REDKEY USB V5

USERS MANUAL

Table of Contents

1 About REDKEY USB

1.1 Overview

Eliminate Risk & Protect Your Privacy.

Introducing the Redkey USB - Computer Data Wipe Tool. Now you can sell, recycle or donate used computers without worry! Essential tool, for use prior to Selling or recycling a computer. Once the wipe is complete, you are protected. Safe & Secure.

Simple & easy to use.

Only Redkey features an automated wipe process. Now you can wipe all of your old computers – effortlessly! Specifically designed for simplicity, Redkey works automatically. Just plug it in to a spare USB port & power on your computer to initiate a wipe.

A powerful tool.

Wipe all data securely & permanently. Sanitize used equipment. RedKey uses a special process to irrecoverably destroy all data from the storage drives inside a computer. Protect yourself from Fraud, Forensics, snooping, data recovery and even hackers. Data recovery is impossible after a Redkey wipe. The end result is a clean computer – ready for safe sale or disposal.

1.2 Minimal System Requirements

For Redkey USB Software:

- An X86 or X64 PC with minimum 1GB RAM.
- A suitable USB 2.0 port with USB boot capability.
- A suitable display adaptor.
- A suitable display, keyboard and mouse.

For Redkey USB Software (when operated in Remote Mode)

- An X86 or X64 PC with minimum 4GB RAM.
- A suitable USB 2.0 port with USB boot capability.
- A suitable display adaptor.
- A suitable display, keyboard and mouse.

For Redkey USB Updater Application:

- A Windows 7 (or above) X86 or X64 PC with minimum 1GB RAM.
- A live, unhindered, direct internet connection. (Download size Approx. 1GB)
- A suitable USB 2.0 port.
- A suitable display adaptor.
- A suitable display, keyboard and mouse.

1.3 Redkey versions – Home / Professional / Ultimate

Redkey USB has three versions, the features that are included in each are detailed in the following table:

		Home	Professional	Ultimate
Data Wipe Features	Select Standard Algorithm	✓	✓	✓
	Customize Wipe Algorithm		✓	✓
	Create Custom Binary Sequence		✓	✓
	Save & Load Custom Binary Sequence		✓	✓
AutoNuke™	Immediate Mode	✓	✓	✓
	Interval Mode	✓	✓	✓
	Auto-Destruct Mode		✓	✓
Remote Wipe	Boot & wipe remote computers via LAN	✓	✓	✓
Report Features	Basic Reports View (End of Wipe)	✓	✓	✓
	Extended Reports		✓	✓
	Save PDF Reports on Redkey & USB Drives		✓	✓
	Report Editable Fields, Details Save & Load		✓	✓
Extra Features	View RAW Data	✓	✓	✓
	View Extended System Information		✓	✓
	View Disk Detailed Information		✓	✓
Audio Visual Features	Custom Images		✓	✓
	Custom Music		✓	✓
Advanced Features	Scripting			✓
Mobile Devices	Wipe Apple Devices			✓
	Wipe Android Devices			✓
	Notation in this manual:		`Pro & Ult`	`Ultimate`

2 Starting Redkey

2.1 Booting up

A. Connect the Redkey into a USB 2.0 or USB 3.0 Port

B. Power on or restart the computer

Remember to keep Redkey connected to the USB port !
Removing it while the PC is running will cause the application to crash with unexpected results !

C. Press the keyboard key required to open the Boot Menu,
Most computers use the F12 key, others usually display the required key on screen during start-up. The following table may also help to find the one used in your model:

Make	**Boot Menu**	**System Config (Bios / UEFI)**
Acer	Esc, F12, F9	Del, F2
Asus	F8 or ESC	F2, F9 or DEL
Compaq	Esc, F9	F10
Dell	F12	F2 or DEL
Dell Servers	Reboot the computer, and when prompted, press F11 to enter the BIOS Boot Manager. Select 'Continue to Normal Boot.' After a short loading time, your device will boot from the Redkey.	
eMachines	F12	Tab, Del
Fujitsu	F12	F2, F12
Geo	Del	Del
HP	Esc, F9	F1, F2, F10, ESC
HP Servers	Upon rebooting the computer, press F11 to access the boot menu. Then, select option 3 which will initiate a one-time boot from the USB Drive Key. Your device will now boot from the Redkey.	
Intel	F10	DEL
Lenovo	F12, F8, F10	F1, F2
Lenovo	F12, Nano Btn, Fn+F11	F1, F2 or Nano Btn
NEC	F5	F2
Packard Bell	F8	F1, F2 or DEL
Samsung	Esc, F12	F2, F10
Sony	Assist Btn, Esc, F11	Assist Btn, F1, F2, F3, F11
Toshiba	F12	F1 F2, F12 Esc

* On some computers the Boot Menu is accessed through the BIOS / UEFI Config Menu

D. From the Boot Menu - select the option showing ‘Redkey’ or ‘USB’

* if you have multiple options with ‘Redkey’:
prefer the one that says ‘EFI’ / ‘UEFI’ over ones that say ‘BIOS’ / ‘Legacy’

If you are running Redkey on a server,
please read section 20.1 - Server RAID setup
before starting

2.2 Redkey Boot Options

The Boot Menu's display in UEFI computers and on BIOS ones:

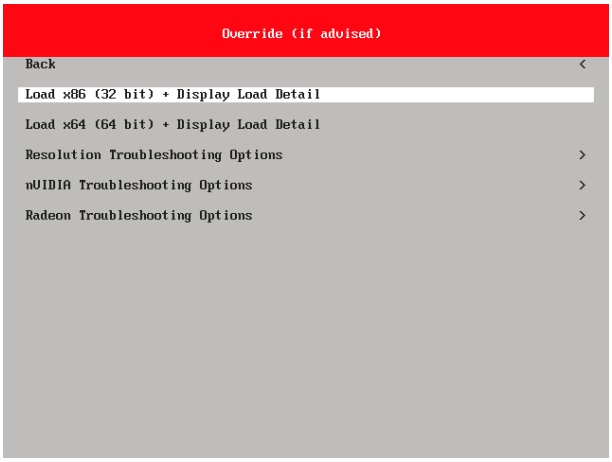
UEFI Boot Menu

BIOS Boot Menu

If no key is pressed within a few seconds the application will load using default settings automatically.

For troubleshooting, the Boot Options menu is available by selecting the 'Override' option:

UEFI Boot Options



BIOS Boot Options

Refer to section 20 - Troubleshooting options guide for the usage of the Boot Options menu.

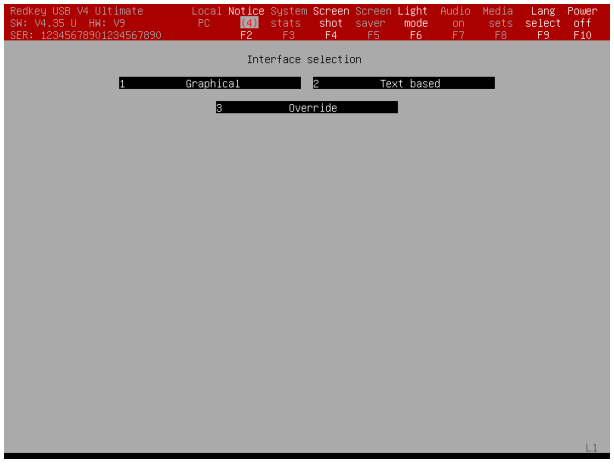
3 Quick Start / Basic Usage

3.1 Interface Selection – Graphical (GUI) / Text (TUI)

Redkey can be used via both a graphical interface and via a text interface in case the graphical one cannot be used due to incompatible h/w.

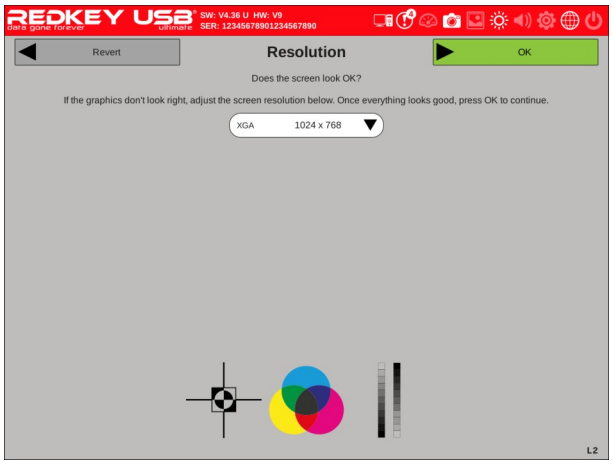
All of Redkey functions are supported by both interfaces, with the exception of the screen saver function and AutoNuke™ Auto-Destruct Mode which are only available via the GUI.

The Interface selection displayed allow to select which interface would be used.

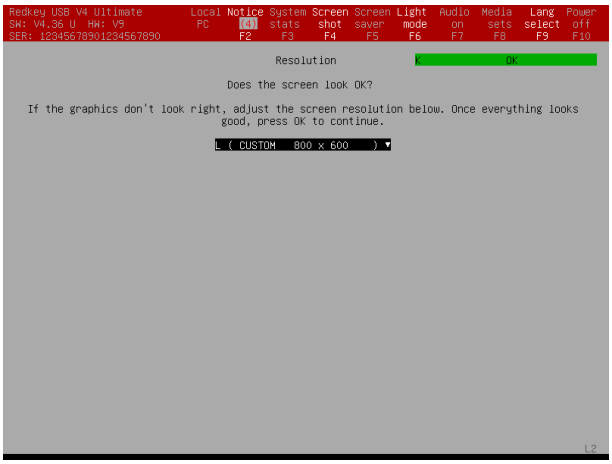


3.2 Screen Resolution selection

The native resolution for the display is pre-selected automatically as detected.
If the display is showing properly - click OK to continue.
If needed – select a different resolution. A newly set resolution will revert back to the previous setting if not confirmed within 20 seconds.



GUI



TUI

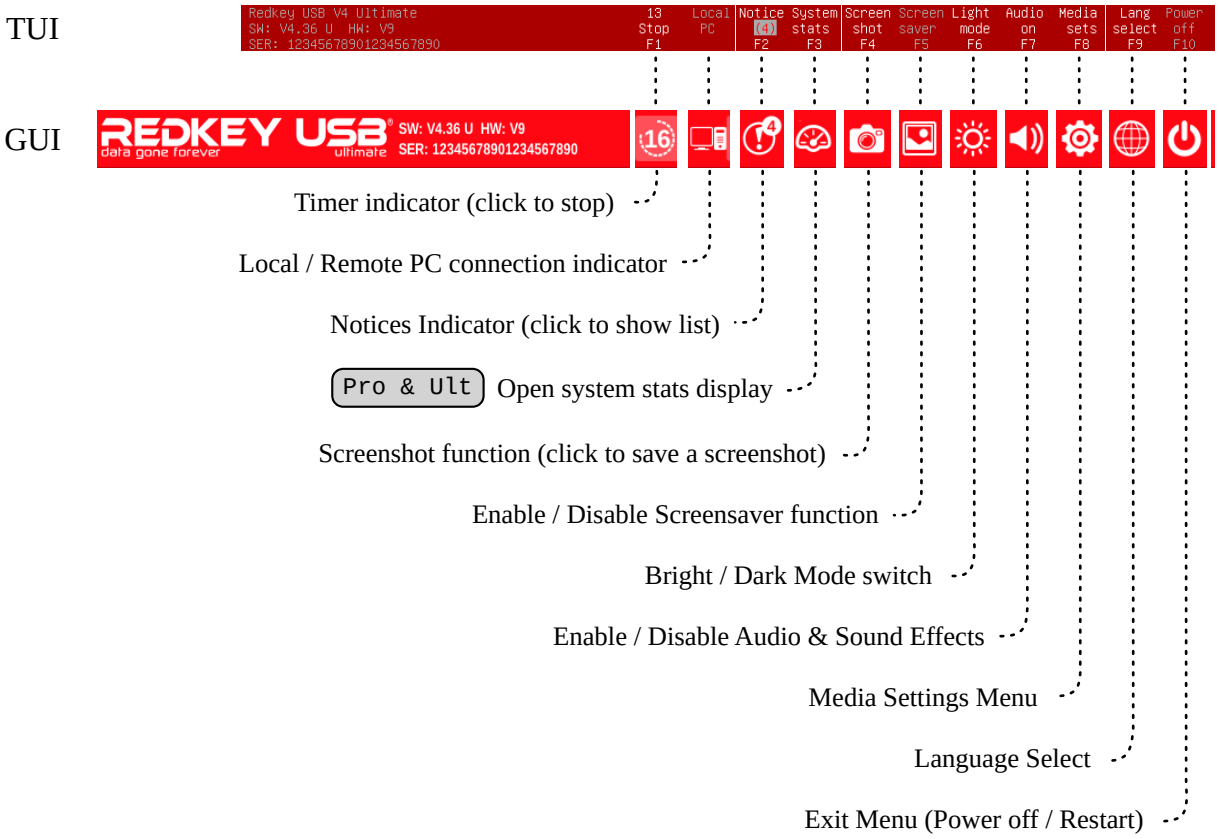
3.3 Language Select

Redkey supports multiple languages, the menu allows to select the language for menu displays and voice prompts.

The language can also be pre-set using the Redkey Updater's settings menu or by editing the settings file (see 18 - Options File).

3.4 Top Bar functions

In all menus the top of the display provides quick access to various functions as detailed below. Depending on the current menu and state – some of the functions may be disabled.



3.5 Keyboard shortcuts

When using the TUI for each option displayed a keyboard key to select it is shown next to it. These keyboard shortcuts allow to operate the application using only the keyboard in case a mouse is not available.

Using the GUI – if no mouse is available – the TAB and arrow keys can be used to select an option or setting and the space bar or enter key can be used to activate it.

3.6 Media Settings Menu

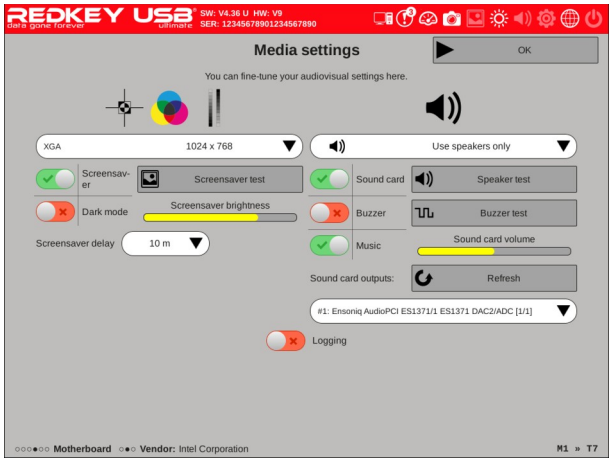
The Media Settings menu can be accessed using the Top Bar.

The functions available:

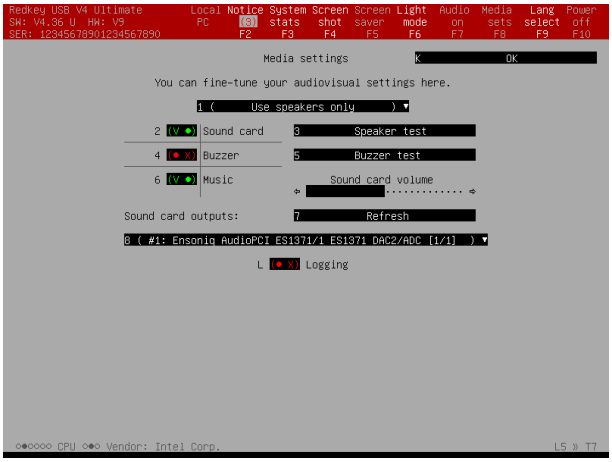
- Select sound effects option – Speakers and/or the PC Buzzer and to test them
- Select the sound card output used and set the volume
- Enable debug logging (only enable if requested by technical support).

In GUI mode these options are also available:

- Adjust the screen resolution
- Adjust Screen Saver settings



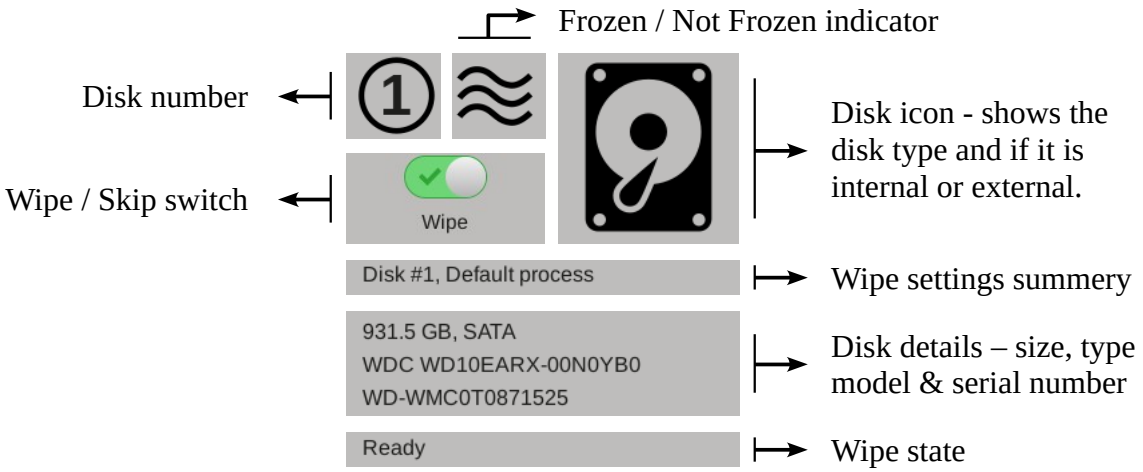
GUI



TUI

3.7 Disk Display

The various menus in Redkey use this format to show detected disks, settings and status:



3.8 Main Menu

- **Wipe Wizard™**
  A guided and user-friendly mode, guides through the wipe process step-by-step.

  * `Ultimate` Wiping Mobile devices is also accessed via this mode.

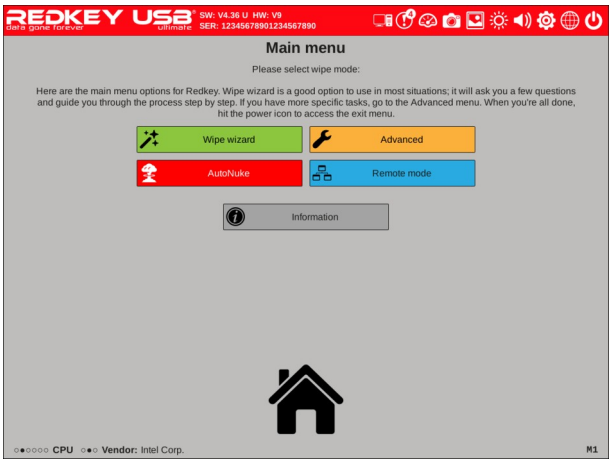
  See 4 - Wipe Wizard™ for more details.

- **Advanced Mode**
  Intended for advanced & power users, allows to customize the wipe process and other advanced functions.

  See 5 - Advanced Menu for more details.

- **AutoNuke™ Mode**
  A 'Set & Forget' wipe mode for wiping everything quickly and efficiently

  See 8 - AutoNuke™ Mode for more details.



- **Remote Mode**
  Used to wipe remote computers connected over a LAN (Local Area Network)

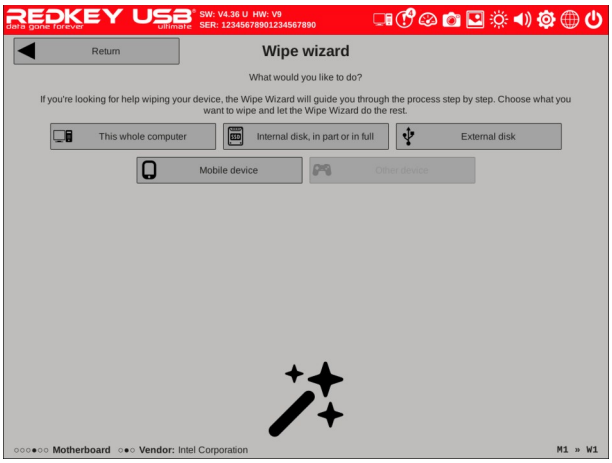
  See 9 - Remote Mode for more details.

- **Information menu**
  Shows system information for the currently selected PC (local / remote) and allows to clear logs & report data.

4 Wipe Wizard™

From the Wipe Wizard™ main menu select whether you would like to wipe the whole computer, just a single internal / external device or a mobile device.

The Wipe Wizard™ will guide through the process with on-screen instructions.



* For more detail about the default settings used - refer to section 11 - Default Wipe Settings.

* See section 10 - Wipe Sequence for details on the actual wipe sequence.

5 Advanced Menu

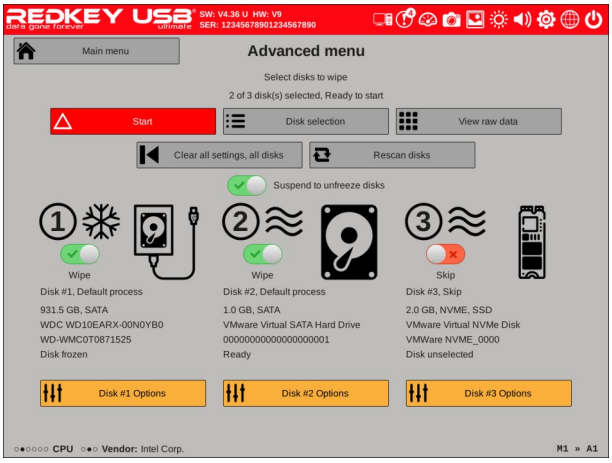
From the Advanced Menu all the advanced functions supported by Redkey are performed.

The process when using advanced mode usually is:

A. Selecting the disks to wipe - this can be done using the switches next to each disk or using the 'Disk selection' menu (see 5.2 - Disk Selection).

B. Customizing the wipe settings for each disk – this is done by clicking the 'Disk #n Options' button under each disk. (see 5.7 - Disk Options Menu for more details)

C. Clicking 'Start' to begin the wipe process.



5.1 Start

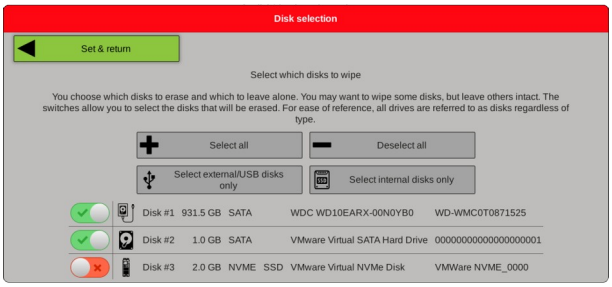
Starts the wipe for selected disks (see 5.2 - Disk Selection) using the settings as customized for each disk by the Disk Options Menu (see in 5.7).

See section 10 - Wipe Sequence for details on the actual wipe sequence.

5.2 Disk Selection

The Disk Selection menu can be used to quickly view a list of all detected disks and to select which of them to wipe.

Quick shortcut functions are available to select / de-select all disks, or select all external / internal disks.



5.3 View Raw Data

Opens Redkey's Raw Data viewer to inspect the current (pre-wipe) contents of the disks
See 6 - View Disk Raw Data for more details.

5.4 Clear All Settings

Select this to reset all the settings (for all disks) to default (also see 11 - Default Wipe Settings).

5.5 Re-Scan Disks

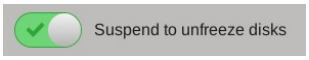
This function can be used if an external disk or USB flash device was connected after entering the menu.

5.6 Suspend Switch

For SATA disks Redkey uses by default secure erase commands, in some systems at power up the BIOS places disks in a ‘Frozen’ state that does not allow to use these secure erase commands.

To ‘Unfreeze’ the disks and allow secure erase commands to be used a system suspend is done.

When the switch is enabled, upon pressing ‘Start’ Redkey will first do a system suspend before starting the actual wipe.

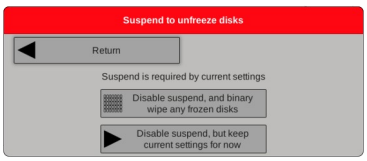


Redkey automatically detects if a suspend is required based on the disks selected to wipe and the current wipe settings, and automatically sets the suspend switch accordingly.

Redkey allows the user to override this automatic setting, by manually setting the switch on/off:

- If suspend is not detected as required, it can be manually enabled, this might be required for some troubleshooting situations (see 20 - Troubleshooting options guide).
  When doing so - a prompt as shown will request to confirm.

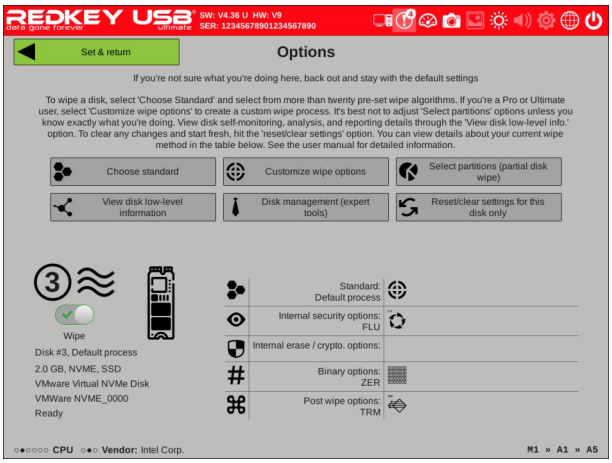
- If suspend is detected as required, it can be manually disabled, this can help with systems that are known to not support suspend properly.
  When doing so - the prompt as shown will allow to select between automatically changing wipe settings to not require suspend (use binary wipe methods instead for frozen disks), or to disable suspend without changing the settings.
  Please mind that if current settings are kept - you would then need to change the settings manually or de-select the frozen disk(s) before being able to start the wipe.



See 10.1 - System Suspend for more details on system suspend.

5.7 Disk Options Menu

The Disk Options menu can be accessed by clicking the ‘Disk #n Options’ button shown under each disk.



This menu allows to:

- View the details of the currently set wipe process (shown on the table on the lower right part of the screen)
- Change the wipe settings
- View low-level disk details
- Perform other disk management functions

5.7.1 Choose Standard

Allows to use pre-set standard algorithms, as detailed in section 15 - Supported Standards.

Selecting a standard from the list will clear any custom settings previously set for that disk.

5.7.2 Customize Wipe

See section 16 - Customizing the wipe sequence.

5.7.3 View Disk low-level Information Pro & Ult

Displays the low level detailed information of the disk as detected by the application.

5.7.4 Disk Management

See section 7 - Disk Management Menu.

5.7.5 Reset / Clear Settings

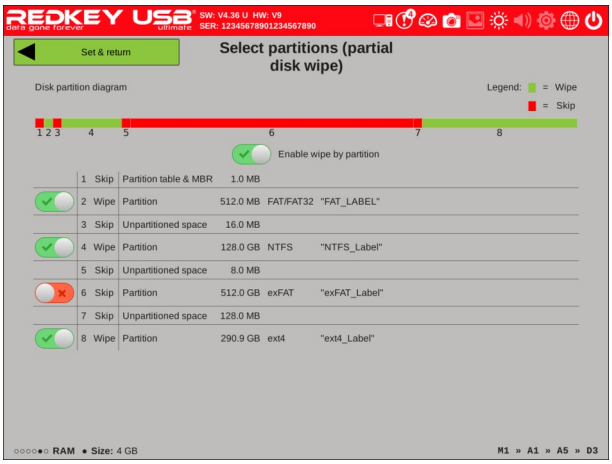
Resets the wipe process settings of the selected disk back to their defaults.
See section 11 - Default Wipe Settings for details on the defaults used.

5.7.6 Select Partitions – partial disk wipe

Redkey is able to only wipe selected partitions.

From this menu the existing partitions on the selected disk are shown and ‘wipe by partition’ mode can be enabled to only wipe selected partitions.

Once enabled, use the switches next to each partition shown to set to Wipe or Skip.



With this mode enabled only the partitioned disk areas can be selected to wipe - the unpartitioned areas cannot be wiped ! These unpartitioned areas can only be wiped as part of a normal (whole) disc data wipe.
To perform a whole disc data wipe, turn wipe by partition off.

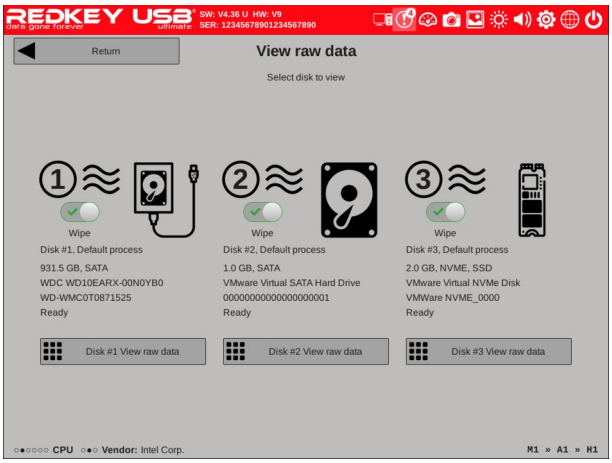
When this mode is enabled, only binary wipe methods or standards that only employ binary steps can be used.

In addition, the following features cannot be used when this mode is enabled:

- HPA
- DCO
- Internal erase functions
- Trim
- Disk partitioning

The same wipe settings will be applied to all selected partitions, If a formatting post wipe step is enabled, all selected partitions will be formatted with the same selected file system format.

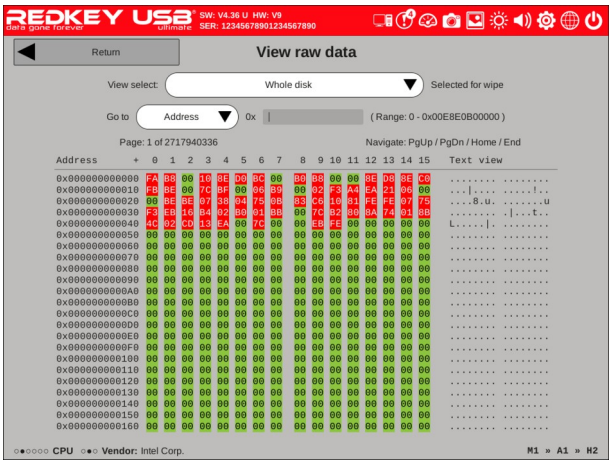
6 View Disk Raw Data



Redkey includes a raw data viewer (‘Hex Viewer’) designed to allow inspecting the entire disk’s / media’s area for it’s actual contents.

The viewer can be accessed from the Advanced Menu or the Wipe Complete screen.

To view a disk’s raw data first select the disk to view using the button below it.



The top box selects the area of the disk to view, selecting ‘Whole Disk’ will show the entire disk media, selecting a partition (if any are detected) will show only that partition.
* When viewing after completing a wipe - viewing a partition may fail as the partition table has already been erased.

To use PgUp / PgDn keys to browse the disk – first click the Address / Page entry box at the top middle.

When viewing the disk’s contents from the Advanced Menu, if no wipe has been done yet the disk is to be expected to contain data other than all zeroes

When viewing the disk’s contents from the Wipe Complete Menu the disk contents is expected to be in accordance with the last step of the wipe sequence, examples:
All zeros if the last step was Zero Fill (ZER) / Secure Erase
All ones (= hex FF) if the last step was Ones Fill (ONE)
Random data if last step was Random Fill (RND/SRD) or if a crypto internal erase method was used.

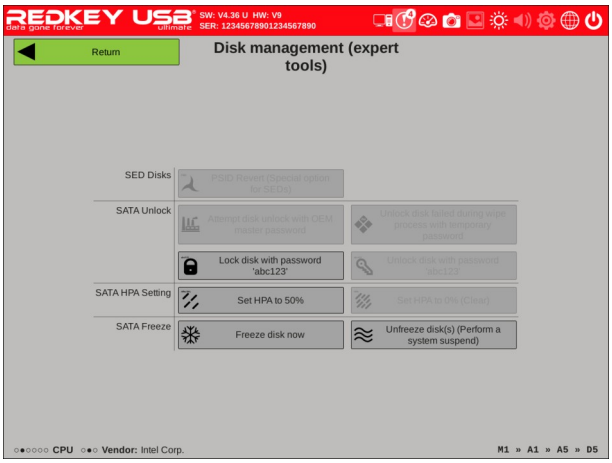
If the wipe sequence included partitioning or formatting the disk will also contain the partition table and file system data.

7 Disk Management Menu

The Disk Management menu contains advanced disk management functions.

Some of the functions may be disabled if not relevant to disk type or state.

Some of the functions also require to be enabled using the options file (see 18 - Options File).



7.1 SED Revert with PSID

This function allows to revert (reset) an SED (Self Encrypting Disk) using PSID code.
The option would only enable when selecting an SED device.

7.2 Unlock Disk With Manufacturer Master Password

This function can unlock a SATA disk which is locked with an unknown code, using manufacturer master passwords.
The option would only enable when selecting a locked disk.

7.3 Unlock Disk failed during wipe process

In order to use SATA Secure Erase commands, a disk must first be locked, when the erase is properly finished the disk is automatically unlocked, but if the erase is interrupted by a power failure or other reason, the disk might stay in locked state. This option is intended for such a case and will try to unlock the disk with the temporary password the application uses to lock the disk during wipe (which is ‘dw’).

The option would only enable when selecting a locked disk.

7.4 Lock / Unlock Disk with password abc123

Options used for testing, usually disabled – see section 18 .

7.5 Set HPA 50% / 0%

Options used for testing, usually disabled – see section 18 .

7.6 Freeze Disk

Option used for testing, usually disabled – see section 18 .

7.7 Unfreeze Disks

Initiates a forced System Suspend as detailed in 10.1 - System Suspend.

** It is usually not required to initiate suspend manually, as the application will automatically prompt to suspend if required when starting the wipe. **

8 AutoNuke™ Mode

Using AutoNuke™ mode will wipe
all data from **all disks** !

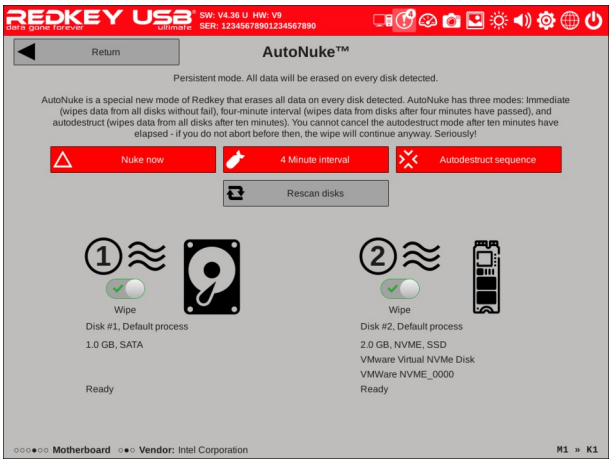
To wipe only some of the disks or change
the wipe settings use the Wipe Wizard™ or Advanced Mode

AutoNuke™ is an automated mode to wipe all data on all detected disks, internal and external.

AutoNuke™ will automatically use the best applicable wipe method for each disk according to its type and state.

For more detail about the default settings used - refer to section 11 - Default Wipe Settings.

See section 10 - Wipe Sequence for details on the actual wipe sequence.



9 Remote Mode

Remote mode can be used to wipe remote computers connected to the PC running redkey via LAN (a Local Area Network).

This mode can help with wiping computers which have faulty displays or incompatible graphics cards.

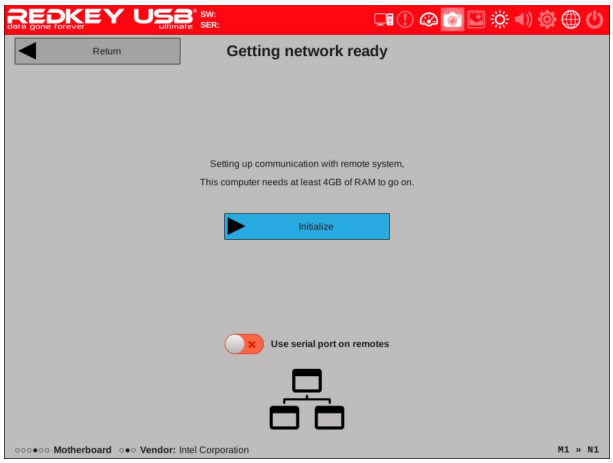
9.1 Initializing Remote Mode

A. From Redkey's Main Menu – select Remote Mode

* for details about serial mode switch: see section 19.2 .

B. Click 'Initialize'

C. Wait for the process to complete



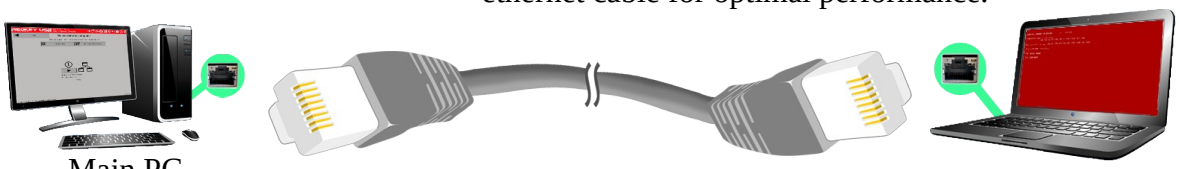
D. Once the 'Select remote computer' screen is showing, proceed to connect and setup the remote computers.

9.2 Connecting and setting up remote computers

A. Connect the remote PC to the PC running Redkey using one of the methods below:

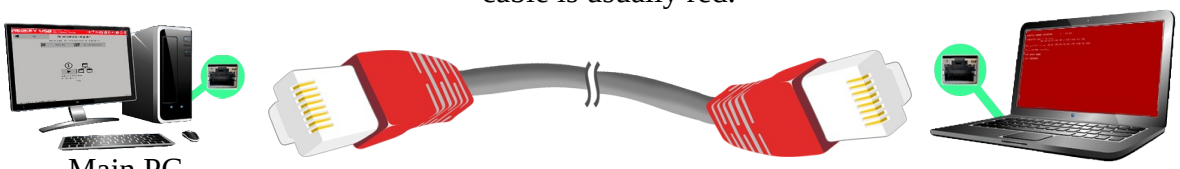
Using a Direct cable

If at least one of the PCs supports Gigabit LAN then this is the recommended option. Use a CAT-8 LAN ethernet cable for optimal performance.



Using a Crossover cable

If both PCs only support 10/100Base LAN, this is a suitable solution. The RJ45 connector on a crossover cable is usually red.



Via a Network Switch

If you need to connect more than one PC at once - this is the recommended option.

Via a Router

The router's DHCP function **must be disabled** !

We recommend using CAT-8 LAN cables for optimal performance and compatibility.

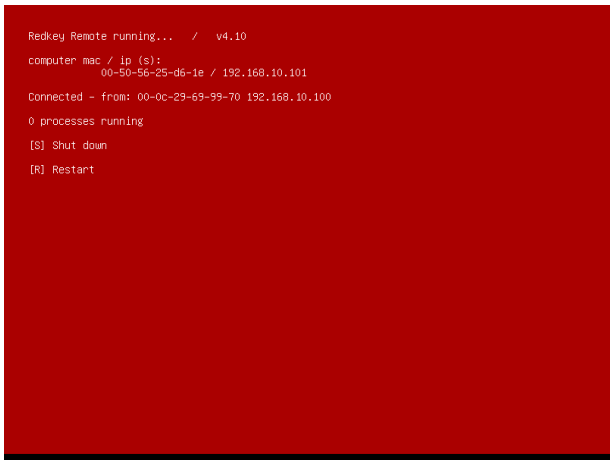
B. Set the remote computer(s) to boot via network
This is usually done by entering the BIOS menu at power up, and in boot settings menu selecting LAN Boot / Network boot as the first preferred option.

C. Power up or reboot the remote computer

D. Wait until the boot process completes and the remote wipe display is shown.

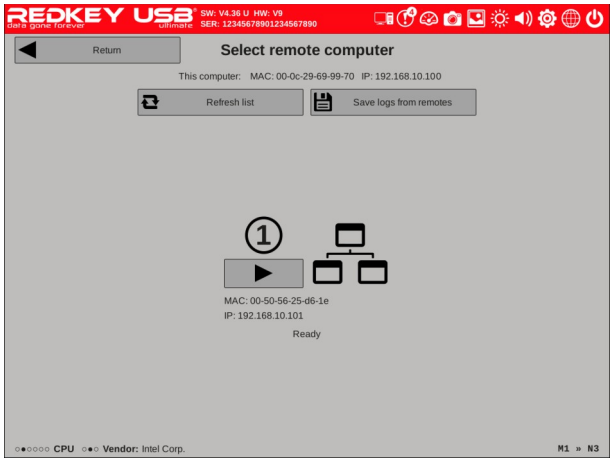
E. Within a few seconds the display should show ‘connected’ to indicate a connection is established with the main PC.

F. If more than one remote PC was connected to the main PC - the MAC and IP details can be noted to assist in identifying it on the list shown on the main PC.



G. On the main PC running Redkey, click ‘Refresh list’

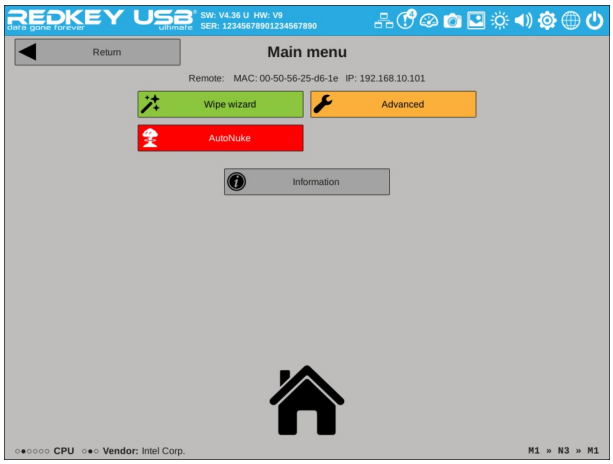
H. The remote computer should now show on the list of detected remote computers, select it to proceed.



I. The Top Bar will change color to blue to indicate the displays and operations now refer to a remote computer.

J. You can now proceed to wipe the remote PC using the same modes that are available for wiping local PCs as detailed in section 3.8 - Main Menu.

K. When done – the Exit Menu can be used to remotely shut down the remote computer.



10 Wipe Sequence

When starting the wipe from any mode, the wipe sequence will begin, the common wipe sequence steps and displays as detailed in this section.

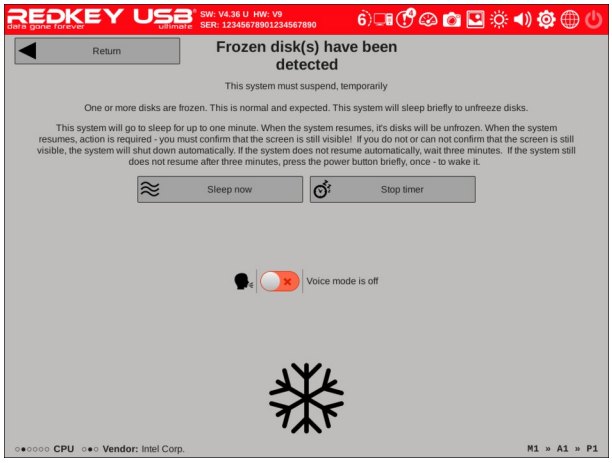
10.1 System Suspend

For SATA disks Redkey uses by default secure erase commands, in some systems at power up the BIOS places disks in a ‘Frozen’ state that does not allow to use these secure erase commands.

To ‘Unfreeze’ the disk and allow secure erase commands a system suspend is done.

If it is required to do a suspend, the suspend prompt will show before starting the wipe.

The prompt will only show if current settings require doing a suspend or if it was manually enabled by the user (using Advanced Menu).



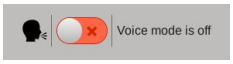
Options at this prompt:

- **Return** - Cancels starting the wipe and returns to the previous menu.
- **Skip** - Available when using Wipe Wizard™ or AutoNuke™, can be used on systems that are known to not support suspend properly, depending on the mode used after the suspend is skipped Redkey will either prompt to change settings (when using Wipe Wizard™) or automatically change them (when using AutoNuke™ mode).

(detail continues on next page)

- **Voice Mode Switch**

(only available when using Advanced Menu or AutoNuke™ mode)

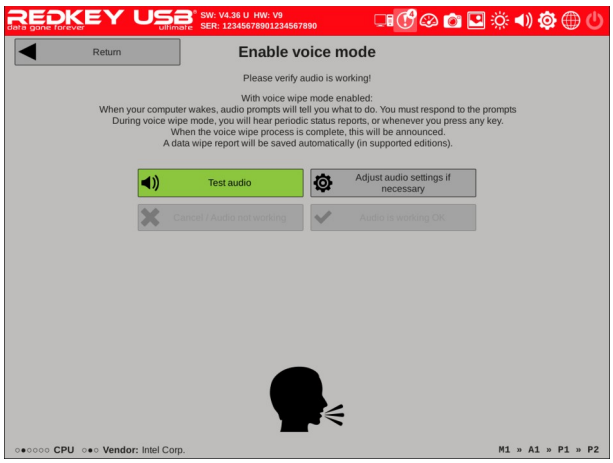


Voice mode is designed for systems in which suspend is not fully supported by the graphics drivers and the screen does not work properly after resuming from suspend.

Redkey offers a solution to these systems by providing the option to continue the wipe using voice readouts for progress and menu options.

When the voice mode switch is enabled, upon resuming from suspend the option to start wipe using voice mode will be available.

When enabling the voice mode switch this prompt will show to test and confirm the audio is working properly.

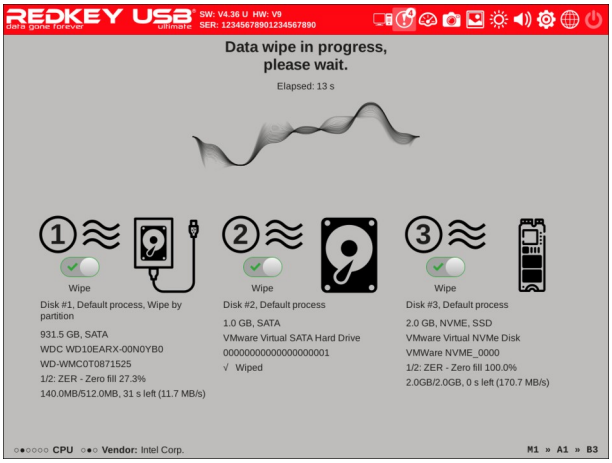


To Enable voice mode:

1. Click the ‘Test audio’ button
2. Listen if the test prompt is audible
3. Adjust audio settings if needed
4. Click ‘Audio is working ok’ button

10.2 Wipe Running Display

While the wipe is in progress, Redkey displays the progress of each disk and the total elapsed time.



10.2.1 Warning Statuses during wipe

Redkey monitors the wipe progress to identify if a wipe step is taking longer than expected, this is usually caused by the disk being in a degraded condition.

Warning are displayed with yellow/red highlight, alternating over the disk's current status (step # and time left).

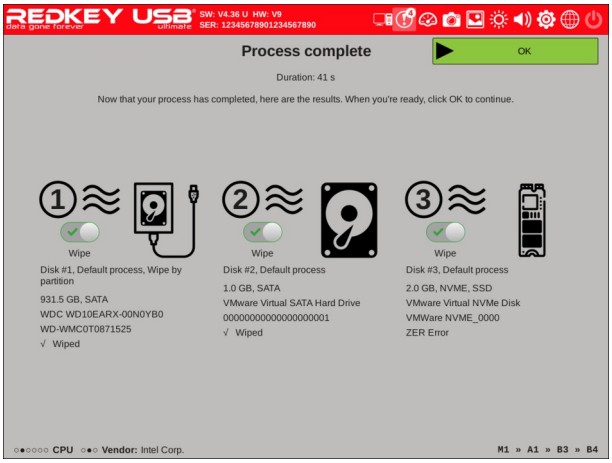
The following table details the possible warnings and their cause:

Warning	Detail
"Disk Response Slow. Disk/Sector may be Degraded"	While performing a binary fill or verify step, the write/read speed is much lower then can normally be expected.
"Overtime"	A SATA Secure Erase / Enhanced Secure Erase step is taking more than 5 minutes over the manufacturer estimated time to complete.
"Taking too long"	A SATA Secure Erase / Enhanced Secure Erase step is taking more than 45 minutes over the manufacturer estimated time to complete.

10.3 Process Complete prompt

When the wipe process is complete, a summery screen will show detailing:

- The total time duration
- Result wiping of each disk - disks that successfully wiped will show '√ Wiped' on their status.

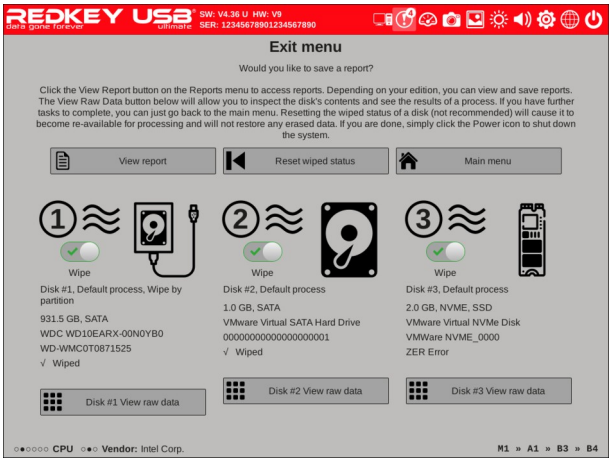


10.4 Wipe Complete Menu

In this menu are the tasks and functions that can be done when the wipe process is complete:

- View report – opens the View report menu, details in section 10.5 below.
- View raw data – a button under each disk will open the Raw data viewer to inspect its actual contents.

  See 6 - View Disk Raw Data for more details.

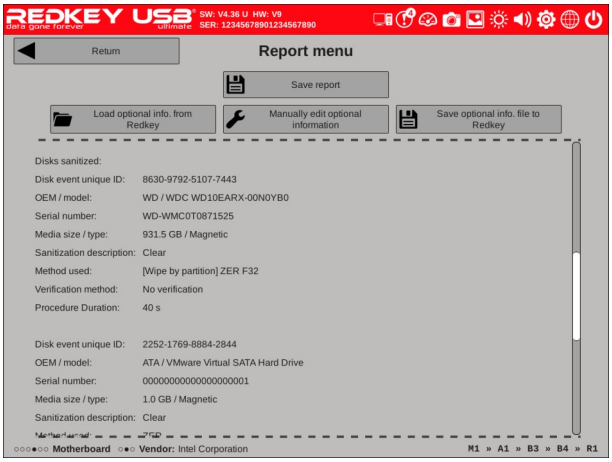


- Reset wiped status
  Once a defined wipe process has completed successfully, Redkey notes the disk as '√ Wiped', this state will prevent the disk from being wiped again unintentionally to save time.
  The 'Reset wiped status' will clear this status from all disks to allow wiping the disk again.

10.5 View Report Menu

From the View Report menu you can:

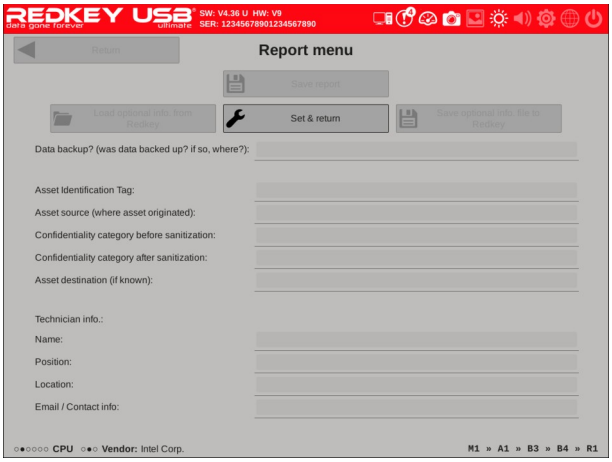
- View the wipe report
- Edit user fillable report fields. `Ultimate`
- Save a PDF report to the Redkey USB / Other device. `Pro & Ult`



`Ultimate` - Click the ‘edit optional Information’ button to switch to edit mode, once done press ‘Set & return’ to return.

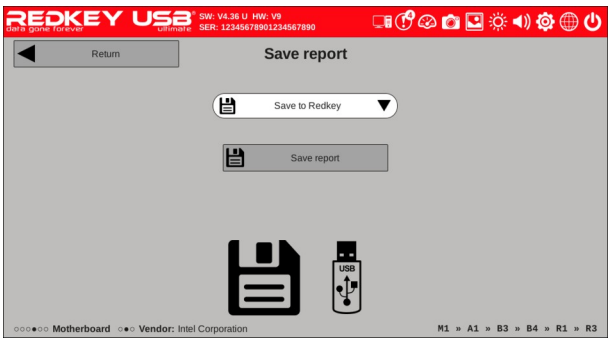
The texts entered can be saved to the Redkey USB for use in next runs by clicking the ‘Save Optional info’ button.

To load previously saved texts – use the ‘Load optional info’ button.

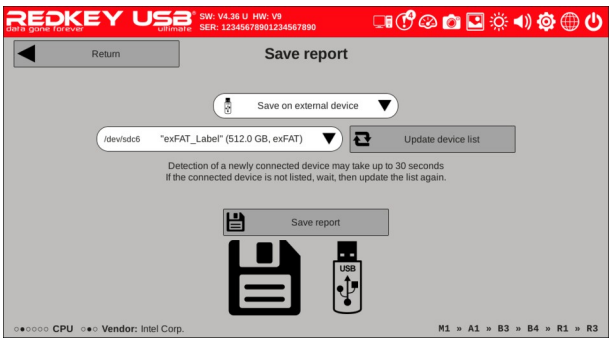


`Pro & Ult` - the ‘Save report’ menu can save a PDF report to the Redkey USB itself or to an external device

Saving a report to the Redkey USB:



Saving a report to an external device:
* the external device must be connected only after the wipe has completed ! *



11 Default Wipe Settings

The following table details the default settings and function priority as applied to different disk types.

These settings are used when using the basic mode (Main Menu) and when resetting the settings to default for all disks or for a single disk.

Refer to these following sections for detail regarding the terms and codes used:

- 12.1 - Internal Wipe Methods for SATA disks
- 12.2 - Other SATA Functions
- 12.3 - Internal Wipe Methods for NVMe devices
- 13 - Binary Wipe Methods
- 15.2 - Process Codes

	SATA Disks	NVME Disks	Flash & External (USB) SATA
Security Options:	**HPA**	**-**	**-**
	DCO	**-**	**-**
	FLU*	**FLU***	**-**
	* FLU refers to enabling the 'Flush Cache' option. (see section 16.1)		
Erase Method:			
1st Priority (if supported):	**SAN**	**NSR**	**-**
2nd Priority (if supported):	**ESE**	**NFR**	**-**
3rd Priority (if supported):	**SER**	**-**	**-**
4th Priority:	**ZER**	**ZER**	**ZER**
Trim:	**TRM** (for SSD only)	**TRM** (for SSD only)	**TRM** (External SATA SSD only)
Partition:	**-**	**-**	**PRT** (for external only)
Format:	**-**	**-**	**F32** (smaller than 1.5TB) **FAT** (larger than 1.5TB) (both for external only)

12 Disk functions used

12.1 Internal Wipe Methods for SATA disks

General

Methods detailed are commands to the disks as specified by the ATA standard.
Data erasure is performed internally by the disk's own firmware.

A specific disk might support only some (or even none) of the detailed functions.

Secure Erase

Fills the disk with binary zeros.

Once started the operation does not provide indication of the progress,
estimated time to complete is provided beforehand.

Enhanced Secure Erase

Fills the disk with a binary data pattern defined by the disk's manufacturer.

The pattern is designed to prevent any extraction of previous content from the disk's physical media. In some disks the pattern written is zeros.

Once started the operation does not provide indication of the progress,
estimated time to complete is provided beforehand.

Sanitize

The method is intended for Solid State drives and activates an erase function of the internal storage medium (usually flash devices).

The method provides with progress status while the erase is performed.

Sanitize Crypto Scramble

This method is intended for SED devices and makes any currently stored data unrecoverable by changing the internal encryption key.

Sanitize Overwrite

Similar to the Secure Erase command, this command overwrites the medium with zeros.

12.2 Other SATA Functions

HPA

Remove any Host Protected Area setting – an area the disk ‘hides’ from any installed O/S.

DCO

Resets Device Configuration Overlay, a setting that might ‘hide’ advanced disk functions.

12.3 Internal Wipe Methods for NVMe devices

General

Methods detailed are commands to the disks as specified by the NVMe standard.
Data erasure is performed internally by the drive’s own firmware.

A specific device might support only some (or even none) of the detailed functions.

NVME Format

Performs Secure Erase similar to the SATA Secure Erase Command

NVME Format Crypto Scramble

This method is intended for SED devices and makes any currently stored data unrecoverable by changing the internal encryption key.

NVME Sanitize

Performs Secure Erase similar to the SATA Sanitize command, and provides with progress status while the erase is performed.

NVME Sanitize Crypto Scramble

This method is intended for SED devices and makes any currently stored data unrecoverable by changing the internal encryption key.

12.4 SSD Trim

Trim command informs the SSD hardware that the storage space is unused, this allows for better management of the storage medium’s wear distribution and optimization.

13 Binary Wipe Methods

13.1 Zero Fill

Fills the entire area of the media with binary zeros.

13.2 One Fill

Fills the entire area of the media with binary ones

13.3 Random Fill

Fills the entire area of the media with random data.
The fill data is generated by a 48 bit pseudo-random generating function (LRAND48), which is initialized by system generated random data.
Initializing data is kept in RAM to allow a Verify step to produce the same data for compare.

Also see - 13.5 - Random Fill Methods Illustration

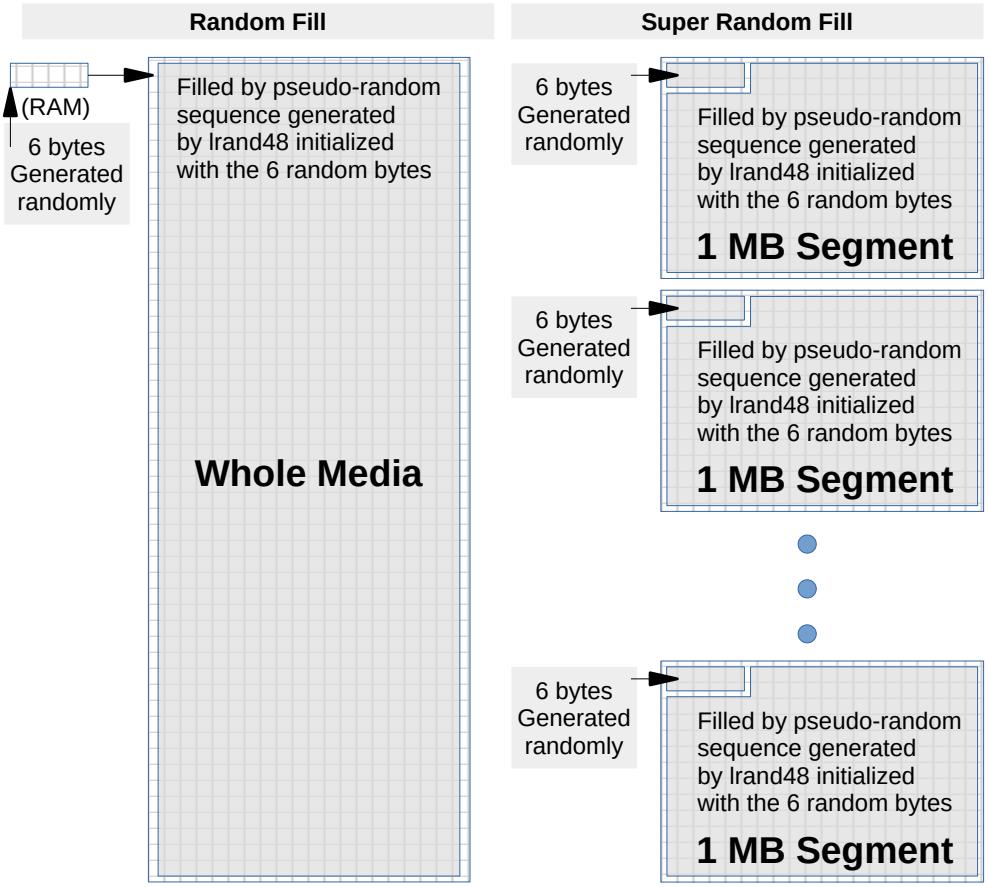
13.4 Super Random Fill

An augmented version of the Random Fill method, the random generating function is re-initialized with new system random data for each 1MB segment of the disk.

In each 1MB segment the initializing system random data is first saved to allow a Verify step to produce the same data for compare, the rest of the 1MB segment's area is filled with the random data produced by the 48 bit pseudo-random generating function.

Also see - 13.5 - Random Fill Methods Illustration

13.5 Random Fill Methods Illustration



14 Binary Verify Methods

14.1 Full Verify

Reads back the entire area of the media and compares to the expected contents according to the last binary fill step performed.

14.2 Quick Verify

Reads back 10% of the media and compares to expected content to provide a quick test.
The sample area is randomly selected, in 1MB segments - for each 1MB segment, a 10% / 90% 'coin toss' is done to decide if to verify it or not.
This results in a verify of 10% of the media's area randomly spread across the entire area.

15 Supported Standards

15.1 Standards List

The following table lists the standards supported by Redkey:

#	KB Key	Code	Standard / Algorithm	Process * See Process Codes table in section 15.2 * In green – SATA Only * In blue – Alternate Action for NVME
0	0	**ZER**	Zero Fill	ZER
1	1	**ONE**	One Fill	ONE
2	2	**ARQ**	Aperiodic Random Overwrite	RND
3	3	**ARO**	Aperiodic Random Overwrite with Verify	RND VER
4	4	**AIR**	Air Force System Security Instruction 5020	ZER ONE ZER RND VRQ
5	5	**AUZ**	Australian Government Information Security Manual AGISM	Size < 15GB: HPA DCO RND RND RND VER SER/NFR Size >= 15GB: HPA DCO RND VER SER/NFR
6	6	**BRU**	Bruce Schneier's Algorithm	ONE ZER RND RND RND RND RND
7	7	**BSI**	BSI-GS	HPA DCO ZER ONE ZER ONE ZER ONE ZER ONE SER/NFR VER
8	8	**BSG**	BSI-GSE	HPA DCO ZER RND ONE ZER ONE ZER ONE ZER ONE SER/NFR VER
9	9	**CES**	CESG CPA – Higher Level	HPA DCO RND RND RND VER
10	A	**DOD**	DoD 5220.22 M	ZER ONE RND VER
11	B	**DOM**	DoD 5220.22 M ECE	ZER ONE RND VER RND ZER ONE RND VER
12	C	**NIC**	NIST 800-88 Clear	HPA DCO ZER VER
13	D	**NIP**	NIST 800-88 Purge	HPA DCO SER/NFR ZER VER
14	E	**HML**	HMG Infosec Standard 5, Lower Standard	HPA DCO ZER VER
15	F	**HMG**	HMG Infosec Standard 5, Higher Standard	HPA DCO ONE ZER RND VER
16	G	**NCS**	National Computer Security Center NCSC-TG-025	ZER VER ONE VER RND VER
17	H	**NAV**	Navy Staff Office Publications NAVSO P-5239-26	ZER ONE RND VER
18	I	**NSA**	NSA 130-1	RND RND ZER VER
19	J	**OPN**	OPNAVINST 5239.1A	RND ZER ZER VER

(Table continues on next page)

Standards List (continued):

#	KB Key	Code	Standard / Algorithm	Process * See Process Codes table in section 15.2 * In green – SATA Only * In blue – Alternate Action for NVME
20	K	**PGA**	Peter Gutmann's Algorithm	35 steps, detailed in section 15.3
21	L	**USA**	U.S. Army AR380-19	RND ZER ONE VER
22	M	**RCM**	Royal Canadian Mounted Police RCMP TSSIT OPS-II	ZER ONE ZER ONE ZER ONE RND VER
23	N	**RK1**	Redkey Data Wipe Level 1	HPA DCO SER/NFR SRN ZER VER TRM
24	O	**RK2**	Redkey Data Wipe Level 2	HPA DCO CRY/NSC SRN SAN/NSR ONE ESE/NFR ZER SER/NFR ZER VER TRM

15.2 Process Codes

The following table lists the process codes used throughout the application:

Code	Detail
	Binary Options
ZER	Zero Fill
ONE	One Fill
RND	Random Fill
SRN	Super Random Fill
VER	Verify
VRQ	Verify 10%
	Security Options (SATA)
HPA	Remove Host Protected Area
DCO	Reset Device Configuration Overlay
	Internal Erase Options (SATA)
SER	ATA Secure Erase
ESE	ATA Enhanced Secure Erase
SAN	ATA Sanitize
CRY	ATA Sanitize Crypto Scramble
SOV	ATA Sanitize Overwrite
	Internal Erase Options (NVME)
NFR	NVME Format
NCR	NVME Format Crypto Scramble
NSR	NVME Sanitize
NSC	NVME Sanitize Crypto Scramble
	Post Wipe Options
PRT	Partition Disk
PAC	Make Partition Active
FAT	Quick Format exFAT
F32	Quick Format FAT32
NTF	Quick Format NTFS
EX4	Format ext4
EX3	Format ext3
EX2	Format ext2

15.3 Peter Gutmann's Algorithm

The following table details the steps in Peter Gutmann's Algorithm:

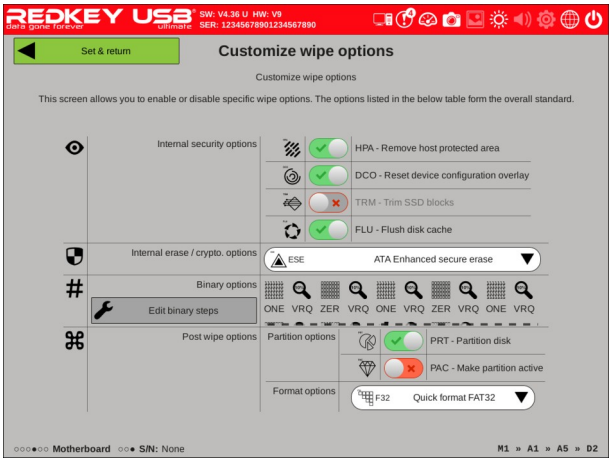
Step	Binary Fill Pattern:
1	Random Data
2	Random Data
3	Random Data
4	Random Data
5	55h 55h 55h
6	AAh AAh AAh
7	92h 49h 24h
8	49h 24h 92h
9	24h 92h 49h
10	00h 00h 00h
11	11h 11h 11h
12	22h 22h 22h
13	33h 33h 33h
14	44h 44h 44h
15	55h 55h 55h
16	66h 66h 66h
17	77h 77h 77h
18	88h 88h 88h

Step	Binary Fill Pattern:
19	99h 99h 99h
20	AAh AAh AAh
21	BBh BBh BBh
22	CCh CCh CCh
23	DDh DDh DDh
24	EEh EEh EEh
25	FFh FFh FFh
26	92h 49h 24h
27	49h 24h 92h
28	24h 92h 49h
29	6Dh B6h DBh
30	B6h DBh 6Dh
31	DBh 6Dh B6h
32	Random Data
33	Random Data
34	Random Data
35	Random Data

16 Customizing the wipe sequence

Redkey allows to create a customized wipe sequence, this is done by:

1. Entering the Advanced Menu (see 5 - Advanced Menu)
2. Selecting ‘Disk Options’ (see 5.7 - Disk Options Menu)
3. Selecting ‘Customize Wipe Options’



16.1 Internal Security Options Pro & Ult

HPA & DCO – See 12.2 - Other SATA Functions. (Only enabled for SATA disks)

TRM – See 12.4 - SSD Trim. (Only enabled for SSDs)

FLU – When enabled the disk’s controller will be commanded to flush any pending writes from the controller’s write cache into the actual storage medium, at the end of each wipe step.

16.2 Internal Erase/Crypto Options Pro & Ult

Sets the internal erase method to use, only options supported by the selected disk are enabled.

If ‘None’ is selected, a binary Zero Fill step will be added instead.

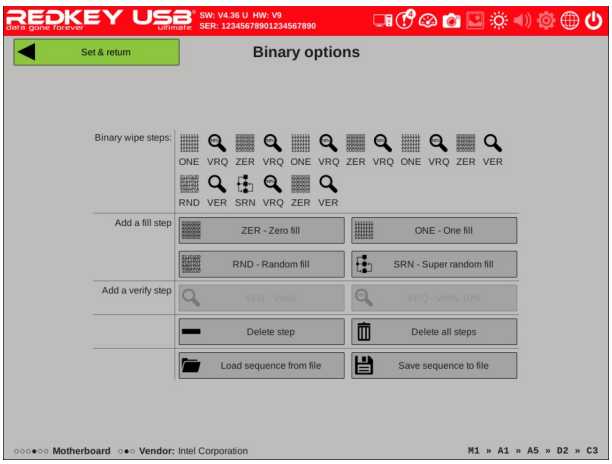
16.3 Binary Options Pro & Ult

Click ‘Edit binary steps’ to open the ‘Binary options menu.

The menu allows to create, edit, save and load a customized binary wipe sequence.

For more detail about the available binary wipe methods see these sections:

13 - Binary Wipe Methods
14 - Binary Verify Methods



16.4 Post Wipe Options

Sets whether a disk will be partitioned and formatted following the wipe, and to select to preferred format file system.

* To enable formatting, partitioning must first be enabled.

17 Scripting Ultimate

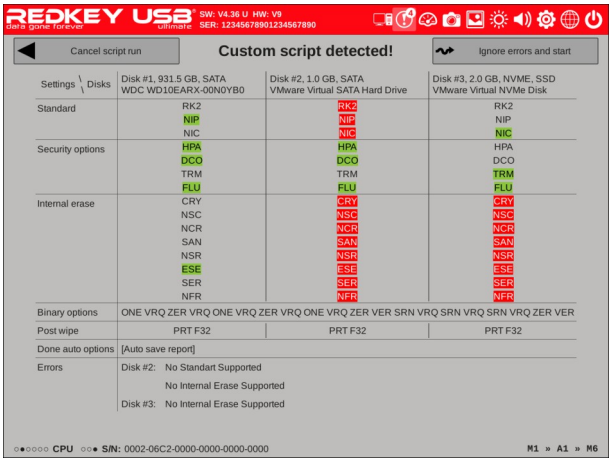
The scripting feature enables to use a script file that defines a custom wipe sequence, this script can include:

- ✶ Custom priorities for the internal erase functions used
- ✶ Selecting pre-set standard(s) to be used (a prioritized list, first applicable used)
- ✶ Defining a custom sequence of binary wipe steps
- ✶ Enabling additional features – auto-saving a report and auto-shutdown when complete.

The script file is named ‘customscript.txt’ and is located at the root folder of the Redkey USB.

See the file itself for further information on the syntax and usage.

When an enabled script file is detected, Redkey will automatically enter Advanced Mode (skipping the Main Menu) and attempt to apply the script it to all disks.



The results are then displayed to show:

- Which of the defined priority / functions are selected for each disk
- Any functions defined that could not be applied

The color legend used in this screen:

Green - Enabled Function / Selected Option.

Red - Indicates an apply error – when none of the priorities defined is supported.

If the script can be applied fully (no apply errors), the wipe will auto-start after a timer countdown.

If some apply error occurred, Redkey will stop at this screen (as shown above), ‘Ignore errors and start’ can be selected to continue with the wipe if so preferred.

18 Options File

The options file is a file named ‘donotmodify.txt’ located at the root folder of the Redkey USB.
This file controls enabling / disabling some of the functions of the Redkey application.

Please Note:
The detail in this section is provided for informational purposes only.
Any modification of the options file is:
1. Not supported.
2. Violates the End User License Agreement.
3. Will void any warranty provided by Redkey.

Each option can be set by the option’s label followed by a space and ‘False’ or ‘True’.
All the options are disabled by default.

Label	Detail
OPT_01	**ATA Commands for USB Devices** ATA commands are used with SATA disks for HPA, DCO and Internal Erase functions (See sections 12.1 & 12.2 for more details). by default the application will not use these commands with disks connected via a USB connection as it’s not safe to do so. Enabling this function will enable these functions for disks connected via USB.
OPT_02	**Internal Erase Command - Sanitize Overwrite (SOV)** Sanitize Overwrite Internal Erase method (see section 12.1) has been reported to cause problems with some disks. By default the application will not allow to select it from the Internal Erase/Crypto Options menu (see 16.2), Enabling this option will allow to select it.
OPT_03	**Advanced disk option 4 - Lock disk with a password** Enable to use this option in the Disk Management Menu (see section 7).
OPT_04	**Advanced disk option 6 - Set HPA 50%** Enable to use this option in the Disk Management Menu (see section 7).
OPT_05	**Advanced disk option 8 - Freeze Disk** Enable to use this option in the Disk Management Menu (see section 7).
OPT_06	**Screen Saver Disable** - disables the screen saver function.
OPT_07	**Music Tracks Disable** - disables the music tracks function (during screen saver).

(Table continues on next page)

OPT_08	**Wipe Disable - Local Computer** Disables all wipe and formatting functions from being done on the local computer (computer running redkey).
OPT_09	**Wipe Disable - Remote Computer** Disables all wipe and formatting functions from being done on any remote PC connected via LAN in remote wipe mode.
OPT_10	**Wipe Disable - Mobile Devices** Disables all wipe functions of mobile devices (Apple & Android devices).
OPT_11	**AutoNuke Mode Disable** Disables using AutoNuke mode.
OPT_T_01	**Disable Timer - UI Menu**
OPT_T_02	**Disable Timer - Resolution Select**
OPT_T_03	**Disable Timer - Language Select**
OPT_T_04	Not used.
OPT_T_05	**Disable Timer - Script Apply Results**
OPT_LANG	**Language select preset, using one of the codes below:**
OPT_LOG	**Enables debug logging.**

Code	Language	Code	Language
eng_us	english (US)	nyo	norsk
eng_uk	english (UK)	por	português
eng_ca	english (CA)	fin	suomi
eng_au	english (AU)	pol	polski
deu	deutsch	jap	日本人
spa	español	kor	**한국어**
fre	français	rus	русский
swe	svenska	tur	türkçe
ned	nederlands	chi	中文(简体)
ita	italiano	hin	हिंदी

19 Serial port mode

For wiping computers which do not contain a video output (or ones with a display fault) Redkey supports using the PC serial port (COM1) for both the display and user input.

This support exists for when booting a PC using the Redkey directly and when using remote wipe mode.

19.1 Regular serial mode

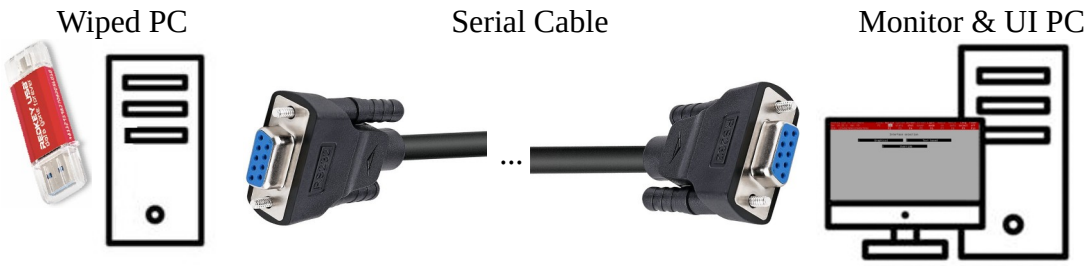
To use this mode the Redkey USB key must first be configured to run in serial port mode, this can be done using the Redkey Updater's Settings menu – set the serial port mode switch to 'On', confirm the warning prompt and press 'Update Settings'.

Alternatively – if required to switch the mode without the updater – it can also be done using the batch files found in the 'Mode_Switch' folder on the USB, run 'set_serial.bat' to enable or 'set_video.bat' to reset to regular mode.

Please mind that when serial port mode is enabled all application displays are routed via the serial port only !

No application displays will show on the regular video monitor and it might seem as the application is not running, unless viewing via a serial port terminal

Connection diagram:



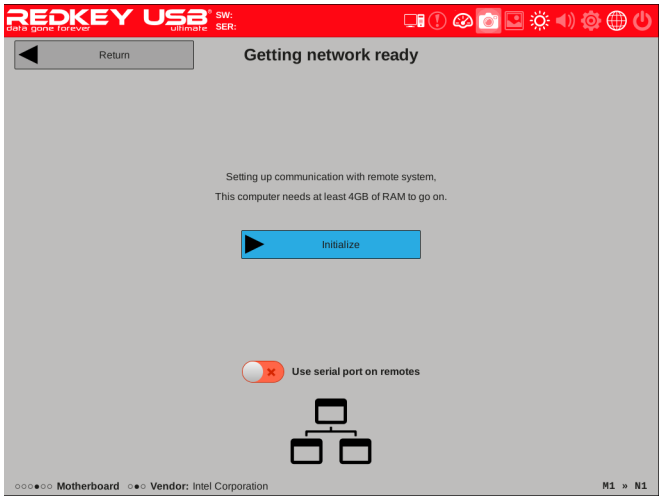
Connection settings:

Set serial port on the monitor PC to use baud rate of 38400.
To use Fn keys (Topbar functions) from the terminal application on the monitor PC should be set to to use one of these keyboard mode options: 'ESC[n~' / 'Linux' / VT400. (the PuTTY terminal application has these settings under Settings > Terminal > Keyboard).

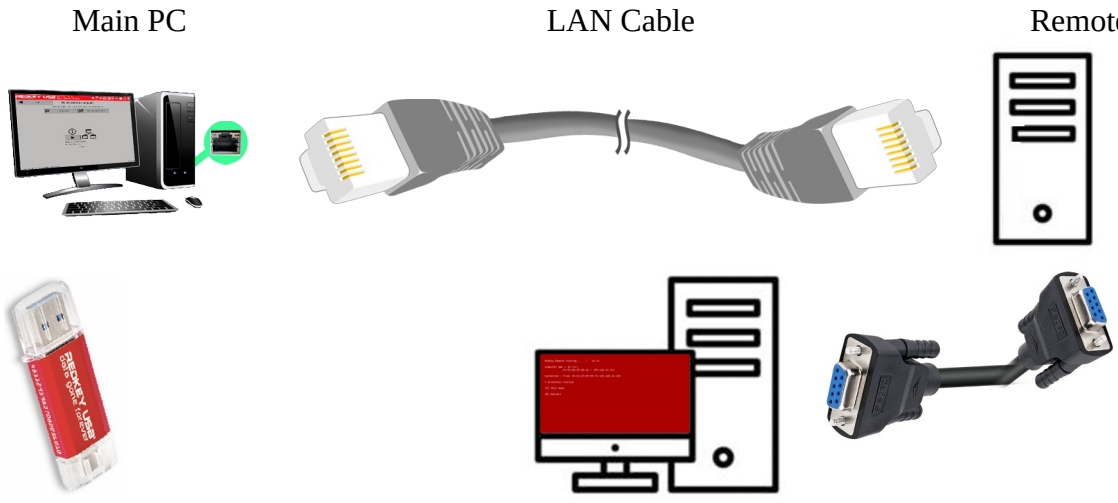
19.2 Serial mode when running remote wipe

When wiping a PC using remote wipe (as detailed in section 9), the display of the remote PC can also be routed to a serial port instead of the video monitor.

To enable this mode, before initializing remote wipe set the switch at the bottom of the screen to ‘on’. Any remote PC booting via LAN will use the serial port instead of the video display. (screenshot below shows the switch in regular mode before enabling it)



Connection diagram:



20 Troubleshooting options guide

Problem	Steps	
Cannot boot Redkey	1	Refer to section 2.1 - Booting up
Application does not start	1	At the Boot Options menu (see in 2.2 - Redkey Boot Options) select: ‘Override’ > ‘Load - x86 (32 bit) - Display Load Detail’
	2	select: ‘Override’ > ‘Load - x64 (64 bit) - Display Load Detail’
Cannot run in graphical (GUI) mode	1	At the Redkey Boot Menu (see in 2.2 - Redkey Boot Options) select ‘Override’
	2	Select ‘Resolution Troubleshooting Options’
	2	Try each of the options in that menu
	4	If none help – Use the Text Interface for that computer. Select one of the ‘Text Interface Only’ options in the boot menu if a warning shows in the Interface Selection menu.
Dell PCs: Disks not recognized	1	Reset the computer, press F12 to enter the Boot menu
	2	Select ‘BIOS Setup’
	3	Enter the ‘System information’ / ‘System Configuration’ menu
	4	If the setting for ‘SATA Operation’ is set to ‘RAID ON’ change it to ‘AHCI’.
A Disk is locked after power failed during wipe	1	If prompted by the BIOS to enter a password at startup - Do not enter a password (leave the disk locked)
	2	Re-Start the Redkey application, it will unlock the disk automatically at start-up.
	3	If the disk still shows as ‘Locked’ – Use the ‘Unlock Disk failed during wipe process’ function (see section 7.3)

(Table continues on next page)

Troubleshooting options guide (continued):

Problem	Steps		
Suspend Fails to resume	1	**See of section 2.1 - Booting up - par. D:** Prefer boot options that say ‘EFI’ / ‘UEFI’ over ones that say ‘BIOS’ / ‘Legacy’	
	2	**If sound prompts are audible after suspend resumes:**	
		A	Use Advanced Menu instead of other modes
		B	At the suspend prompt enable ‘Voice Mode’ (see 10.1 - System Suspend)
		C	Select ‘Suspend Now’
		D	Follow the voice instructions
	3	**If no sound prompts are audible after suspend resumes:**	
		If using **Advanced Menu**:	
		A	Manually disable doing a suspend (see 5.6 - Suspend Switch)
		B	Select ‘Disable suspend, and binary wipe any frozen disks’ when prompted.
		If using the **Wipe Wizard™** or **AutoNuke™** mode:	
		A	At the suspend prompt select ‘Skip’
		B	Select ‘Disable suspend, and binary wipe any frozen disks’ if prompted.
Samsung NVME Internal Erase methods Fail		If either NFR, NCR, NSR, NSC method fails with one of the NVME models listed below – Use Advanced mode and manually **enable** the suspend switch. (see 5.6 - Suspend Switch). Known problem models: Samsung PM951 / MZFLV256HCHP-000MV Samsung PM981 / MZVLB256HAHQ-000L7 Samsung PM981a	

(Table continues on next page)

Troubleshooting options guide (continued 2):

Other	1	Start Redkey and when reaching the Main Menu, use the TopBar to open the Media settings menu, set the Logging switch to enabled
	2	Perform again the same action that fails or does not work as expected, when done use the Exit Menu to safely shut down the PC.
	3	Connect the Redkey USB to another computer and copy from it the ‘Logs’ folder, compress the folder into a ZIP file if possible.
	4	Contact contact@redkeyusb.com, detail the problem encountered, and attach the log files copied.

20.1 Server RAID setup

For cases requiring high data security it is recommended to remove the disks and wipe them by connecting them to a PC that does not use a RAID controller where direct access to the disk would be possible to enable internal erase functions

On servers in which the disks are connected via a RAID controller it is required to properly setup **all the connected** disks to be used as part of a logical RAID device in order for Redkey to be able to access them and wipe contained data.

Any physical disk that is not defined as part of a RAID will not be detected and therefor not wiped by Redkey.

It is recommended to setup the RAID in RAID 0 mode and as one logical disk for best performance.

Below are instruction for setup on common server types:

Dell Servers:

1. **S**tart by rebooting your computer.
2. When the option becomes available, press Ctrl+R.
3. In the RAID configuration menu, scroll to the PERC and press F2, which allows you to access operations.
4. Clear the current configuration and confirm your decision.
5. Scroll back to the PERC and press F2 again to create a new Virtual Disk (VD).
6. Select RAID 0 and highlight each disk using the space bar, this will display the total disk size.
7. Confirm by hitting OK and skip the initialization for now.
8. Instead, scroll to the new VD and select 'Fast Init' for initialization.
9. After seeing the 'Initialization Complete' message, escape and exit the process. You will then be prompted to press Ctrl+Alt+Del to reboot.

HP Servers:

1. Firstly, reboot your computer.
2. When you see the message "Press any key to view optional ROM messages," press any key to enter the optional ROM configuration for the array menu.
3. Once there, delete the existing logical drives.
4. Press F8 to select this operation, then F3 to confirm and enter to continue.
5. Proceed to create a single logical drive and select all available physical drives. Opt for RAID 0 as the RAID configuration. Press enter, then F8 to save the changes, followed by enter again to continue. Finally, escape to exit the process.