Vendor: VMware,, Model: VMware Virtual S, Serial: None found, Size: 21.47 GB**
Action Result	SUCCESS
DCO-Locked	WARNING: Drive has DCO features but they have been locked out prior to WipeDrive running.
UUID	C335DC29-635A-488D-A488-69C53CD93DD6
Time started	Wednesday, 03 Oct 2018 at 09:45:27
Duration	00:01:26
Dirty Sectors	0
Drive Errors Detected	0
DCO found / removed	No / No
HPA found / removed	No / No
AMAX found / removed	No / No
Sectors overwritten	41943040
Sectors not overwritten	0
Sectors verified	838861
NIST Method Type	Unknown

Note: Our hardware tests only test basic functionality. For a more thorough check, you will need to use specialized testing software. Page 1/1

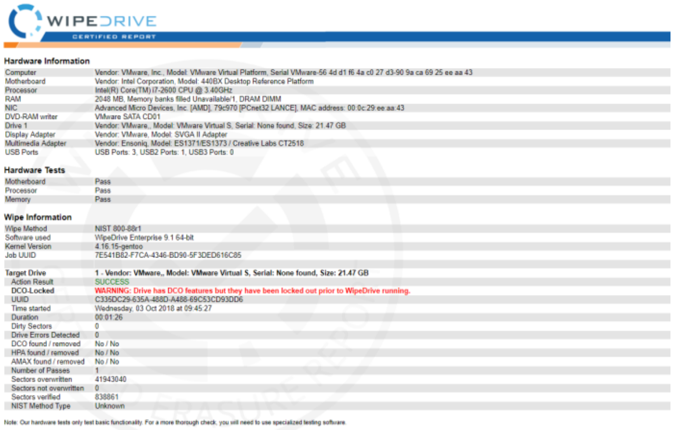
This report includes the following details:

- Hardware Information
  - Computer Vendor
  - Computer Model
  - Computer Serial
  - Motherboard Vendor
  - Motherboard Model
  - Processor
  - RAM
  - NIC
  - Which includes: Vendor and Mac Address
  - DVD Writer
  - Drive(s)
  - Which includes: Vendor, Product, Serial, and Size

  - Display Adapter
  - Multimedia Adapter
  - USB Ports
- Wipe Information
  - Software Version
  - Target Drive
  - Wipe Method
  - Action Result
  - Time
  - Duration
  - Vendor
  - Drive Model
  - Drive Serial
  - Drive Size
  - Dirty Sectors
  - Drive Errors Detected
  - DCO Found
  - DCO Removed
  - HPA Found
  - HPA Removed
  - AMAX Detected
  - AMAX Removed
  - Secure Erase Passes (if applicable)
  - Secure Erase Enhanced Passes (if applicable)
  - Sanitize Crypto Erase Passes (if applicable)
  - Sanitize Block Erase Passes (if applicable)
  - Sanitize Overwrite Passes (if applicable)
  - Opal Crypto Erase Passes (if applicable)
  - NIST Method Type

HTML LOG FILE OPTION

WipeDrive includes the option to log a report in HTML format which can be saved to any destination option. An example can be seen below:



WIPEDRIVE
CERTIFIED REPORT

Hardware Information

Computer	Vendor: VMware, Inc., Model: VMware Virtual Platform, Serial VMware-56 4d d1 f6 4a c0 27 d3-90 9a ca 69 25 ee aa 43
Motherboard	Vendor: Intel Corporation, Model: 440BX Desktop Reference Platform
Processor	Intel(R) Core(TM) i7-2600 CPU @ 3.40GHz
RAM	2048 MB, Memory banks filled Unavailable/1, DRAM DIMM
NIC	Advanced Micro Devices, Inc. [AMD], 79c970 [PCnet32 LANCE], MAC address: 00:0c:29:ee:aa:43
DVD-RAM writer	VMware SATA CD01
Drive 1	Vendor: VMware,, Model: VMware Virtual S, Serial: None found, Size: 21.47 GB
Display Adapter	Vendor: VMware, Model: SVGA II Adapter
Multimedia Adapter	Vendor: Ensoniq, Model: ES1371/ES1373 / Creative Labs CT2518
USB Ports	USB Ports: 3, USB2 Ports: 1, USB3 Ports: 0

Hardware Tests

Motherboard	Pass
Processor	Pass
Memory	Pass

Wipe Information

Wipe Method	NIST 800-88r1
Software used	WipeDrive Enterprise 9.1 64-bit
Kernel Version	4.16.15-gentoo
Job UUID	7E541B82-F7CA-4346-BD90-5F3DED616C85
Target Drive	**1 - Vendor: VMware,, Model: VMware Virtual S, Serial: None found, Size: 21.47 GB**
Action Result	SUCCESS
DCO-Locked	**WARNING: Drive has DCO features but they have been locked out prior to WipeDrive running.**
UUID	C335DC29-635A-488D-A488-69C53CD93DD6
Time started	Wednesday, 03 Oct 2018 at 09:45:27
Duration	00:01:26
Dirty Sectors	0
Drive Errors Detected	0
DCO found / removed	No / No
HPA found / removed	No / No
AMAX found / removed	No / No
Number of Passes	1
Sectors overwritten	41943040
Sectors not overwritten	0
Sectors verified	838861
NIST Method Type	Unknown

Note: Our hardware tests only test basic functionality. For a more thorough check, you will need to use specialized testing software.

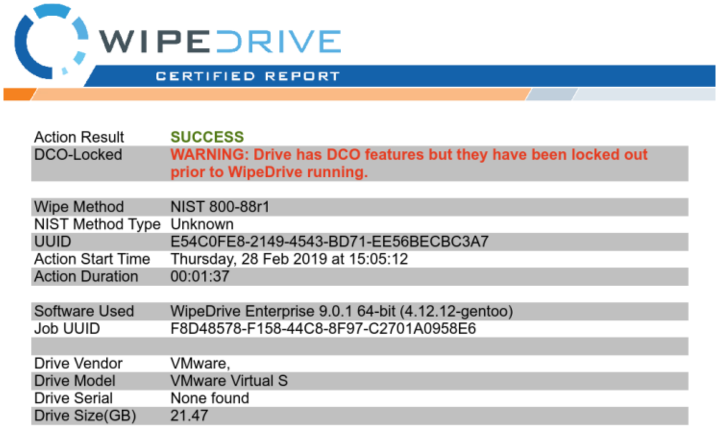
This report includes the following details:

- Hardware Information
  - Computer Vendor
  - Computer Model
  - Computer Serial
  - Motherboard Vendor
  - Motherboard Model
  - Processor
  - RAM
  - NIC
  - Which includes: Vendor and Mac Address
  - DVD Writer
  - Drive(s)
  - Which includes: Vendor, Product, Serial, and Size
  - Display Adapter
  - Multimedia Adapter
  - USB Ports
- Wipe Information
  - Software Version
  - Target Drive
  - Wipe Method
  - Action Result
  - Time

- Duration
- Vendor
- Drive Model
- Drive Serial
- Drive Size
- Dirty Sectors
- Drive Errors Detected
- DCO Found
- DCO Removed
- HPA Found
- HPA Removed
- AMAX Detected
- AMAX Removed
- Secure Erase Passes (if applicable)
- Secure Erase Enhanced Passes (if applicable)
- Sanitize Crypto Erase Passes (if applicable)
- Sanitize Block Erase Passes (if applicable)
- Sanitize Overwrite Passes (if applicable)
- Opal Crypto Erase Passes (if applicable)

BOOTABLE REPORT

WipeDrive includes the option to log a bootable report to the hard drive. The report is then accessed by booting to the hard drive itself.



Action Result	**SUCCESS**
DCO-Locked	**WARNING: Drive has DCO features but they have been locked out prior to WipeDrive running.**
Wipe Method	NIST 800-88r1
NIST Method Type	Unknown
UUID	E54C0FE8-2149-4543-BD71-EE56BECBC3A7
Action Start Time	Thursday, 28 Feb 2019 at 15:05:12
Action Duration	00:01:37
Software Used	WipeDrive Enterprise 9.0.1 64-bit (4.12.12-gentoo)
Job UUID	F8D48578-F158-44C8-8F97-C2701A0958E6
Drive Vendor	VMware,
Drive Model	VMware Virtual S
Drive Serial	None found
Drive Size(GB)	21.47

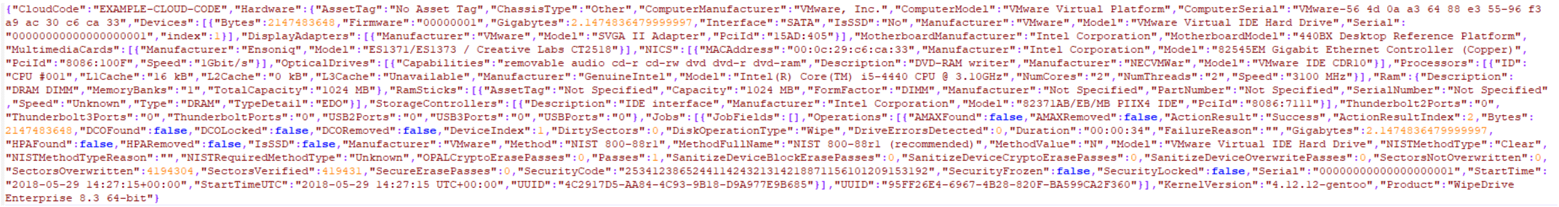
This report includes the following details:

- Wipe Information
  - Software Version
  - Target Drive
  - Wipe Method
  - Action Result
  - Time
  - Duration
  - Drive Vendor
  - Drive Model
  - Drive Serial
  - Drive Size
  - Dirty Sectors
  - Drive Errors Detected
  - DCO Found
  - DCO Removed
  - HPA Found
  - HPA Removed
  - Secure Erase Passes (if applicable)
  - Secure Erase Enhanced Passes (if applicable)

- Sanitize Crypto Erase Passes (if applicable)
- Sanitize Block Erase Passes (if applicable)
- Sanitize Overwrite Passes (if applicable)
- Opal Crypto Erase Passes (if applicable)

JSON

WipeDrive includes the option to log a JSON file.



```
{"CloudCode":"EXAMPLE-CLOUD-CODE","Hardware":{"AssetTag":"No Asset Tag","ChassisType":"Other","ComputerManufacturer":"VMware, Inc.","ComputerModel":"VMware Virtual Platform","ComputerSerial":"VMware-56 4d 0a a3 64 88 e3 55-96 f3
a9 ac 30 c6 ca 33","Devices":[{"Bytes":2147483648,"Firmware":"00000001","Gigabytes":2.1474836479999997,"Interface":"SATA","IsSSD":"No","Manufacturer":"VMware","Model":"VMware Virtual IDE Hard Drive","Serial":
"00000000000000000001","index":1}],"DisplayAdapters":[{"Manufacturer":"VMware","Model":"SVGA II Adapter","PciId":"15AD:405"}],"MotherboardManufacturer":"Intel Corporation","MotherboardModel":"440BX Desktop Reference Platform",
"MultimediaCards":[{"Manufacturer":"Ensoniq","Model":"ES1371/ES1373 / Creative Labs CT2518"}],"NICS":[{"MACAddress":"00:0c:29:c6:ca:33","Manufacturer":"Intel Corporation","Model":"82545EM Gigabit Ethernet Controller (Copper)",
"PciId":"8086:100F","Speed":"1Gbit/s"}],"OpticalDrives":[{"Capabilities":"removable audio cd-r cd-rw dvd dvd-r dvd-ram","Description":"DVD-RAM writer","Manufacturer":"NECVMWar","Model":"VMware IDE CDR10"}],"Processors":[{"ID":
"CPU #001","L1Cache":"16 kB","L2Cache":"0 kB","L3Cache":"Unavailable","Manufacturer":"GenuineIntel","Model":"Intel(R) Core(TM) i5-4440 CPU @ 3.10GHz","NumCores":"2","NumThreads":"2","Speed":"3100 MHz"}],"Ram":{"Description":
"DRAM DIMM","MemoryBanks":"1","TotalCapacity":"1024 MB"},"RamSticks":[{"AssetTag":"Not Specified","Capacity":"1024 MB","FormFactor":"DIMM","Manufacturer":"Not Specified","PartNumber":"Not Specified","SerialNumber":"Not Specified"
,"Speed":"Unknown","Type":"DRAM","TypeDetail":"EDO"}],"StorageControllers":[{"Description":"IDE interface","Manufacturer":"Intel Corporation","Model":"82371AB/EB/MB PIIX4 IDE","PciId":"8086:7111"}],"Thunderbolt2Ports":"0",
"Thunderbolt3Ports":"0","ThunderboltPorts":"0","USB2Ports":"0","USB3Ports":"0","USBPorts":"0"},"Jobs":[{"JobFields":[],"Operations":[{"AMAXFound":false,"AMAXRemoved":false,"ActionResult":"Success","ActionResultIndex":2,"Bytes":
2147483648,"DCOFound":false,"DCOLocked":false,"DCORemoved":false,"DeviceIndex":1,"DirtySectors":0,"DiskOperationType":"Wipe","DriveErrorsDetected":0,"Duration":"00:00:34","FailureReason":"","Gigabytes":2.1474836479999997,
"HPAFound":false,"HPARemoved":false,"IsSSD":false,"Manufacturer":"VMware","Method":"NIST 800-88r1","MethodFullName":"NIST 800-88r1 (recommended)","MethodValue":"N","Model":"VMware Virtual IDE Hard Drive","NISTMethodType":"Clear",
"NISTMethodTypeReason":"","NISTRequiredMethodType":"Unknown","OPALCryptoErasePasses":0,"Passes":1,"SanitizeDeviceBlockErasePasses":0,"SanitizeDeviceCryptoErasePasses":0,"SanitizeDeviceOverwritePasses":0,"SectorsNotOverwritten":0,
"SectorsOverwritten":4194304,"SectorsVerified":419431,"SecureErasePasses":0,"SecurityCode":"253412386524411424321314218871156101209153192","SecurityFrozen":false,"SecurityLocked":false,"Serial":"00000000000000000001","StartTime":
"2018-05-29 14:27:15+00:00","StartTimeUTC":"2018-05-29 14:27:15 UTC+00:00","UUID":"4C2917D5-AA84-4C93-9B18-D9A977E9B685"}],"UUID":"95FF26E4-6967-4B28-820F-BA599CA2F360"}],"KernelVersion":"4.12.12-gentoo","Product":"WipeDrive
Enterprise 8.3 64-bit"}
```

This report includes the following details:

- Hard Drive Information
  - Date & Time
  - Drive Model
  - Drive Serial
  - Drive Size
- Operation Results
  - Action Result
  - Action Duration
  - Action Start Time
  - Username
  - Action
  - Number of Wipes
  - Detected Drive Errors
  - Dirty Sectors
- Hardware Information
  - Motherboard Vendor
  - Motherboard Product
  - CPU (Will include all CPUs present)
  - RAM
  - NIC

  - Optical Drive
  - Hard Drive(s)
  - Video Card
  - Multimedia Card
  - Number of USB, USB2, and USB3 ports
  - Number of Thunderbolt, Thunderbolt2, and Thunderbolt3 ports
- Computer Information
  - Computer Vendor
  - Computer Model
  - Computer Serial
- Hard Drive Security Features
  - HPA Detected
  - HPA Removed
  - DCO Detected
  - DCO Locked
  - DCO Removed
  - AMAX Detected
  - AMAX Removed
  - User Number
  - Username
  - Secure Erase Passes (if applicable)
  - Secure Erase Enhanced Passes (if applicable)
  - Sanitize Crypto Erase Passes (if applicable)
  - Sanitize Block Erase Passes (if applicable)
  - Sanitize Overwrite Passes (if applicable)
  - Opal Crypto Erase Passes (if applicable)

Audit Log Destination Options

USB DRIVE OPTION

Any log file type can be sent to a USB drive connected to the wipe machine. The USB drive must meet the following criteria:

1. The USB size must be less than 16 GB otherwise WipeDrive see it as an external HDD.
2. Formatted in Fat 32.
3. The USB drive must be formatted and connected prior to booting into WipeDrive.

LOCAL FILE SYSTEM OPTION

WipeDrive Enterprise will write any of the log file types to a local location on the current machine. This option requires the user to designate the file system location within the Linux kernel.

Warning: Files saved to the local file system can only be stored there temporarily. The local file system will be erased when the system is turned off.

NETWORK FILE SYSTEM OPTION

WipeDrive Enterprise will write any of the log file types to a location on the local network. This log option requires a network connection for the PC and permission to access the designated folder. It also needs the following information:

1. Protocol – Samba/ FTP
2. Server Name
3. User Name
4. Password
5. Path

EMAIL OPTION

WipeDrive Enterprise will send any of the log file types to a specific email address. This log location requires the following information:

1. Server Name
2. From
3. To
4. CC
5. SMTP Username
6. SMTP Password

MYSQL/MS SQL AUDIT LOGGING OPTION

WipeDrive Enterprise will send any of the log file types to a MYSQL or MS SQL database. More information can be found under Addendum 1. This log location requires the following information:

1. Host
2. Database
3. Username
4. Password

Addendum 1 - Setting Up SQL Logging

System Requirements (Server)

- MySQL Server 5.0 (or newer)
- MS SQL Server 2008 (or newer)
- Any operating system that supports a MySQL/MS SQL installation

System Requirements (Workstation/Client)

- Windows Vista SP2, or 7, 8, 8.1, 10
- .NET Framework 4.5.2

Preparation

Before the database can be initialized, you will need to create a new blank database. This step must be performed by hand. For security purposes, it is also highly recommended to create a new user who only has access to this database. Please consult the MySQL/MS SQL documentation or your systems administrator if you need assistance creating the database or new user.

Initialization

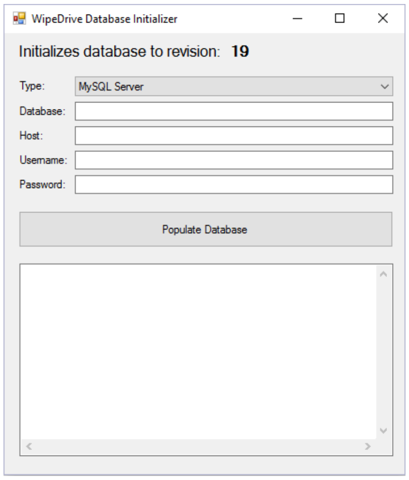
Once the database has been created, launch the WipeDrive Database Initializer.

Please fill in all provided fields:

1. **Database Name:** The name of the newly created database.
2. **Host:** The machine hosting the SQL database. This can be either an IP address or a DNS hostname.
3. **Username:** The name of a SQL user that has sufficient privileges to create tables in the database you just created.
4. **Password:** The password for above username.

Click the ‘Populate Database’ button to complete initialization of the database. If there are any errors during the initialization process, the program will display a message box with debugging information.

Once complete the server is configured for use with WipeDrive Enterprise.



Initializes database to revision: **19**

Type: MySQL Server

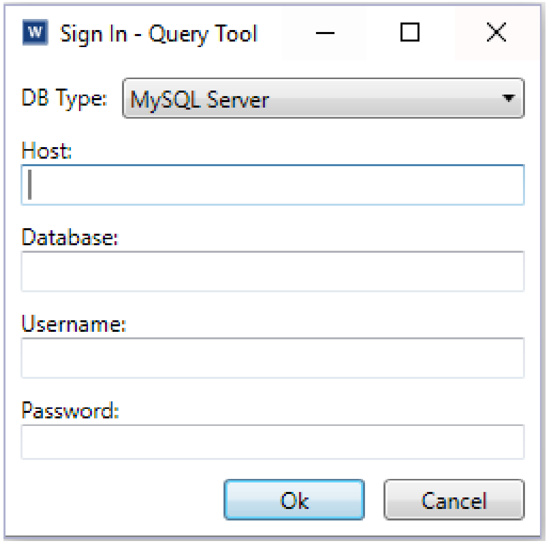
SQL Database Viewer (Audit Tool)

The SQL database viewing utility, herein known as the Audit Tool, is used to view the audit logs created by WipeDrive when used in conjunction with a SQL database.

System Requirements

- Windows Vista Sp2, 7 (32-/64-bit compatible), 8, 8.1, 10
- .NET Framework 4.5.2

Basic Operation



DB Type: MySQL Server

To connect to the database you will need to provide the following details:

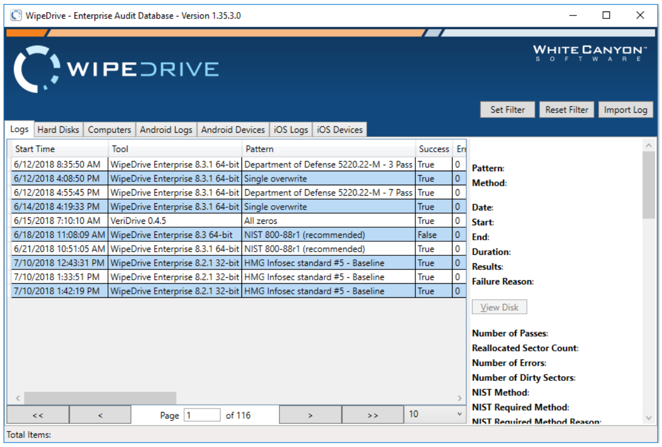
Host: The IP address or DNS hostname of the server hosting the SQL database.

Database: The name of the WipeDrive database.

Username: The user account with credentials allowing it to view the WipeDrive database.

Password: The password for the user account provided above.

Once successfully connected to the database, you will see the main UI appear that shows all of the logging operations that have been performed as well as their results. You are able to view which logs are connected to which drives as well as which computer hardware was used when wiping said drive. You can also import XML files by clicking on Import Log in the top right-hand corner then browsing for the XML you wish to import.



WipeDrive - Enterprise Audit Database - Version 1.35.3.0

Start Time	Tool	Pattern	Success	Er
6/12/2018 8:35:50 AM	WipeDrive Enterprise 8.3.1 64-bit	Department of Defense 5220.22-M - 3 Pass	True	0
6/12/2018 4:08:50 PM	WipeDrive Enterprise 8.3.1 64-bit	Single overwrite	True	0
6/12/2018 4:55:45 PM	WipeDrive Enterprise 8.3.1 64-bit	Department of Defense 5220.22-M - 7 Pass	True	0
6/14/2018 4:19:33 PM	WipeDrive Enterprise 8.3.1 64-bit	Single overwrite	True	0
6/15/2018 7:10:10 AM	VeriDrive 0.4.5	All zeros	True	0
6/18/2018 11:08:09 AM	WipeDrive Enterprise 8.3 64-bit	NIST 800-88r1 (recommended)	False	0
6/21/2018 10:51:05 AM	WipeDrive Enterprise 8.3.1 64-bit	NIST 800-88r1 (recommended)	True	0
7/10/2018 12:43:31 PM	WipeDrive Enterprise 8.2.1 32-bit	HMG Infosec standard #5 - Baseline	True	0
7/10/2018 1:33:51 PM	WipeDrive Enterprise 8.2.1 32-bit	HMG Infosec standard #5 - Baseline	True	0
7/10/2018 1:42:19 PM	WipeDrive Enterprise 8.2.1 32-bit	HMG Infosec standard #5 - Baseline	True	0

Page 1 of 116 10

Addendum 2 - Command Line Parameters

WipeDrive can be configured on the fly by passing in parameters from the command line using the optional parameters below. In order to access the command line, simply type 'exit' anytime within the GUI. When at the command prompt, typing 'wd_ui' with no parameters will start the standard GUI based WipeDrive program.

Command Line Usage:

Example setup: wd_ui --wipe-level=1 --disk=0 --log-directory=removable --log-file-types=x

This particular command tells WipeDrive to perform a Standard Overwrite on the first hard drive and to record an XML log to an attached USB drive.

Here is a list of commonly used command parameters.

WIPING AND VERIFYING

--wipe-level	Sets the default wipe level and disables the option for the user to choose a wipe level through the interface. (Values 1-9 and a-z) (1=single overwrite, 2=DoD 3-pass, i=SSD Smart Wipe, n= NIST 800-88r1, etc.)
--disk	Sets the selected disk to wipe. (Use -1 to wipe all drives)
--do-verify	Performs a full verification pass.

LOGGING

--log-directory	Path where log files will be saved.
--log-file-types	Log file(s) format (d=delimited, h=html, p=pdf, q=sql, r=regular, x=xml, etc.)
--username	User value, if no value is provided you will be prompted to enter one.
--computer-id	Computer ID value, if no value is provided you will be prompted to enter one.
--custom field	Custom field, if no value is provided you will be prompted to enter one.

LOGGING TO FTP

--ftp-server	FTP server name
--ftp-user	FTP username
--ftp-password	FTP password
--ftp-directory	Directory on the FTP server where the log files should be saved.

LOGGING TO EMAIL

--mail-server	Email server to use to email logs
--mail-from	Name of person email is from (note: root will be the sender)
--mail-to	Email address of log(s) recipient
--mail-cc	Additional address to email logs
--mail-password	Password of SMTP user (only specify if required by email server)
--mail-subject	Subject for email
--mail-usetls	Whether to use TLS (Transport Layer Security)

LOGGING TO SQL DATABASE

--db-host	Hostname of machine serving the database
--db-name	Name of the WipeDrive logging database
--db-username	Database username
--db-password	Database password

For a more complete list of any of the possible command line parameters, please contact our support team.

Addendum 3 – Drive Verification

Drive verification is done as part of a specific wipe pattern (i.e. DoD 5220.22-M) or as a stand-alone function.

When drive verification is performed, the disk is checked to certify that the drive is in one of three states:

1. The drive contains all binary 0’s
2. The drive contains all binary 1’s
3. The drive contains a repeated value (i.e. all a’s)
4. The drive contains random data*

If the drive is in one of the four states the verification will pass, if not the process will fail.

***Note:** WipeDrive uses a random pattern where two random characters are generated, followed by the bitwise compliments of those two bytes. In this way, it is possible to determine that the drive has been overwritten by random data by the WipeDrive program.

Addendum 4 – Log Field Explanation

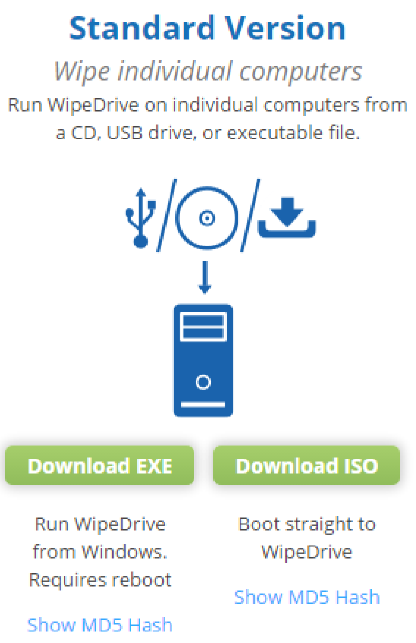
Below is a brief explanation of each log field that the software reports.

- Hardware Information
  - Computer Vendor – Lists the vendor of the computer.
  - Computer Model – Lists the model of the computer
  - Computer Serial Number – Lists the serial number of the computer
  - Motherboard Vendor – Lists the vendor of the motherboard
  - Motherboard Model – Lists the model of the motherboard
  - Asset Tag – Lists the asset tag (usually in place of the computer serial number)
  - Chassis Type – Lists the chassis type
  - Processor – Lists information about the processor (vendor, name, speed, etc.)
  - RAM – Lists information about the RAM (vendor, capacity, speed, etc.)
  - NIC – Lists information about the NIC (vendor, MAC Address, Speed, etc.)
  - Hard Drive – Lists information about each individual drive
  - Display Adapter – Lists information about the display adapter (vendor, product, PciID)
  - Multimedia Adapter – Lists information about multimedia cards (vendor and product)
  - Storage Controller – Lists information about the storage controller (vendor, product, etc.)
  - Number of USB, USB2, and USB3 ports – Lists the number of each type of USB port.
- Wipe Information
  - Number of Target Drive – Numbers each of the drives
  - Manufacturer of Hard Drive – Lists the manufacturer of each hard drive
  - Drive Model – Lists the model of each hard drive
  - Drive Serial Number – Lists the serial number of each hard drive
  - Hard Drive Size – Lists the size of each hard drive
  - Time Operation Began – States the time the wipe or verify began
  - Result of Operation – States the result of the operation (success, failure, or canceled by user)
  - Username (Only applies if Username prompt is selected under 'Settings.') – Lists the username
  - Computer ID (Only applies if Computer ID prompt is selected under 'Settings.') – Lists the computer ID
  - Custom Field (Only applied if custom fields are created under 'Settings.') – Lists the custom fields
  - Duration – States how long the operation lasted
  - Wipe Method – States the overwrite pattern used
  - Dirty Sectors – Lists the number of dirty sectors. Dirty sectors occur when a hard drive is failing but WipeDrive is still able to read/write to the drive.
  - Drive Errors Detected – Lists the number of drive errors. Drive errors occur when a hard drive is failing and WipeDrive is unable to read/write to the drive.

- HPA Found – States if a Host Protected Area was found at startup
- HPA removed – States if a Host Protected Area was removed
- DCO Found – States if a Device Configuration Overlay was found at startup
- DCO Removed – States if a Device Configuration Overlay was removed by WipeDrive
- DCO-Locked – States whether DCO commands are locked. If the commands are locked, DCOs may not be detected or removed.
- AMAX Detected – States if an Accessible Max Address was found at startup.
- AMAX Removed – States if an Accessible Max Address was removed.
- Secure Erase Passes – Lists the number of Secure Erase passes that occurred
- Secure Erase Enhanced Passes – Number of Secure Erase passes
- Sanitize Crypto Erase Passes – Number of Sanitize Crypto Erase passes
- Sanitize Block Erase Passes – Number of Sanitize Block Erase passes
- Sanitize Overwrite Passes – Number of Sanitize Overwrite passes
- Opal Crypto Erase Passes – Number of Opal Crypto Erase passes

Addendum 5 – MD5 Hash

To verify the validity and add to the security of files downloaded from WhiteCanyon, we have created MD5 Hash codes which will enable you to cross-check the downloads to ensure they are the legitimate, original files.



Standard Version

Wipe individual computers

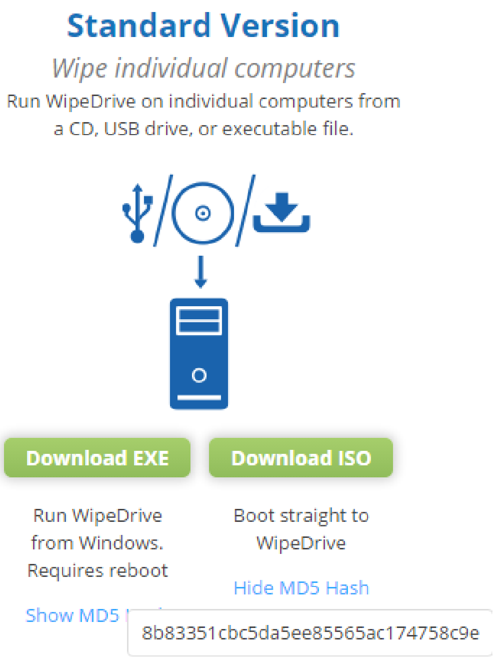
Run WipeDrive on individual computers from a CD, USB drive, or executable file.

Run WipeDrive from Windows. Requires reboot

Show MD5 Hash

Boot straight to WipeDrive

Show MD5 Hash



Standard Version

Wipe individual computers

Run WipeDrive on individual computers from a CD, USB drive, or executable file.

Run WipeDrive from Windows. Requires reboot

Show MD5

Boot straight to WipeDrive

Hide MD5 Hash

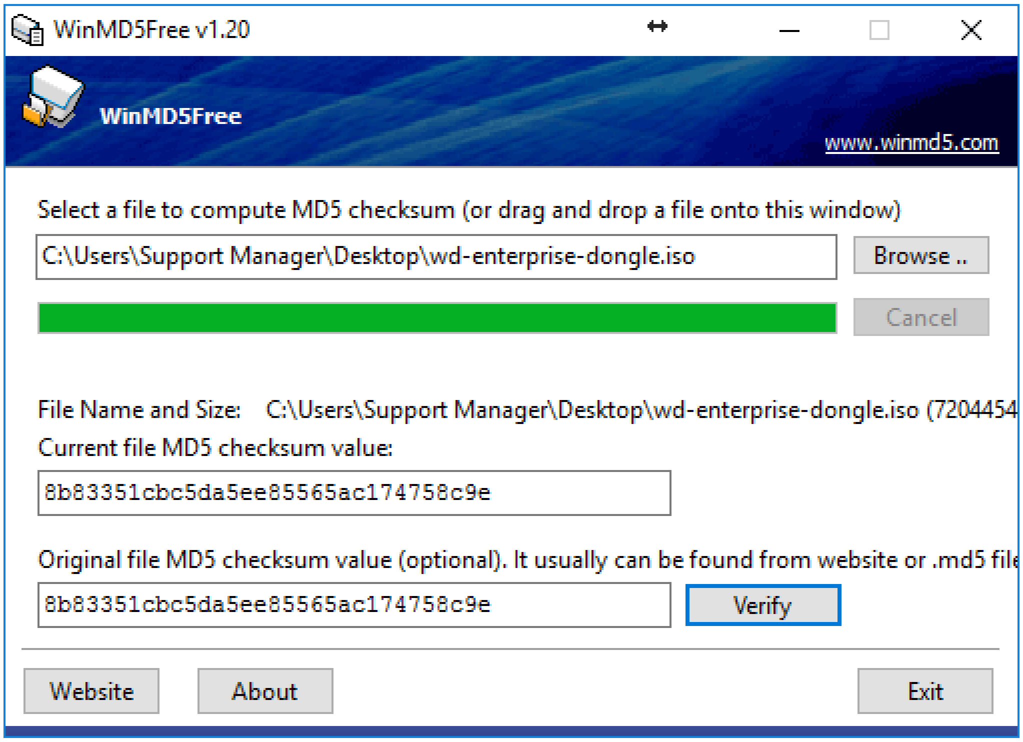
8b83351cbc5da5ee85565ac174758c9e

Below each file download, you will see a link that says "Show MD5 Hash." Clicking on that link below each file download will display the custom MD5 hash code for that file.

To cross-check our file with the MD5 hash, you will need to use a third-party software for verification. One such program is WinMD5Free found at http://www.winmd5.com/

After downloading the utility and extracting the zip file, run the executable.

It will display a screen like shown below:



Select a file to compute MD5 checksum (or drag and drop a file onto this window)

C:\Users\Support Manager\Desktop\wd-enterprise-dongle.iso

File Name and Size: C:\Users\Support Manager\Desktop\wd-enterprise-dongle.iso (7204454

Current file MD5 checksum value:

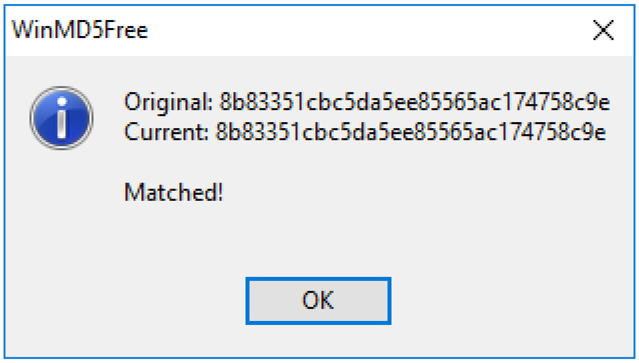
```
8b83351cbc5da5ee85565ac174758c9e
```

Original file MD5 checksum value (optional). It usually can be found from website or .md5 file

```
8b83351cbc5da5ee85565ac174758c9e
```

Simply drag and drop or browse to the file you are checking. It will automatically scan the file and display the current file MD5 checksum value in the space provided.

Next, copy the MD5 checksum value from our downloads page in the bottom box, then click verify. You will get the following message:



Original: 8b83351cbc5da5ee85565ac174758c9e
Current: 8b83351cbc5da5ee85565ac174758c9e

Matched!

This message indicates that there is a match, and the file you downloaded was from the original source.

Addendum 6 – Options: Wiping Tab

Number of Confirmations:

Set the number of times the user should be prompted to confirm a wipe operation prior to starting.

Allow Secure Erase:

If the hard drive being wiped supports Secure Erase or Sanitize, WipeDrive will use that function as a replacement for all zero pass overwrites (this includes zero passes in multiple overwrites, such as the DOD 5220.22-M). To disable that functionality, uncheck this option.

NOTE: if the wipe pattern specifies secure erase in the pattern this flag is ignored.

Allow TRIM:

If a hard drive/SSD supports the TRIM command, WipeDrive will use it during part of the cleaning process. To disable this functionality, uncheck this box. If you need to be able to verify a wipe after the fact you may need to disable this option so the last pattern put on the device remains.

Run short SMART self-test:

Run a captive short SMART self-test before the wipe, and fail if any self-test has failed.

Fail drive on SMART failure:

By default, WipeDrive will attempt to erase drives that are considered "bad" based on their SMART overall health status. If the company policy is to physically destroy bad drives, it's a considerable speed improvement to fail the drives immediately.

Disable cancel during operation:

Prevents the user from cancelling a wipe operation once it has started.

Stop verification if dirty sector found:

By default, WipeDrive will continue attempting to erase drives even if dirty or bad sectors are found. If your company policies are to physically destroy bad drives, it's a considerable speed improvement to fail those drives immediately.

Use Write Same:

Enable use of hard drive command write same. If your setup is bandwidth limited this may help speed up wiping. Not all drives support this feature or implement it correctly.

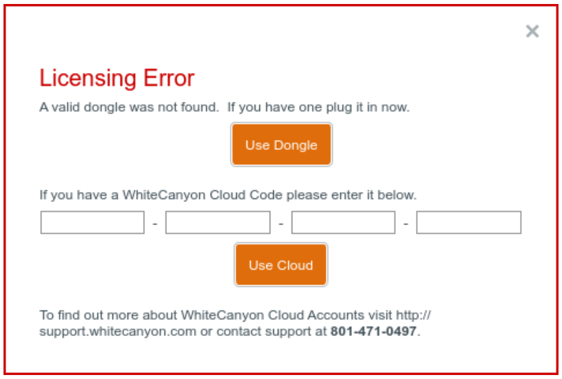
Use Solid Random:

Use a random repeating character in place of a random pattern (this can help if wiping many drives at a time).

Addendum 7 – Common Problems

ACTIVATION SCREEN

If the cloud account code or dongle is invalid, an error message indicating the problem will be displayed to the user. If the account is expired, or if the account no longer has enough licenses, contact support.

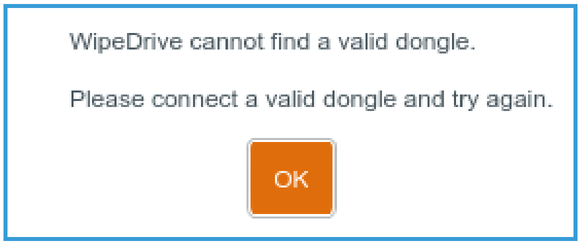


Licensing Error

A valid dongle was not found. If you have one plug it in now.

If you have a WhiteCanyon Cloud Code please enter it below.

To find out more about WhiteCanyon Cloud Accounts visit http://support.whitecanyon.com or contact support at **801-471-0497**.

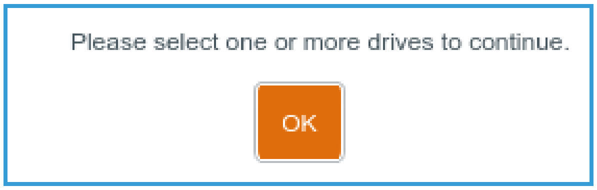


WipeDrive cannot find a valid dongle.

Please connect a valid dongle and try again.

DRIVE SELECTION SCREEN

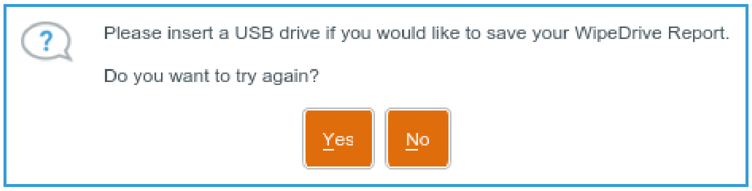
If the "Next" button is selected but no drives are selected for wiping, a dialog saying "Please select one or more drives to continue" will appear. In order to continue, close the dialog by clicking "OK", and select at least one drive to be wiped.



Please select one or more drives to continue.

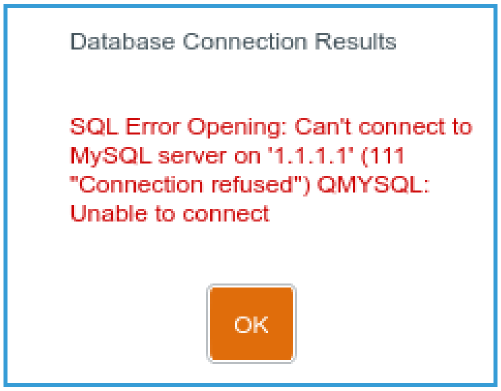
OPTIONS SCREEN

When the "Accept Settings" button is selected, if invalid entries are detected a dialog will appear indicating what error was detected. The indicated problem must be fixed before the selected options can be saved. Alternatively, if an error is indicated, selecting "Cancel" will exit the options screen without saving the changes. When configuring logging destinations, clicking the “Test” button for the corresponding logging option will indicate if the destination is reachable.



Please insert a USB drive if you would like to save your WipeDrive Report.

Do you want to try again?

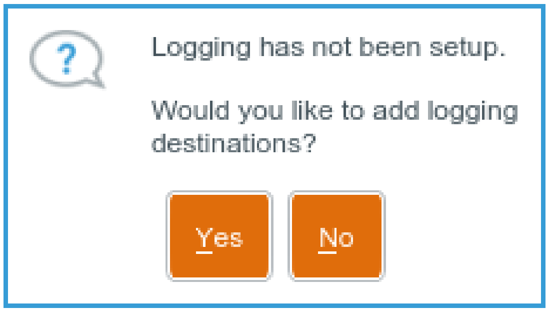


Database Connection Results

SQL Error Opening: Can't connect to MySQL server on '1.1.1.1' (111 "Connection refused") QMYSQL: Unable to connect

DRIVE SUMMARY SCREEN

If logging was not previously configured, WipeDrive will prompt the user with their last chance for configuring log file types and destinations. If “No” is selected, then logging is skipped and no logging information for that wipe operation is saved. If “Yes” is selected, the user is taken to the settings screen where they can configure the desired settings. Once complete, audit logs are saved according to the configurations.



Logging has not been setup.

Would you like to add logging destinations?