



WipeDrive Enterprise User Guide

Version: 1.5

Publication Date: 01-27-2021

Table of Contents

IMPORTANT! PLEASE READ CAREFULLY:.....	4
General Information	4
Security Considerations.....	4
Administrators.....	4
Storage	4
Updates.....	4
Date/Time	4
WipeDrive Enterprise.....	5
Overview	5
Configuration Settings.....	5
Overwrite Patterns	7
Activation	8
Key Features.....	8
Secure Removal of HPA, DCO and Accessible Max Address	8
Enhanced Secure Erase and Sanitize Device Options.....	9
Detailed Audit Logging.....	9
Running WipeDrive Enterprise	10
WipeDrive Boot Via CD or USB	11
Overview	11
System Requirements	11
BIOS Settings	11
Wipe Process	12
WipeDrive Boot Via .EXE	15
Overview	15
System Requirements	15
Wipe Process	15
WipeDrive Boot Via PXE.....	18
Setup Diagram.....	19
Wipe Process	20
VNC	21
Install the PXE Server	22
Overview	22
Updating Your Install.....	23

Wiping Remote Computers Via WipeDrive .EXE.....	23
Overview	23
Setup Diagram.....	24
Remote Desktop Connection Walkthrough.....	24
Requirements for Remote Desktop Connection:.....	24
Remote Wiping via PsExec Walkthorough	26
Requirements for PsExec:	26
Drive Verification	29
Command Line Parameters	29
Wiping.....	29
Logging.....	30
Logging to FTP	30
Logging to Email.....	30
Logging to SQL Database.....	31
Logging to Network Share	31
Hardware Inventory	32
Detalys Hardware Testing	32
Log Field Explanation.....	32
Options	35
Wiping Tab	35
Wireless Tab.....	36
Common Problems	37
Activation Screen	37
Drive Selection Screen.....	37
Options Screen.....	38
Drive Summary Screen.....	38
Remapped Sectors & SMART Data.....	39
MD5 / SHA3 Hash	40
Authentication via LDAP	41
Drive Life Remaining Estimation	42

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) attached to the system when running; the information will NOT be recoverable by any means including forensic recovery tools.

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.)
- It is Important to note that when WipeDrive is run using the CD/USB boot method, the environment created is one that conforms fully to what is outlined within the WipeDrive Security Target Document.

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.

CONFIGURATION SETTINGS

Logging

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.

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.



For instructions and information on all logging options, log file types, and log file destinations that WipeDrive Enterprise provides, please refer to the [Enterprise Logging Manual](#).

Note: If your needs for logging change at any point during the erasure process, additional logging attempts can be processed from the wipe summary screen. Simply click the 'Create Log' button found in the bottom right-hand corner of the wipe summary screen to configure new logging destinations and log file types.



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.

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.

When all the desired options have been setup, a copy of those configuration options can be saved out to the source boot media for future use. To do this, simply check the box 'Save Out Config' before pressing the 'Accept Settings' button in the settings menu. This method can make updating any existing custom build quickly and with ease.



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 Smart Wipe – Three overwrites. (0's, specialized pattern designed for SSD's, 0's)
- DoD 5220.22-M 3 Pass- Three overwrites with one verification. (0's, 1's, Random)
- DoD 5220.22-M 7 Pass - Seven overwrites with one verification. (0's, 1's, Random, 0's, 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 one verification.
- US Army AR380-19 – Three overwrites with one verification.
- US AFSSI 5020 – Three overwrites with one verification.
- US AFSSI 8580 – Eighteen overwrites.
- German VSITR Standard - 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. (Random)
- 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 one verification. (0's and 1's)
- BSI-2011-VS – Two overwrites with two verifications.
- NIST 800-88r1 – Meets NIST requirements and tailors the erasure custom to the drive's media type.
- NIST 800-88r1 3 Pass – Meets NIST requirements and tailors the erasure custom to the drive's media type, then adds two more overwrite passes plus one verification.
- Custom Overwrite - User defined overwrite pattern.

ACTIVATION

WipeDrive Enterprise supports multiple varieties of activation methods to suit the needs of a variety of setups. The primary activation methods are:

- Cloud Activation using a WhiteCanyon Cloud Account Code
- Dongle Activation using a WhiteCanyon USB Dongle locally
- Dongle Activation using a network attached WhiteCanyon USB Dongle

In closed network and offline settings where normal cloud activation isn't available, WipeDrive can be activated in an offline manner using a [generated surrogate code](#).

The WhiteCanyon USB Dongle comes in a Tier 1 and Tier 2 variety. Information on Tier 1 dongles can be found [HERE](#). Information on Tier 2 dongles can be found [HERE](#).

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 (AMAX) 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. There are cases however where the DCO lock cannot be bypassed. In this case, the total amount of sectors overwritten can be compared with the sector counts documented in official specification sheets made public by the respective hard drive manufacturers, and in doing so the user may be able to determine complete erasure of the drive despite the DCO configuration being locked.

ENHANCED SECURE ERASE AND SANITIZE DEVICE 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 Enhanced Secure Erase and Sanitize Device. These completely erase all reallocated disk sectors (sectors that the drive no longer uses because they have hard errors in them and have since relocated the sector to another working area of the drive).

If supported by the drive, and in conjunction with running a “firmware command supporting” wipe pattern, WipeDrive will use the Enhanced Secure Erase and/or Sanitize Device commands to ensure the erasure of these now unreachable bad areas that were remapped to new locations. When these before mentioned firmware commands are not used however, there is no way to erase the old sectors associated with the newly remapped sectors and WipeDrive will present a warning message along with a count of the unreachable remapped sectors. This warning message reads: “This drive contains a number of remapped sectors which were not overwritten. These sectors were flagged as bad by the drive and are not included in the user accessible portion of the drive.”

There are many benefits to using firmware commands when performing drive erasure and it is highly recommended that the users of WipeDrive do so. For Hard Disk drives (HDD), the benefit to using these firmware commands is to erase all sectors in the user accessible space and beyond, as mentioned previously. For flash-based media (SSD, NVMe, and eMMC drives) the benefits are much more significant. Using firmware commands on these media types can help immensely with erasure speed, and quality. These commands help overcome special drive features like wear leveling and overprovisioning by accessing the portions of the drive that are not normally accessible to the user.

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.

In order to produce audit logs in accordance with NCSC standards, the configuration option ‘dco-lock-warning-level=verbose’ must be used so that a more complete warning message can be displayed in the event that a drive fails to have its DCO configuration removed during the erasure process. For more information on how to use this option, see Addendum 2 – Command Line Parameters. A preconfigured build following the NCSC guidelines can be downloaded from the WhiteCanyon Enterprise download portal.

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 11)

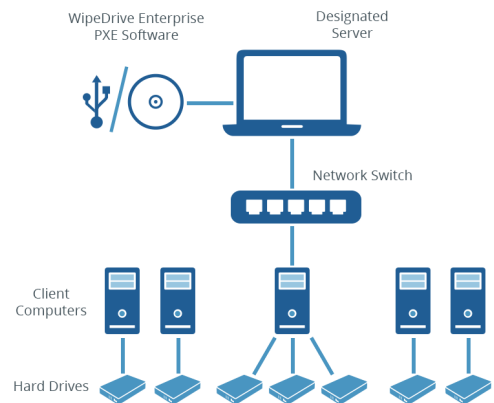
Booting from the EXE (see page 15)

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



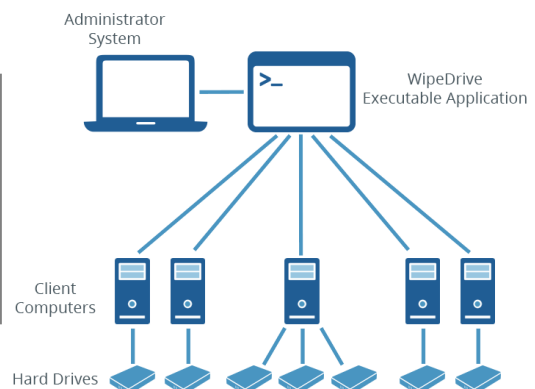
Via PXE network booting (see page 18)

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



Via Remote .EXE (see page 23)

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



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 Windows XP, Vista, 7, 8, 8.1, and 10, Linux, Unix and Intel-based Mac systems.
- Any type of hard drive (IDE, SCSI, SATA, SAS, SSD, NVMe, eMMC).
- CD-ROM Drive or USB port
- 2 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 computer manufacturer is not displayed, the BIOS keys are normally either DEL or F2.

WIPE PROCESS

Step 1

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

WipeDrive will now load the necessary drivers.



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'**.



Step 3

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

Select **'Next'** to continue.



Step 4

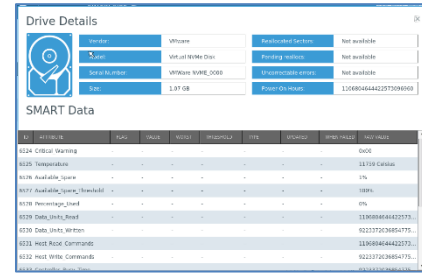
If you wish to change the log format or destination; please select **'Options'**.

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



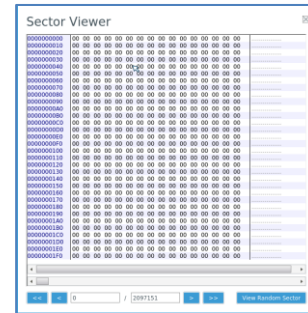
Step 5

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



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.



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 7 for more details on wipe patterns.

Select **'Next'** to continue.



WipeDrive Boot Via .EXE

OVERVIEW

Running WipeDrive via EXE is normally a good choice when the number of computers to be wiped are small as the WipeDrive EXE must be ran from the Windows desktop of each system.

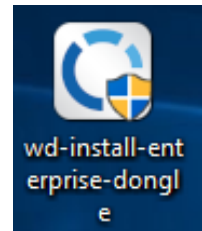
SYSTEM REQUIREMENTS

- Computer running Windows XP, Vista, 7, 8, 8.1 or 10
- 256 MB Free Hard Drive Space
- 2 GB RAM

WIPE PROCESS

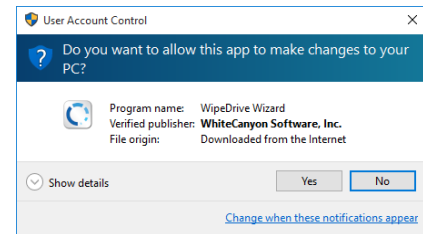
Step 1

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'**.



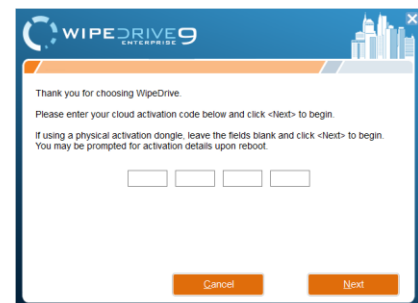
Step 3

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.



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.



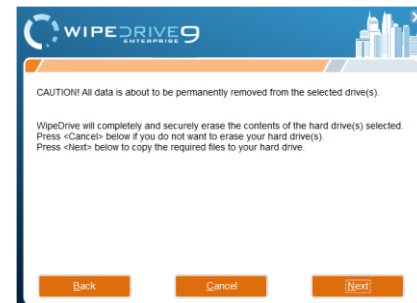
Step 5

At the Wipe Selection menu, select the required wipe and select 'Next'.



Step 6

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



Step 7

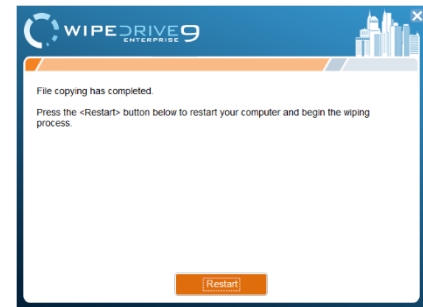
Before beginning the wiping process WipeDrive will first install the required files.



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.

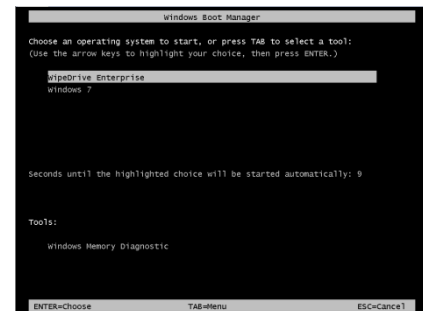
Click '**Restart**' to begin this process.



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.

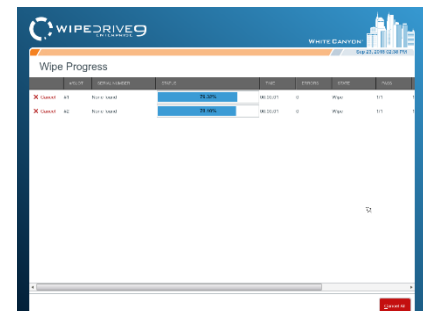
Press '**Enter**' to continue.



Step 10

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

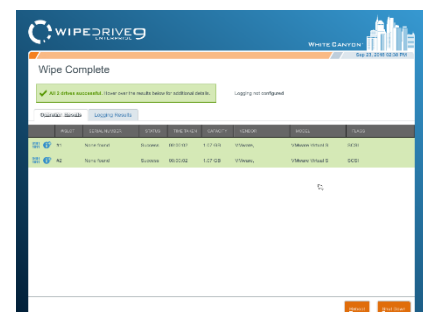
This screen will provide some useful information such as 'Time Remaining' and if any disk errors are detected.



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.



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

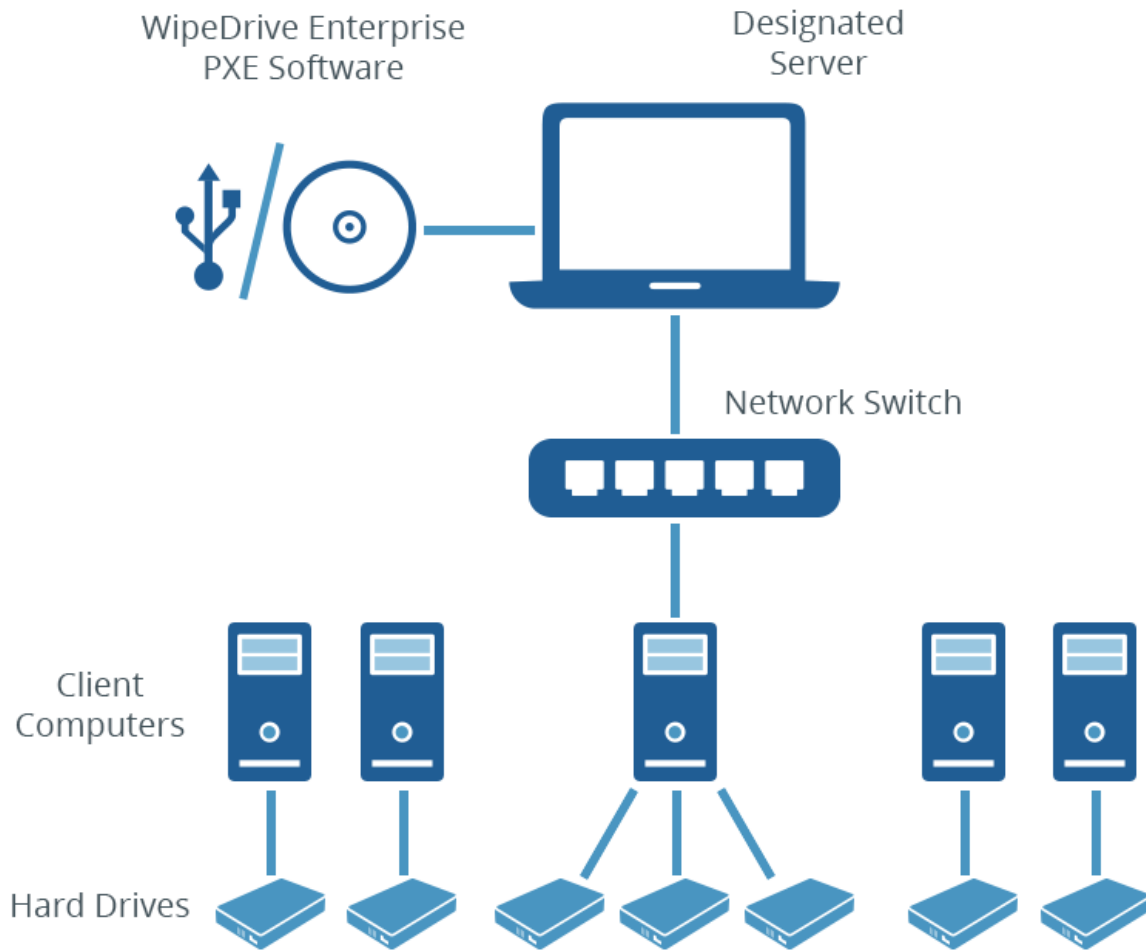
Computer designated to be the server (will not be wiped) with at least the following hardware:

- Core 2 Duo or better / Intel-based Mac OSX v10.6 or better
- 2 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
- 2 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

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 2 GB of RAM.

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



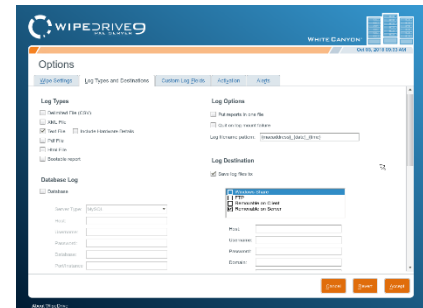
Step 2

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



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.



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.

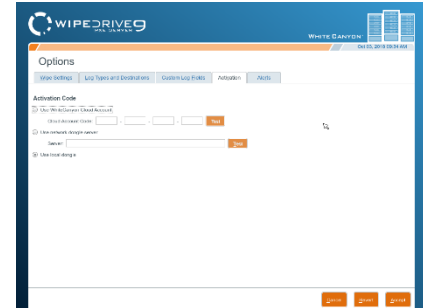
Please select the '**Activate**' tab.



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.



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.



Step 7

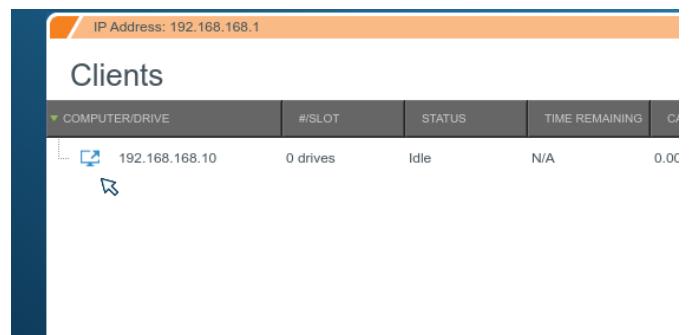
Restart each Client machine. The Client machines will boot into WipeDrive over the Network and begin the wipe.

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

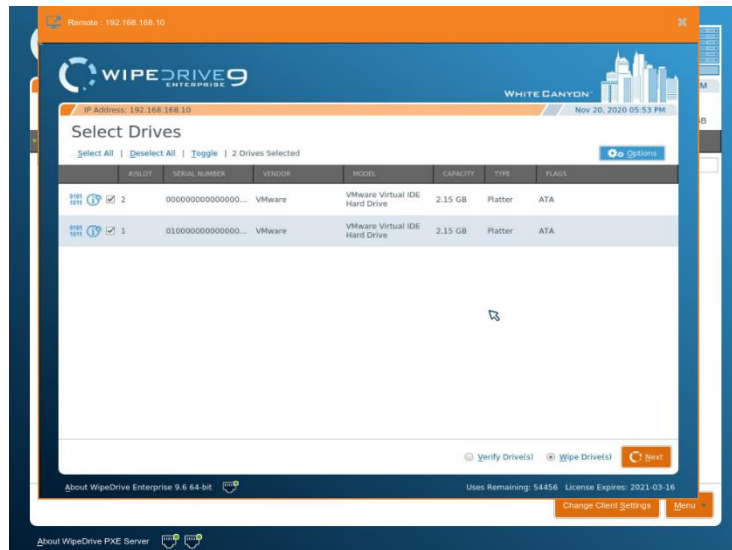


VNC

With PXE deployment, sometimes it is necessary to interact with a client device in order to help it move along through the erasure process. This can now be done remotely through the PXE server via the VNC feature. To interact with a specific device, simply locate the device in the list of active computers found on main screen of the PXE Server. Once the device has been located, click on the computer monitor icon to open the VNC client window.



Once a connection has been successfully established, the VNC window will display the UI of the client device that was selected. Through this window you can view and interact with the client device, performing any task necessary as if you were physically there working on the client device.



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 2 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.



UPDATING YOUR INSTALL

Step 1

Download a copy of the newest version of WipeDrive PXE Server ISO and burn the image file to a USB drive.

On the machine running the installed version of WipeDrive PXE, plug in the newly created USB and exit to the command line by typing 'exit' and selecting yes at the confirmation prompt.

Step 2

At the command line, type the following without quotations and press enter: "cd /hard_drive_install"

Now type the following without quotations and press enter to update the current installation on the hard drive: "./update.sh"

Once the update script has ran, your installation of WipeDrive PXE should now be updated to the latest version.

Wiping Remote Computers Via WipeDrive .EXE

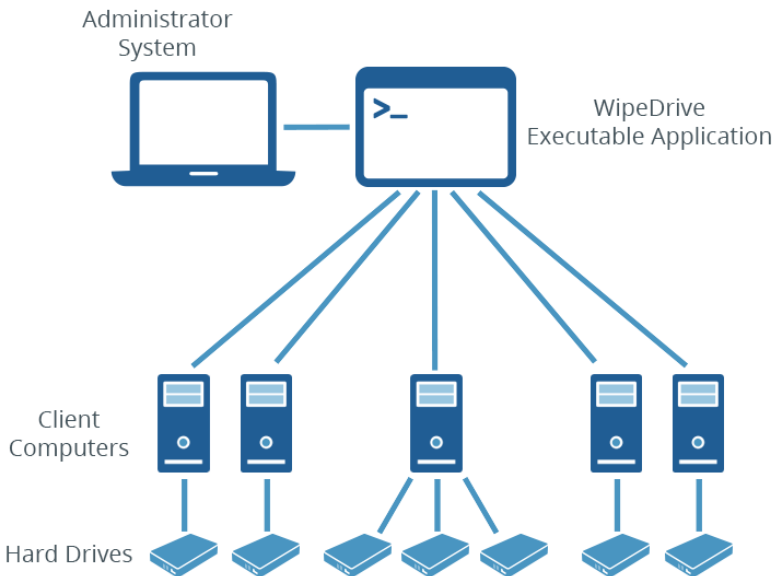
OVERVIEW

Running WipeDrive Remotely via EXE is normally a good choice when the 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.

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.

SETUP DIAGRAM



REMOTE DESKTOP CONNECTION WALKTHROUGH

Requirements 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:

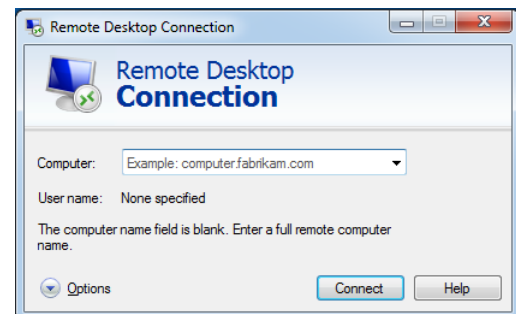
<https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/remote-desktop-client-faq>

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.

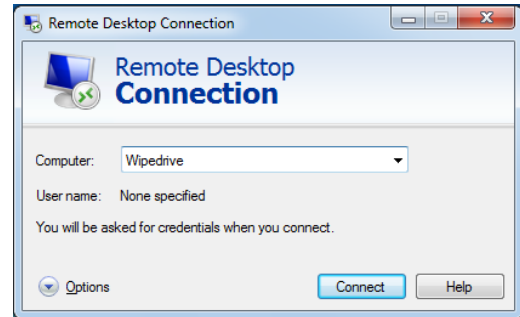
Note: On Windows 10 it can be found under 'Start' - 'All Apps' - 'Windows Accessories'.



Step 2:

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

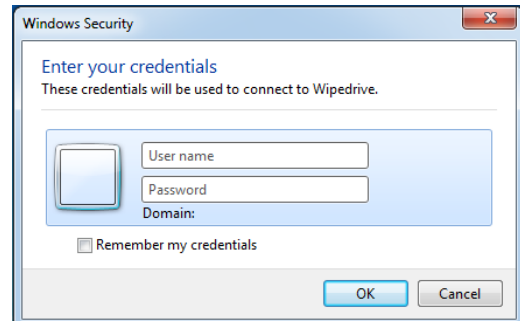
If it doesn't ask for a user at this point just enter the Computer name and click '**Connect.**'



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.

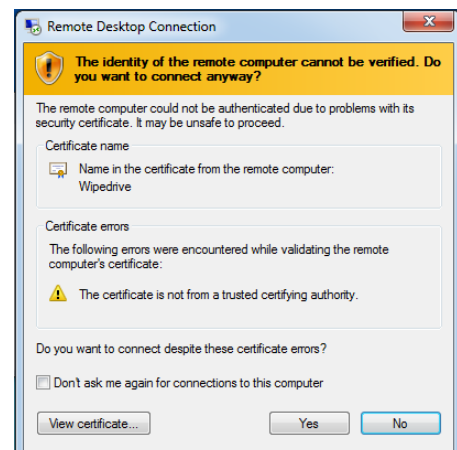


Once the Username and Password are entered click '**OK.**'

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.

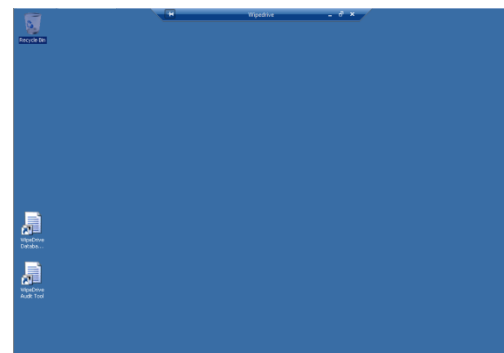


Step 5:

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 15 for a walkthrough on using the WipeDrive executable.



REMOTE WIPING VIA PSEXEC WALKTHORUGH

Requirements 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)

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.

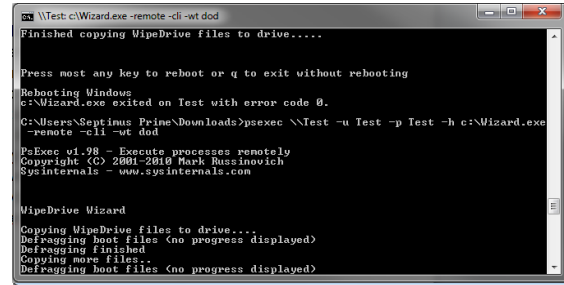
Step 1:

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

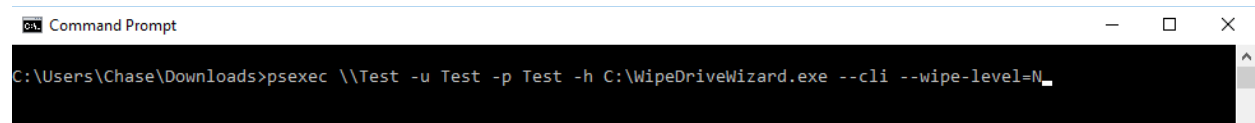


Step 2:

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.

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



The following is an explanation of each command being passed to PsExec:

- 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.

From this point, all other parameters are parameters for the WipeDrive EXE. Any existing WipeDrive option can be passed here. Make sure to always use double dashes.

- --cli: required to run WipeDrive in console form.
- --wipe-level: sets the wipe pattern to be used when WipeDrive runs

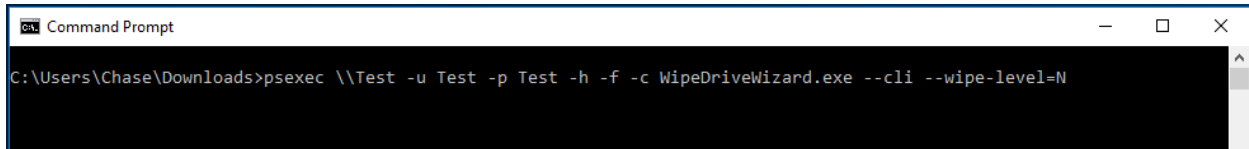
If all parameters are valid and PsExec can find the location of WipeDrive, the WipeDrive Wizard will begin installing the necessary tools to remotely run the software.

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

WipeDrive Enterprise Version 9.7

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.



```
Command Prompt
C:\Users\Chase\Downloads>psexec \\Test -u Test -p Test -h -f -c WipeDriveWizard.exe --cli --wipe-level=N
```

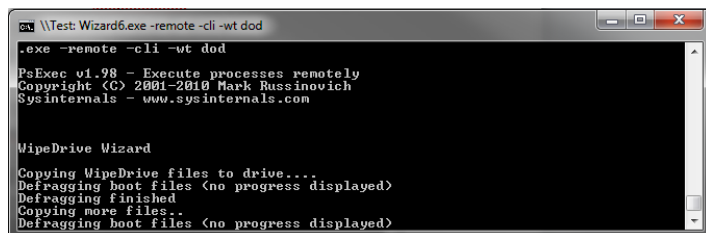
Just as before, here is an explanation of the parameters required to copy the WipeDrive application to the client computer and then run it:

- 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 option is required for clients running Windows Vista or higher
- -f: This option forces the file to be copied even if one already exists
- -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)

From this point, all other parameters are parameters for the WipeDrive EXE. Any existing WipeDrive option can be passed here. Make sure to always use double dashes.

- --cli: required to run WipeDrive in console form.
- --wipe-level: sets the wipe pattern to be used when WipeDrive runs

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



```
\\Test\ Wizard6.exe -remote -cli -wt dod
.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.

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 four 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 sectors 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 byte values are generated, followed by the bitwise compliments of those two byte values. In this way, it is possible to determine that the drive has been overwritten by random data specific to the WipeDrive program.

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

<code>--wipe-level</code>	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.)
<code>--disk</code>	Sets the selected disk to wipe. (Use -1 to wipe all drives)

LOGGING

--log-directory	Path where log files will be saved.
--log-file-types	Log file(s) format (d=delimited, h=html, p=pdf, j=json, r=text, 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.
--dco-lock-warning-level	Configures the presentation of the DCO Locked message presented when a DCO configuration is unable to be removed during erasure.

LOGGING TO FTP

--ftp-protocol	FTP protocol type to be used
--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

LOGGING TO NETWORK SHARE

--samba-server	Hostname of machine serving the network share
--samba-domain	Name of the Windows domain (if applicable)
--samba-directory	Directory where log reports are to be saved
--samba-user	Username of member to the network share
--samba-password	Password for user of the network share

For a more complete list of any of the possible command line parameters, please contact our support team. A Sample Configuration file is always included in the root directory of every ISO image of WipeDrive as well.

Hardware Inventory

WipeDrive Enterprise provides the functionality to perform a non-erasure based operation that will gather system information and create an audit log of the data gathered. To perform this operation, select the 'Hardware Inventory - NO WIPE' pattern from the wipe pattern drop-down menu found in the 'Wiping' tab of the program settings.

If no hard drives are attached to the system when attempting to run WipeDrive, the user will be prompted with a dialog asking to enter 'Hardware Inventory Mode' and upon accepting the prompt, the program is configured for Hardware Inventory.

Note: this feature is licensed separately from the standard WipeDrive erasure licenses. For questions, contact your sales representative by phone, or by emailing sales@whitecanyon.com

Detalys Hardware Testing

Alongside hard drive erasure, it is possible to configure WipeDrive to perform both automated and interactive hardware testing procedures that can help evaluate the functionality of equipment and diagnose any potential issues with your hardware assets. Detalys provides tests for major system components like the CPU, Networking Interfaces, RAM, Storage Devices, and Display, as well as tests for many other peripheral devices.

To enable Detalys hardware testing, navigate to the program settings and select the 'Hardware Test' tab. Once there, tests can be enabled and/or disabled to best suite testing the system that WipeDrive is being ran on. Most tests have additional options to help tailor their behavior to be the most beneficial to your auditing needs.

Note: this feature is licensed separately from the standard WipeDrive erasure licenses. For questions, contact your sales representative by phone, or by emailing sales@whitecanyon.com

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

WipeDrive Enterprise Version 9.7

- 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 found during a verification. Dirty sectors occur when a hard drive is failing and WipeDrive is unable to properly write to those specific bad sectors
 - 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, DCO configurations may not be detected nor 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
- TRIM Passes – Number of times the flash-based storage device was trimmed
- Sectors Overwritten – Lists the total number of user accessible sectors on the drive that were overwritten in a single pass, not to exceed the max sector count
- Sectors Not Overwritten - Lists the total number of user accessible sectors on the drive that weren't able to be overwritten. This count will include a count of remapped sectors in the event that firmware based overwrites were not used
- Sectors Verified – Lists the total number of sectors verified in a single pass, not to exceed the max sector count.
- Remapped Sectors – Lists the total number of physically bad sectors on the drive that have been remapped to new locations on the drive. This does not list any counts of sectors that are pending reallocated or have been repaired by the drive's firmware

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).

Pre/Post Encryption Key Reset:

Uses native OPAL and SanitizeDevice firmware methods to reset device encryption keys before and/or after the erasure operation.

WIRELESS TAB

Systems that have a Linux compatible wireless interface card have the ability to be configured for wireless networking use instead of requiring a wired Ethernet connection. If you would like to configure wireless settings, within WipeDrive you will need to open the Options screen by pressing the 'Options' button found at the initial drive selection screen. With the options screen now open, you will need to navigate to the 'Wireless' tab.

Note: if this tab is not available for you, then your system does not have a Linux compatible wireless interface card.

In order to connect to a network, the correct network will need to be selected from the table. Once that selection is made, you will need to press the 'Connect' button which can be found on the right-hand side of the table. A dialog will appear prompting for the network's password. Once the correct password has been entered and 'Ok' has been selected, WipeDrive will attempt to connect via Wi-Fi. If the connection attempt is successful, the fields 'current connection', 'IP Address', 'Netmask', and 'Gateway' will all display valid values.

The process of connecting to wireless can be automatically configured by adding the following options to the 'network.cfg' file:

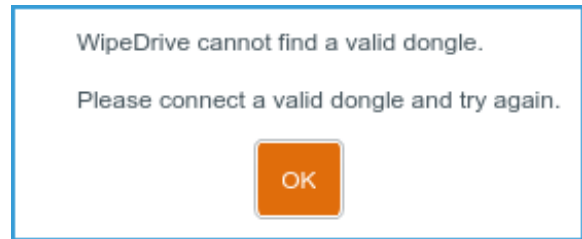
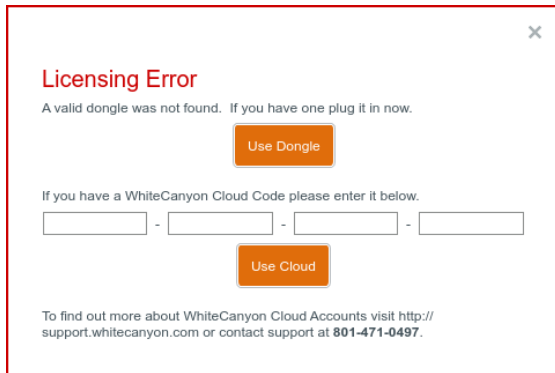
```
ssid="wipedrive"  
wireless_key="wipedrive"  
wireless_timeout=20
```

Once these options have been placed into the 'network.cfg' file and have been filled out to have the correct ssid and password, the 'network.cfg' is ready to be placed within the root of the ISO file. Once this file is placed within the WipeDrive ISO, the next time that WipeDrive is ran, it will automatically configure the network connection to work via wireless.

Common Problems

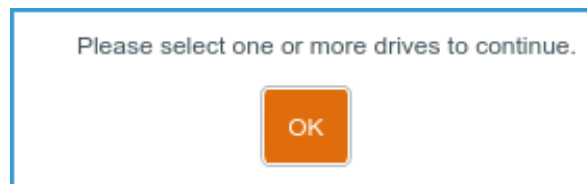
ACTIVATION SCREEN

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.



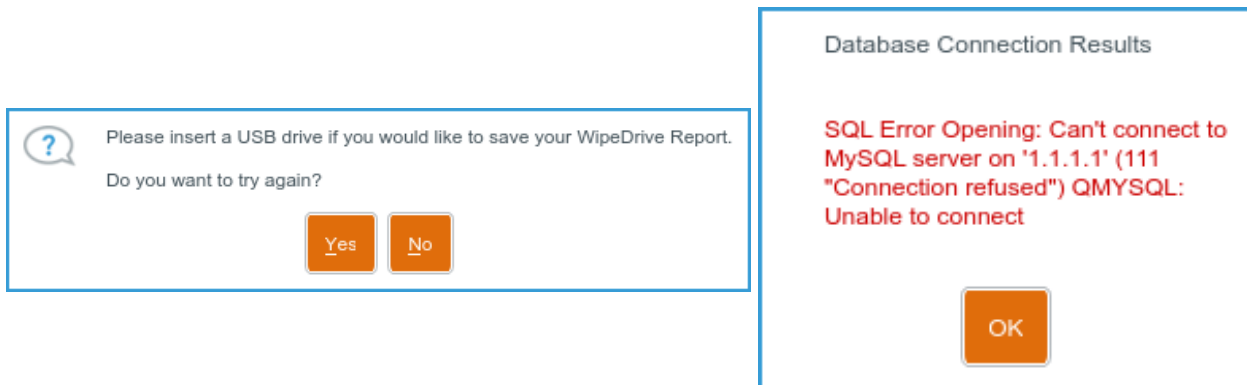
DRIVE SELECTION SCREEN

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.



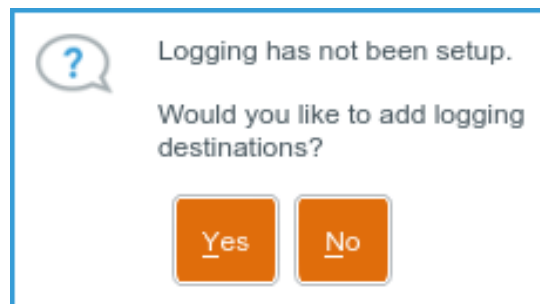
OPTIONS SCREEN

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.



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.



Remapped Sectors & SMART Data

In the event of sector failure, modern hard drives come with a portion of space inaccessible by the user with system commands, for the exclusive use of remapping physically bad sectors, to new ones. This is all controlled by the hard drive's firmware. When this remapping operation occurs, the hard drive keeps count of how many sectors have been remapped. This value can be queried and viewed via SMART data. On the same note, if a sector is starting to go bad, the hard drive's firmware maintains a list of pending reallocated sectors and will perform the reallocation operation once the sectors is consistently failing. This list can change however, due to sectors being repaired or deemed as no longer faulty. This pending reallocated sectors count is also found in a hard drives SMART data. Further information on these operations can be found within the ATA Drive specification sheet.

Since not all log file formats contain the SMART data, a count of Reallocated sectors is displayed in those concise log formats when the count is greater than zero. This count is also displayed as a flag when running WipeDrive. WipeDrive keeps track of the SMART data of a hard drive before a wipe, as well as after. Both pre- and post-SMART attributes are listed in the verbose logs formats and any changes can be seen by comparing the two data sets. SMART data can also be viewed in the GUI of WipeDrive by clicking on the drive info button at the 'Drive Selection' screen. Although SMART data is now very common, it is important to note that some drives may not support various attributes, or any at all.

MD5 / SHA3 Hash

To verify the validity and add to the security of files downloaded from WhiteCanyon, we have created MD5 and SHA3 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.

Download EXE
Show Hash
Run WipeDrive from Windows. Requires reboot.

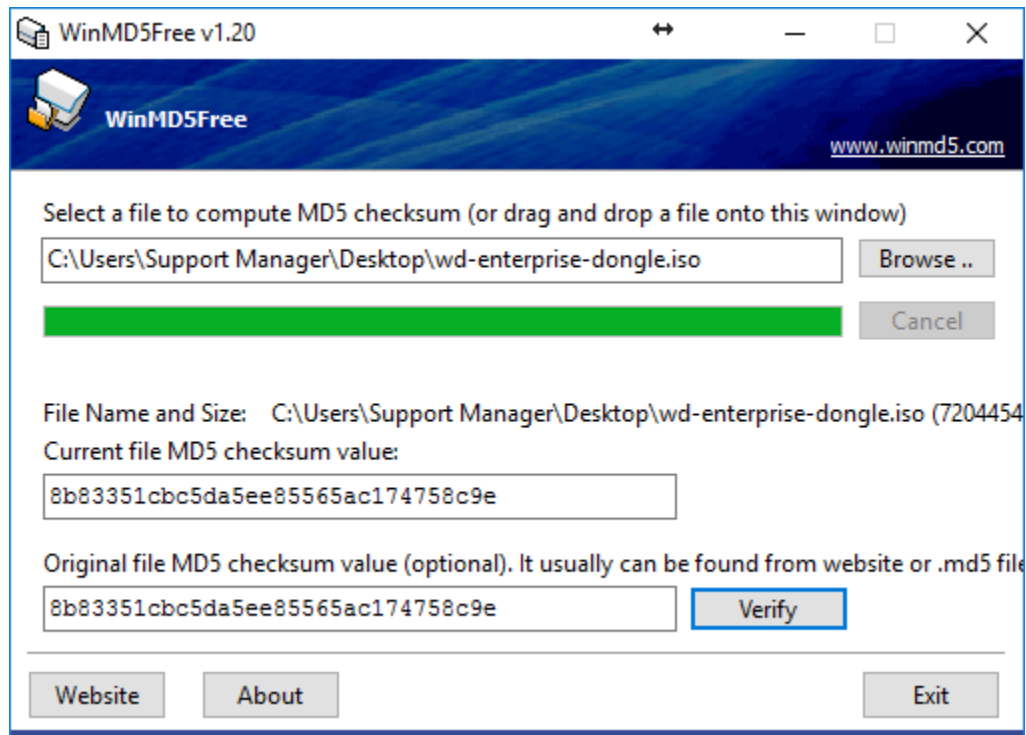
MD5:
b54ad57f06276f05d25e0677f98a0039
SHA3:
267ed899d24f869f8202f7d8374863899d84774fb894229c2a0a23df

Below each file download, you will see a link that says "Show Hash." Clicking on that link below each file download will display the custom MD5 and sha3 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/>

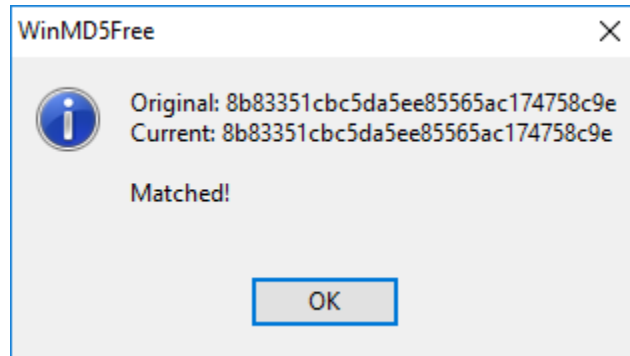
After downloading the utility and extracting the zip file, run the executable.

It will display a screen like shown below:



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:



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

Authentication via LDAP

WipeDrive can be configured to reach out to an existing LDAP server for authentication purposes. If access to WipeDrive is to be restricted to be ran only by authorized users, simply add the following options to the WipeDrive configuration:

```
authorize=ldap://ldap.whitecanyon.com  
ldap-user-base=ou=People,dc=whitecanyon,dc=com  
ldap-group-base=ou=Groups,dc=whitecanyon,dc=com
```

Once those options are set with the appropriate values, WipeDrive will connect to the LDAP server specified and will prompt the user running the software for their username and password and will authenticate that user against the user / groups specified to have WipeDrive permissions. Once authorized, WipeDrive will proceed to run as normal.

Drive Life Remaining Estimation

This feature allows WipeDrive to diagnose a hard drive's health and remaining life based on the SMART data attributes found on the drive. SMART attributes are data points kept within the firmware of a hard drive that help the user keep track of the current state of the drive. These attribute values can be used as predictors to help a user determine the current state of the device and if everything is still functioning properly. Of all the SMART attributes that are generally kept by devices that support the SMART data feature, there are a few that have been identified as correlating with hard drive failure. A few examples of these failure foretelling attributes are Power On Hours, Power Cycle Count, Reallocated Sector Count, and Pending Reallocated Sectors.

The drive life remaining estimate begins with the average expected life expectancy of a hard drive. From there, deductions to this life total are made based on the SMART attributes previously mentioned. Each attribute value is carefully considered, evaluated and compared to various thresholds to determine the likelihood that the hard drive could fail and how soon it could fail. This estimation is then recorded in the log report for the hard drive. It is important to note that this estimation is just that, an estimation. Therefore, a device may out last the estimation given, or may prematurely fail before it was estimated to. The purpose of the life remaining estimation is to give the user a general idea of how long they can expect their device to be in working condition, given its current state as reported by the SMART attributes for the drive.