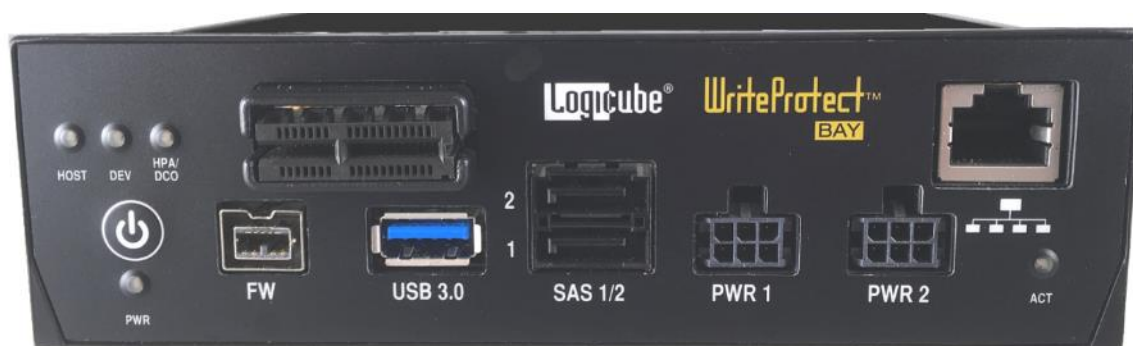




WriteProtect™ BAY User's Manual



Logicube, Inc.
Chatsworth, CA 91311
USA
Phone: 818 700 8488
Fax: 818 700 8466

Version: 2.1
Date: 09/19/2018
MAN-WP-BAY

Limitation of Liability and Warranty Information

Logicube Disclaimer

LOGICUBE IS NOT LIABLE FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO PROPERTY DAMAGE, LOSS OF TIME OR DATA FROM USE OF A LOGICUBE PRODUCT, OR ANY OTHER DAMAGES RESULTING FROM PRODUCT MALFUNCTION OR FAILURE OF (INCLUDING WITHOUT LIMITATION, THOSE RESULTING FROM: (1) RELIANCE ON THE MATERIALS PRESENTED, (2) COSTS OF REPLACEMENT GOODS, (3) LOSS OF USE, DATA OR PROFITS, (4) DELAYS OR BUSINESS INTERRUPTIONS, (5) AND ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE (OR FROM DELAYS IN SERVICING OR INABILITY TO RENDER SERVICE ON ANY) LOGICUBE PRODUCT.

LOGICUBE MAKES EVERY EFFORT TO ENSURE PROPER OPERATION OF ALL PRODUCTS. HOWEVER, THE CUSTOMER IS RESPONSIBLE TO VERIFY THAT THE OUTPUT OF LOGICUBE PRODUCT MEETS THE CUSTOMER'S QUALITY REQUIREMENT. THE CUSTOMER FURTHER ACKNOWLEDGES THAT IMPROPER OPERATION OF LOGICUBE PRODUCT AND/OR SOFTWARE, OR HARDWARE PROBLEMS, CAN CAUSE LOSS OF DATA, DEFECTIVE FORMATTING, OR DATA LOADING. LOGICUBE WILL MAKE EFFORTS TO SOLVE OR REPAIR ANY PROBLEMS IDENTIFIED BY CUSTOMER, EITHER UNDER WARRANTY OR ON A TIME AND MATERIALS BASIS.

Warranty

DISCLAIMER

IMPORTANT - PLEASE READ THE TERMS OF THIS AGREEMENT CAREFULLY. BY INSTALLING OR USING LOGICUBE PRODUCTS, YOU AGREE TO BE BOUND BY THIS AGREEMENT.

IN NO EVENT WILL LOGICUBE BE LIABLE (WHETHER UNDER THIS AGREEMENT, RESULTING FROM THE PERFORMANCE OR USE OF LOGICUBE PRODUCTS, OR OTHERWISE) FOR ANY AMOUNTS REPRESENTING LOSS OF PROFITS, LOSS OR INACCURACY OF DATA, LOSS OR DELAYS OF BUSINESS, LOSS OF TIME, COSTS OF PROCUREMENT OF SUBSTITUTE GOODS, SERVICES, OR TECHNOLOGY, PROPERTY DAMAGE, OR INDIRECT, CONSEQUENTIAL, OR PUNITIVE DAMAGES OF A PURCHASER OR USER OF LOGICUBE PRODUCTS OR ANY THIRD PARTY. LOGICUBE'S AGGREGATE LIABILITY IN CONTRACT, TORT, OR OTHERWISE (WHETHER UNDER THIS AGREEMENT, RESULTING FROM THE PERFORMANCE OR USE OF LOGICUBE PRODUCTS, OR OTHERWISE) TO A PURCHASER OR USER OF LOGICUBE PRODUCTS SHALL BE LIMITED TO THE AMOUNT PAID BY THE PURCHASER FOR THE LOGICUBE PRODUCT. THIS LIMITATION OF LIABILITY WILL BE EFFECTIVE EVEN IF LOGICUBE HAS BEEN ADVISED OF THE POSSIBILITY OF ANY SUCH DAMAGES.

LOGICUBE MAKES EVERY EFFORT TO ENSURE PROPER OPERATION OF ITS PRODUCTS. HOWEVER, THE PURCHASER IS RESPONSIBLE FOR VERIFYING THAT THE OUTPUT OF A LOGICUBE PRODUCT MEETS THE PURCHASER'S REQUIREMENTS. THE PURCHASER FURTHER ACKNOWLEDGES THAT IMPROPER OPERATION OF LOGICUBE PRODUCTS CAN CAUSE LOSS OF DATA, DEFECTIVE FORMATTING, OR DEFECTIVE DATA LOADING. LOGICUBE WILL MAKE EFFORTS TO SOLVE OR REPAIR ANY PROBLEMS IDENTIFIED BY PURCHASER, EITHER UNDER THE WARRANTY SET FORTH BELOW OR ON A TIME AND MATERIALS BASIS.

LIMITED WARRANTY

FOR ONE YEAR FROM THE DATE OF SALE (THE "WARRANTY PERIOD") LOGICUBE WARRANTS THAT THE PRODUCT (EXCLUDING CABLES, ADAPTERS, AND OTHER "CONSUMABLE" ITEMS) IS FREE FROM MANUFACTURING DEFECTS IN MATERIAL AND WORKMANSHIP. THIS LIMITED WARRANTY COVERS DEFECTS ENCOUNTERED IN THE NORMAL USE OF THE PRODUCT DURING THE WARRANTY PERIOD AND DOES NOT APPLY TO: PRODUCTS DAMAGED DUE TO PHYSICAL ABUSE, MISHANDLING, ACCIDENT, NEGLIGENCE, OR FAILURE TO FOLLOW ALL OPERATING INSTRUCTIONS CONTAINED IN THE OPERATING MANUAL; PRODUCTS WHICH ARE MODIFIED; PRODUCTS WHICH ARE USED IN ANY MANNER OTHER THAN THE MANNER FOR WHICH THEY WERE INTENDED, AS SET FORTH IN THE OPERATING MANUAL; PRODUCTS WHICH ARE DAMAGED OR DEFECTS CAUSED BY THE USE OF UNAUTHORIZED PARTS OR BY UNAUTHORIZED SERVICE; PRODUCTS DAMAGED DUE TO UNSUITABLE OPERATING OR PHYSICAL CONDITIONS DIFFERING FROM THOSE RECOMMENDED IN THE OPERATING MANUAL OR PRODUCT SPECIFICATIONS PROVIDED BY LOGICUBE; ANY PRODUCT WHICH HAS HAD ANY OF ITS SERIAL NUMBERS ALTERED OR REMOVED; OR ANY PRODUCT DAMAGED DUE TO IMPROPER PACKAGING OF THE WARRANTY RETURN TO LOGICUBE. AT LOGICUBE'S OPTION, ANY PRODUCT PROVEN TO BE DEFECTIVE WITHIN THE WARRANTY PERIOD WILL EITHER BE REPAIRED OR REPLACED USING NEW OR REFURBISHED COMPONENTS AT NO COST. THIS WARRANTY IS THE SOLE AND EXCLUSIVE REMEDY FOR DEFECTIVE PRODUCTS. IF A PRODUCT IS HAS BECOME OBSOLETE OR IS NO LONGER SUPPORTED BY LOGICUBE THE PRODUCT MAY BE REPLACED WITH AN EQUIVALENT OR SUCCESSOR PRODUCT AT LOGICUBE'S DISCRETION. THIS WARRANTY EXTENDS ONLY TO THE END PURCHASER OF LOGICUBE PRODUCTS. THIS WARRANTY DOES NOT APPLY TO, AND IS NOT FOR THE BENEFIT OF, RESELLERS OR DISTRIBUTORS OF LOGICUBE PRODUCTS. UNLESS OTHERWISE AGREED IN WRITING BY LOGICUBE, NO WARRANTY IS PROVIDED TO RESELLERS OR DISTRIBUTORS OF LOGICUBE PRODUCTS.

IN ORDER TO RECEIVE WARRANTY SERVICES CONTACT LOGICUBE'S TECHNICAL SUPPORT DEPARTMENT VIA PHONE OR E-MAIL. PRODUCTS RETURNED TO LOGICUBE FOR REPAIR UNDER WARRANTY MUST REFERENCE A LOGICUBE RETURN MATERIAL AUTHORIZATION NUMBER ("RMA"). ANY PRODUCT RECEIVED BY LOGICUBE WITHOUT AN RMA# WILL BE REFUSED AND RETURNED TO PURCHASER. THE PURCHASER MUST CONTACT LOGICUBE'S TECHNICAL SUPPORT DEPARTMENT VIA E-MAIL (SUPPORT@LOGICUBE.COM) OR VIA PHONE AT +1-818-700-8488 OPT. 3 TO OBTAIN A VALID RMA#. THE PURCHASER MAY BE REQUIRED TO PERFORM CERTAIN DIAGNOSTIC TESTS ON A PRODUCT PRIOR TO LOGICUBE ISSUING AN RMA#. THE PURCHASER MUST PROVIDE THE PRODUCT MODEL, SERIAL NUMBER, PURCHASER NAME AND ADDRESS, EMAIL ADDRESS AND A DESCRIPTION OF THE PROBLEM WITH AS MUCH DETAIL AS POSSIBLE. AT LOGICUBE'S SOLE AND ABSOLUTE DISCRETION, REASONABLE TELEPHONE AND EMAIL SUPPORT MAY ALSO BE AVAILABLE FOR THE LIFE OF THE PRODUCT AS DEFINED BY LOGICUBE.

EXCEPT AS OTHERWISE SPECIFICALLY PROVIDED IN THIS AGREEMENT, LOGICUBE PRODUCTS ARE PROVIDED AS-IS AND AS-AVAILABLE, AND LOGICUBE DISCLAIMS ANY AND ALL OTHER WARRANTIES (WHETHER EXPRESS, IMPLIED, OR STATUTORY) INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES

OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT OF THIRD PARTY RIGHTS.

SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, OR LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, SO THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION.

RoHS Certificate of Compliance

LOGICUBE PRODUCTS COMPLY WITH THE EUROPEAN UNION RESTRICTION OF THE USE OF CERTAIN HAZARDOUS SUBSTANCES IN ELECTRONIC EQUIPMENT, ROHS DIRECTIVE (2002/95/EC).

THE ROHS DIRECTIVE PROHIBITS THE SALE OF CERTAIN ELECTRONIC EQUIPMENT CONTAINING SOME HAZARDOUS SUBSTANCES SUCH AS MERCURY, LEAD, CADMIUM, HEXAVALENT CHROMIUM AND CERTAIN FLAME-RETARDANTS IN THE EUROPEAN UNION. THIS DIRECTIVE APPLIES TO ELECTRONIC PRODUCTS PLACED ON THE EU MARKET AFTER JULY 1, 2006.

Logicube Technical Support Contact Information

1. By website: www.logicube.com
2. By email: techsupport@logicube.com
3. By telephone: 1 - (818) 700 8488 ext. 3 between the hours of 7am – 5pm PST, Monday through Friday, excluding U.S. legal holidays.

Table of Contents

WRITEPROTECT™ BAY USER'S MANUAL.....	I
LIMITATION OF LIABILITY AND WARRANTY INFORMATION	I
LOGICUBE DISCLAIMER.....	I
WARRANTY	I
ROHS CERTIFICATE OF COMPLIANCE	III
LOGICUBE TECHNICAL SUPPORT CONTACT INFORMATION	III
TABLE OF CONTENTS	I
1: INTRODUCTION.....	1
1.0 INTRODUCTION TO THE WRITEPROTECT BAY.....	1
1.1 FEATURES	1
1.2 SPECIFICATIONS	2
1.3 IN THE BOX	2
1.4 ADDITIONAL OPTIONS.....	2
2: GETTING STARTED.....	4
2.0 OVERVIEW OF THE WRITEPROTECT BAY.....	4
2.1 ADDITIONAL FAN MOUNTING	5
2.1 CONNECTING THE WRITEPROTECT BAY TO A FORENSIC WORKSTATION.....	7
2.2 CONNECTING VARIOUS DRIVE TYPES	7
2.3 USING USB/FIREWIRE/eSATA ENCLOSURES OR EXTERNAL DRIVES	8
2.4 LEDs	9
3: QUICK START	10
3.0 QUICK START GUIDE.....	10
3.1 REGISTRY OPTIMIZATION.....	10
3.2 CONNECTED DRIVES	11
4: REMOTE CONNECTIVITY	12
4.0 REMOTE CONNECTIVITY INTRODUCTION	12
4.1 CONNECTING TO THE WEB INTERFACE.....	12
4.2 USAGE	12
5: USING THE WEB INTERFACE	13
5.0 WEB INTERFACE INTRODUCTION.....	13
5.1 USB DEVICE	13
5.1.1 Drives.....	14
5.1.2 HPA/DCO	15
5.1.3 Exports.....	16
5.2 FILE BROWSER.....	16

5.3	WRITE PROTECT STATISTICS.....	17
5.3.1	About.....	17
5.3.2	Adv. Drive Statistics.....	17
5.3.3	Network Interface Stats.....	18
5.3.4	Debug Logs.....	18
5.3.5	Help.....	18
5.4	SYSTEM SETTINGS.....	19
5.4.1	Profiles.....	19
5.4.2	Passwords.....	21
5.4.2.1	<i>Setting Key Passwords.....</i>	22
5.4.2.1.1	Config Lock Notes.....	22
5.4.2.1.2	Forgotten password for any keys.....	23
5.4.2.2	<i>User Account Passwords.....</i>	24
5.4.3	Language/Time Zone.....	25
5.4.3.1	<i>Language.....</i>	25
5.4.3.2	<i>Time Zone.....</i>	26
5.4.4	USB Device.....	27
5.4.5	HPA.....	28
5.5	NETWORK SETTINGS.....	28
5.5.1	Interfaces.....	29
5.5.1.1	<i>Configuring a Static IP address.....</i>	29
5.5.1.2	<i>Enabling/Disabling Network Services.....</i>	30
5.5.2	HTTP Proxy.....	31
5.5.2.1	<i>Server.....</i>	31
5.5.2.2	<i>Username/Password.....</i>	32
5.6	SOFTWARE UPDATES.....	32
5.7	POWER OFF.....	32
6:	UPDATING/LOADING/RE-LOADING SOFTWARE.....	33
6.0	UPDATING/LOADING/RE-LOADING SOFTWARE – INTRODUCTION.....	33
6.1	UPDATING/LOADING/RE-LOADING SOFTWARE INSTRUCTIONS.....	33
6.1.1	From Network (Over the Internet).....	33
6.1.2	From USB Drive (Through a software file download).....	34
6.2	FIRMWARE LOADING INSTRUCTIONS.....	35
7:	REMOTE OPERATION.....	36
7.0	REMOTE OPERATION - INTRODUCTION.....	36
7.1	WEB INTERFACE.....	36
7.2	COMMAND LINE INTERFACE (CLI).....	37
7.2.1	Connecting via Telnet.....	37
7.2.2	Connecting via SSH.....	37
7.3	ZERO CONFIGURATION NETWORKING (ZEROCONF).....	38
	TECHNICAL SUPPORT INFORMATION.....	38

1: Introduction

1.0 Introduction to the WriteProtect BAY

The WriteProtect™ BAY write-blocker provides secure, read-only, write-blocked access to SAS, SATA, USB 3.0, FireWire™, PATA/IDE, and PCIe and M.2 PCIe suspect hard drives. Extremely fast performance is powered by a SuperSpeed USB 3.0 host connection to easily manage large capacity hard drives. The WriteProtect BAY is the only portable write-blocker on the market that provides support for 6 different storage technologies in a 5.25" half height design that fits into the drive bay of your forensic workstation. Logicube, a pioneer in the digital forensic industry, delivers an easy to use, reliable and professional forensic write-blocking solution.



1.1 Features

- The standalone WriteProtect-BAY mounts into a standard 5.25" half-height forensic workstation drive bay for efficient imaging and preview tasks in the lab.
- SuperSpeed USB 3.0 host connection for extremely fast operation.
- Built-in, read-only, write-blocked support for SAS/SATA/USB 3.0/2.0/1.1/FW400/800 storage technologies, an adapter is included to support 2.5"/3.5" IDE drives.
- PCIe Support is available for M.2 PCIe (SATA, AHCI and NVME types), PCIe and mini-PCIe express cards using the WriteProtect's PCIe port and optional adapters.
- Multiple source drives can be connected to the WriteProtect and imaged, using your forensic imaging software, simultaneously to shorten processing time.
- Features 2 SAS/SATA drive ports, 1 USB 3.0 port, 1 FireWire port, 1 Gigabit Ethernet port, 1 PCIe port.
- Support for IDE, 1.8" IDE, 1.8" ZIF, mSATA, microSATA, eSATA and flash media is available using optional adapters.

- Use the browser-based user interface to manage all WriteProtect operations including software updates. Connect to your network using the WriteProtect's Gigabit Ethernet port.
- Preview drives connected to WriteProtect using the browser-based user interface.
- HPA/DCO detection and capture supported via the browser-based user interface.
- 5 LEDs for power, host, device, activity, HPA/DCO detection allow you to easily monitor all processes.
- Compatible with forensic acquisition and analysis software.

1.2 Specifications

Power Requirements	Power Supply Voltage(DC IN)	Output Voltage (DC OUT)	Net Weight	Dimensions	Agency Approvals
72 watts (including 2 hard disks plus 1 USB to SATA hard disk)	+12VDC +/- 5% from PC required	+5VDC@2.5A, +12VDC@2.5A	1.75 lbs .79kg	8.27" (L) X 5.73" (W) X 1.60" (H) 21.01cm X 14.55cm X 4.06cm	RoHs compliant

1.3 In the Box

The following items are included with WriteProtect BAY:

- 2 SAS/SATA power & data cables
- 1 FireWire cable
- 1 USB 3.0 Type A Male to Micro-B Male
- 1 Cat 6 network cable
- 1 2.5"/3.5" IDE to SATA adapter
- 1 Dual 4-pin Molex to 6-pin PCIe Y adapter

1.4 Additional Options

The following options are available for the WriteProtect BAY:

- eSATA cable
- mSATA adapter
- Flash media reader for compact flash, SD cards and other flash media
- 1.8" IDE to SATA adapter
- 1.8" IDE ZIF to SATA adapter
- 1.8" microSATA adapter
- PCIe Kit (for PCIe, mPCIe, and M.2 SSDs)

**WARNINGS:**

- Avoid dropping the Logicube WriteProtect BAY or subjecting it to sharp jolts. When in use, place it on a flat surface.
- Keep the unit dry. If the WriteProtect BAY needs to be cleaned, use a lightly damp, lint free cloth. Avoid using soap or other cleaning agents particularly those containing bleach, ammonia, alcohol or other harsh chemicals.
- Do not attempt to service or open the WriteProtect BAY. Doing so may void the warranty. If the unit requires service, please contact Logicube Technical Support for assistance.

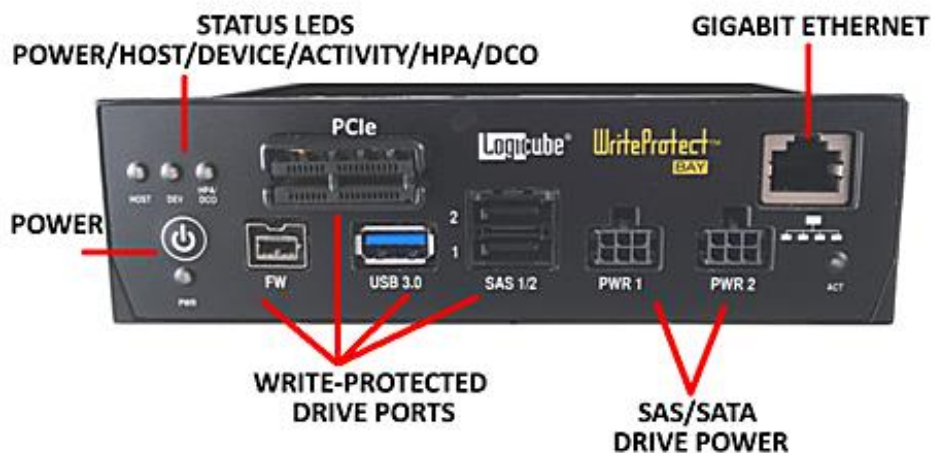
2: Getting Started

2.0 Overview of the WriteProtect BAY



Special Icons – Throughout this manual, there are two icons that can be seen. Please pay close attention when any of these two icons are found. These icons highlight additional information or important warnings on specific topics.

WriteProtect™ BAY MODEL



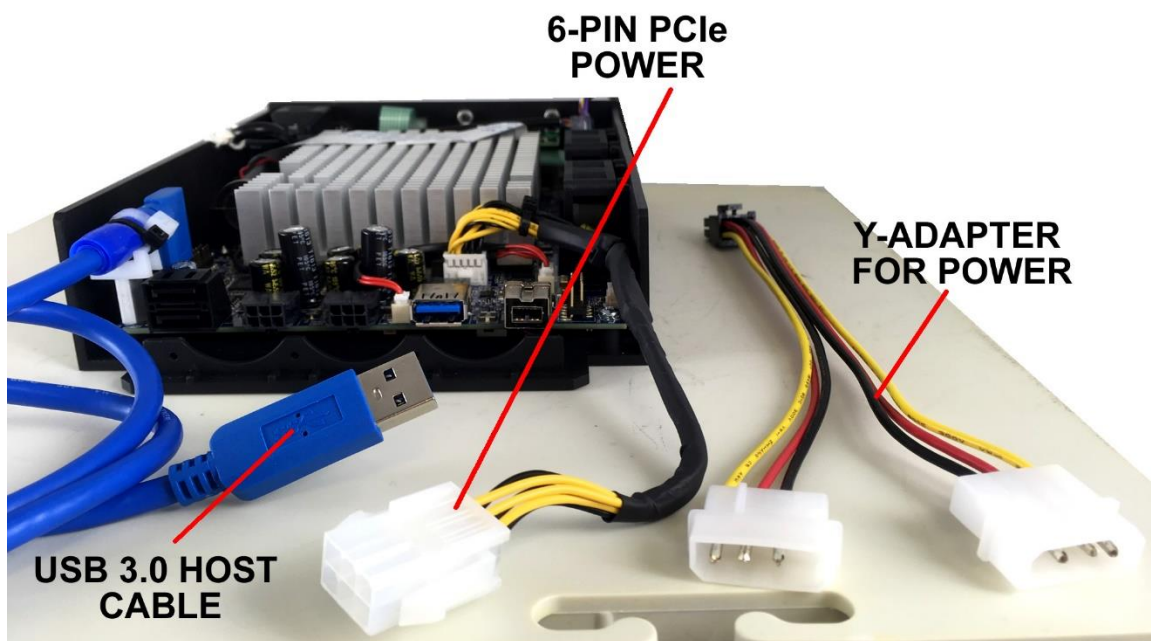
WriteProtect BAY - Left angled view



WriteProtect BAY – Right angled view



WriteProtect BAY – Back view



2.1 Additional Fan Mounting

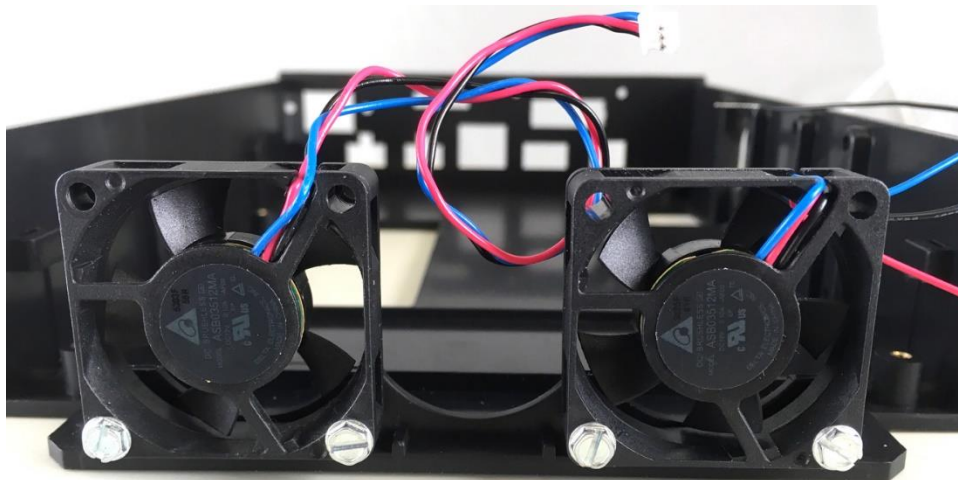
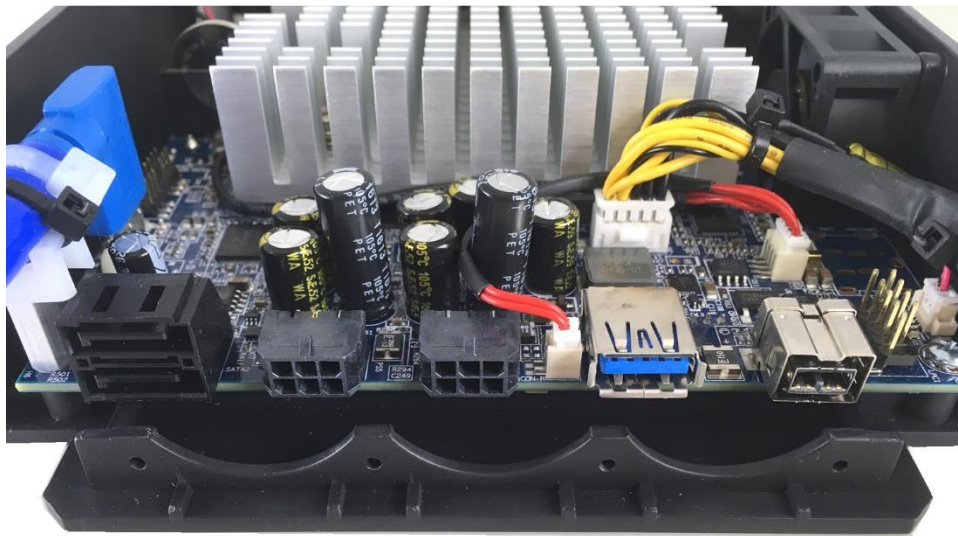
The WriteProtect BAY comes with a slot in the back for mounting additional fans, at the user's discretion, if more air flow is desired. One or two fans can be added.

Important Notes for additional fan mounting:

- Logicube does not supply or sell these fans.
- Use 35mm fans. The mounting holes are designed to fit 35mm fans.
- The depth of the fans available may vary. Make sure that the bay slot of the workstation/computer/server has enough space for the fans to be added.
- Additional fans must be powered using the power supply from the workstation/computer/server. Adapters may be necessary to connect the additional fans to the power supply for power.
- Fans must be mounted to direct air outward, away from the WriteProtect BAY.



Do not disconnect any wiring or cable from the WriteProtect BAY to power the additional fans. Doing so will void the device's warranty.



2.1 Connecting the WriteProtect BAY to a forensic workstation

To mount the WriteProtect BAY to a 5.25" bay on a forensic workstation, please reference the workstation's user's manual or the case manufacturer's manual.



It is recommended the workstation be powered off when mounting and connecting the WriteProtect BAY.

The WriteProtect BAY is powered by a 6-pin PCIe power connector. It comes with dual 4-pin Molex to 6-pin PCIe Y adapter for power supplies that do not have a 6-pin PCIe power output.

Attach a 6-pin PCIe power connector from the power supply or use the adapter to utilize two 4-pin Molex connectors. This will provide power to the WriteProtect BAY.

Connect the USB 3.0 host cable to an available USB port.

The WriteProtect BAY is now ready to be used and will turn on when the computer is turned on.



The PWR LED will blink for up to 30 seconds when turned on. The WriteProtect BAY will be ready to use when the PWR LED turns solid green.

There are three ways of turning the WriteProtect BAY off:

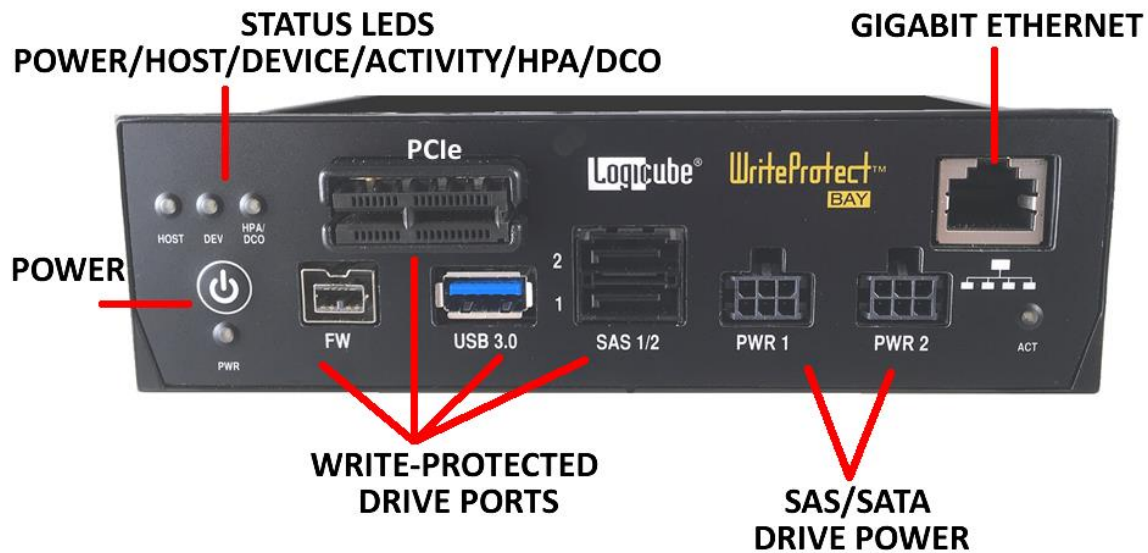
1. Shut down the forensic analysis computer. The WriteProtect BAY will turn off with the computer.
2. Press and immediately release the power button on the WriteProtect BAY. The Power LED will start blinking as the WriteProtect BAY begins to shut down. The Power LED and the fans will turn off within 30 seconds. When the Power LED turns off, the WriteProtect BAY has fully shut down.
3. Using the Graphical User Interface (GUI) via a browser through a remote connection, navigate to the **Power Off** screen and click the **Power Off** icon. The Power LED will start blinking as the WriteProtect BAY begins to shut down. The Power LED and the fans will turn off within 30 seconds. When the Power LED turns off, the WriteProtect BAY has fully shut down.

2.2 Connecting various drive types

Cables and adapters are available for the following drive types:

- SAS
- SATA
- USB
- FireWire
- 2.5" and 3.5" PATA/IDE
- eSATA cable (optional)
- mSATA adapter (optional)
- Flash media reader for compact flash, SD cards and other flash media (optional)

- 1.8" IDE to SATA adapter (optional)
- 1.8" IDE ZIF to SATA adapter (optional)
- 1.8" microSATA adapter (optional)
- M.2 (optional)
- PCIe (optional)



The SAS/SATA cable must be matched with the SAS and Power (PWR) ports. For example, SAS 1 goes with PWR 1 and SAS 2 goes with PWR 2.



Drives do not have to be connected in any order. For example, a single SATA drive does not have to be connected to the SAS/SATA S1 port. It can be connected to the SAS/SATA S2 port without having anything connected to the S1 port.

Any combination of drives can be connected at the same time, up to 5 drives connecting to all available ports.



The PCIe port is not hot-swappable. Always turn the WriteProtect BAY off when connecting or disconnecting drives through the PCIe port.

2.3 Using USB/FireWire/eSATA Enclosures or External Drives

When using drives that came from a USB, FireWire, or eSATA enclosure, or external drives, it is highly recommended to leave the drive inside the enclosure. USB enclosures typically have an on-board controller that may be necessary to read the drive properly. Taking the drive out of the enclosure could cause any device (including computers) not to read the drive contents properly.

2.4 LEDs

The WriteProtect BAY has five (5) LEDs:

HOST – Detects a link connection between the WriteProtect and the host computer

- **On** – Detects an active link between the WriteProtect and host computer
- **Off** – There is no active link between the WriteProtect and host computer

DEV – Device LED

- **On** – This LED is ON when a drive is connected (SATA, SAS, USB, FireWire, etc.)
- **Off** – This LED is OFF when there are no drives connected

HPA/DCO – HPA and/or DCO detection

- **On** – Detects the presence of an HPA and/or DCO on the connected drive
- **Off** – Does not detect the presence of an HPA and/or DCO on the connected drive

PWR – Power LED

- **On** – The WriteProtect is powered on
- **Blinking** – This LED will blink while the WriteProtect is being turned ON or OFF
- **Off** – The WriteProtect is turned off

ACT – Activity LED

- **Blinking** – Detects activity on the connected drive
- **Off** – No activity on the connected drive

3.0 Quick Start Guide

This chapter gives a basic overview and steps on how to set up the WriteProtect.

Two steps must be performed to use the WriteProtect:

- Turn the WriteProtect on
- Connect at least one drive to the WriteProtect



PCIe is not hot-swappable. Always turn the WriteProtect BAY off when connecting or disconnecting drives through the PCIe port.

Optional: Connect the WriteProtect to a network using a Cat5e or Cat6 network cable for remote connectivity to be able to use the built-in file browsing capabilities, configure, or update the software of the WriteProtect.

3.1 Registry Optimization

Logicube recommends a registry entry to optimize the USB 3.0 transfer speeds for windows 7 and Windows 8/8.1. No registry optimization is needed for Windows 10.

The registry entries can be downloaded from:

http://updates.logicube.com/WriteProtectOptimization/WriteProtect_Optimization.zip

Extract the contents of the ZIP file to a folder on your computer. You should see two files:

- Logicube_WriteProtect_Optimization_Win7.reg
- Logicube_WriteProtect_Optimization_Win8.reg



Microsoft recommends backing up the registry and any important/valued data before making any changes to the registry. Please search Microsoft's support site for instructions on how to back up the Windows registry.

To import the optimization registry entry:

1. Make sure you are logged in to a Windows 7 or 8/8.1 computer on an account with administrator rights.
2. Double-click the appropriate registry file (Logicube_WriteProtect_Optimization_Win7.reg for Windows 7 computers and Logicube_WriteProtect_Optimization_Win8.reg for Windows 8/8.1 computers).
3. Windows should prompt you asking if you are sure you want to allow the program (the registry file) to make changes to your computer. Select Yes. You may also be prompted with a warning

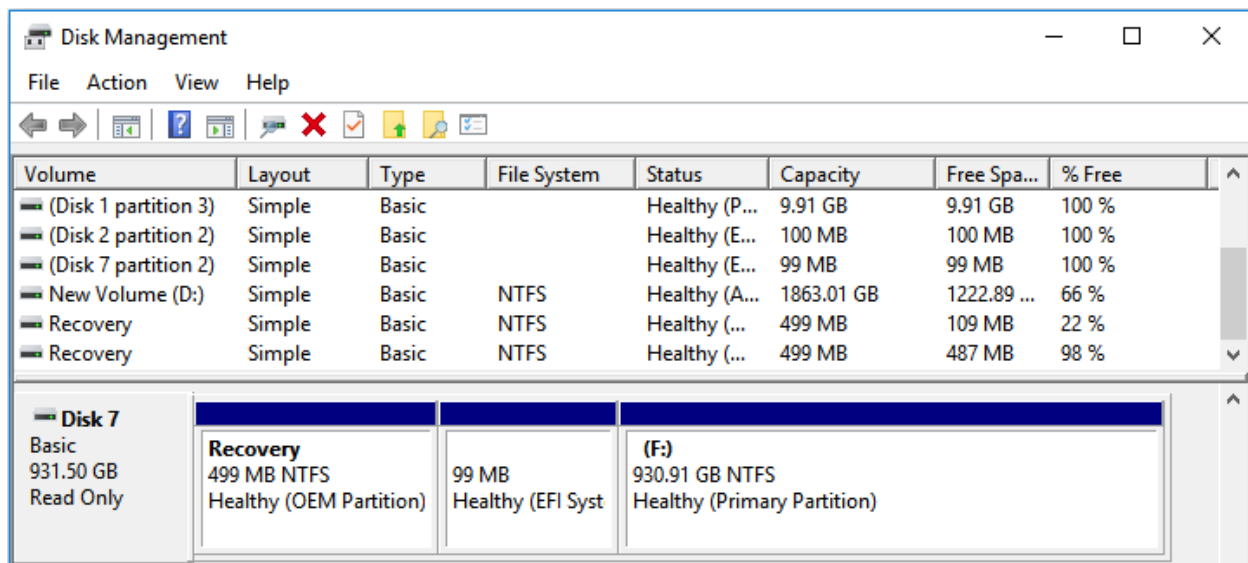
about adding information to the registry may cause components to stop working correctly. Please select Yes to continue adding the registry entry.

- When the registry entry has been imported, you should see a confirmation window stating it has been successfully added to the registry. Once successfully added, we recommend restarting the computer.

3.2 Connected Drives

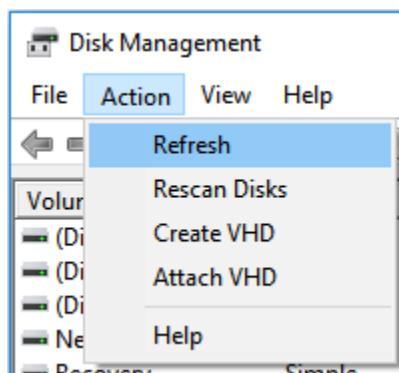
Depending on the Operating System on the computer, drives connected to the WriteProtect may or may not be automatically mounted. Windows should automatically assign a drive letter to partitions that it can recognize.

Disk Management will show the drives as "Read Only":



If at least one drive is already connected and a second, third, or fourth drive is added, Windows may not automatically detect the added drives. It is recommended to go to **Disk Management**, click **Action**, then click **Refresh**.

When drives are disconnected, refreshing **Disk Management** may also be required to refresh the list of connected drives.



FireWire drives may not be seen by the computer when the FireWire drive is already connected to the WriteProtect before the WriteProtect is turned on. If FireWire drives are not detected, disconnect the FireWire drive from the WriteProtect, wait a few seconds, then re-connect the FireWire drive.



HPA/DCO can be managed and configured through the web browser interface. Third party tools can also be used to manage HPA/DCO.

4: Remote Connectivity

4.0 Remote Connectivity Introduction

The WriteProtect comes with a gigabit network connection. Connecting the WriteProtect to a network allows remote access from any computer within the same network using a supported Internet browser (Chrome or Firefox). A network connection with Internet access also allows the WriteProtect software to be updated using the **FROM NETWORK** option.

The WriteProtect is configured for DHCP by default.

4.1 Connecting to the Web Interface

Using a supported web browser, go to the WriteProtect's hostname. The hostname will be: <http://wp-XXXXXX> where XXXXXX is the 6-digit serial number of the WriteProtect. The serial number can be found on a sticker underneath the WriteProtect. The WriteProtect's web interface will appear on the browser screen.

Google Chrome and Mozilla Firefox are the recommended browsers. Other browsers may not display the Graphical User Interface correctly.



On some browsers or Operating Systems, the WriteProtect will need to be accessed by browsing to <http://wp-XXXXXX.local/>.

4.2 Usage

The web interface can be used for built-in file browsing capabilities, configuration, or software updates for the WriteProtect. The built-in file browser can recognize many different file systems and can be a useful tool when the computer being used cannot see the connected drive's file system or contents. See [Section 5.0 Web Interface Introduction](#) for details on the web interface.

5: Using the Web Interface

5.0 Web Interface Introduction

The Web Interface allows the user the following capabilities:

- Advanced configuration and settings
- File Browsing
- Software and firmware updates

The following sections give a brief explanation of each screen on the web interface.



5.1 USB Device



This screen has three tabs: **Drives**, **HPA/DCO**, and **Exports**.




5.1.1 Drives

DRIVES			
PORT	INFORMATION	STATUS	MORE INFO
SAS1	WDC_WD10EZEX-08M2NA0 1.0 TB	ENGAGED	
SAS2	WDC_WD400JD-19MSA1 40.0 GB	ENGAGED	

This screen allows the user to see basic information about drives connected to the device.

The **More Info** icon shows additional information about the drive.

If a drive has an HPA or DCO detected, the following icon will be displayed: 

Clicking the icon will show additional details of about the drive.

DRIVE DETAILS

Mounted:

true

HPAEnabled:

Yes

DCOEnabled:

No

ATASecurityEnabled:

No

ATASecurityLocked:

No

ATASecureErase:

Supported

ATAEnhancedSecureErase:

Not Supported

HPASizeSectors:

10000 (Removed)

DCOSizeSectors:

0

IsPortEnabled:

true

OK

5.1.2 HPA/DCO

DRIVES

HPA/DCO

EXPORTS

PORT	INFORMATION	HPA SIZE	DCO SIZE
SAS1	WDC_WD10EZEX-08M2NA0 1.0 TB	0	0
SAS2	WDC_WD400JD-19MSA1 40.0 GB	10000 (REMOVED)	0

CLEAR HPA/DCO

SET HPA/DCO

This screen shows the HPA (Host Protected Area) size and DCO (Device Configuration Overlay) size.



The HPA or DCO on a drive can be cleared. The behavior depends on what the drive has (HPA, DCO, or both):

HPA only – Clearing the HPA from a drive is a volatile (temporary) change. The next time the drive's power is disconnected then re-connected (the next time the drive powers on), the HPA will stay in-tact.

DCO only – Clearing the DCO from a drive will remove the DCO and preserve any data within the DCO. Clearing the DCO is a permanent change to the drive and will restore the drive capacity to the factory default.

HPA and DCO – Clearing both HPA and DCO from a drive is a permanent change to both HPA and DCO. For the DCO to be cleared, the HPA must be permanently removed first.

You can also set an HPA or DCO on a drive by clicking the **SET HPA/DCO** icon. A window will appear and the HPA and/or DCO size can be set.

HPA SIZE DCO SIZE

0 1 2 3 4 5

6 7 8 9 ←

OK



The connected drive must support HPA or DCO for this function to work. HPA or DCO drive support questions, please contact the drive manufacturer.



This is a persistent change and will alter the drive's total visible capacity/size.

PCIe NVMe SSDs do not support HPA or DCO.

PCIe AHCI drives support HPA but not DCO. Since PCIe is not hot-swappable, the WriteProtect needs to be restarted using either the RESTART icon in the POWER OFF menu in the GUI or by using the Power button in front of or on the top of the WriteProtect once the HPA is set.

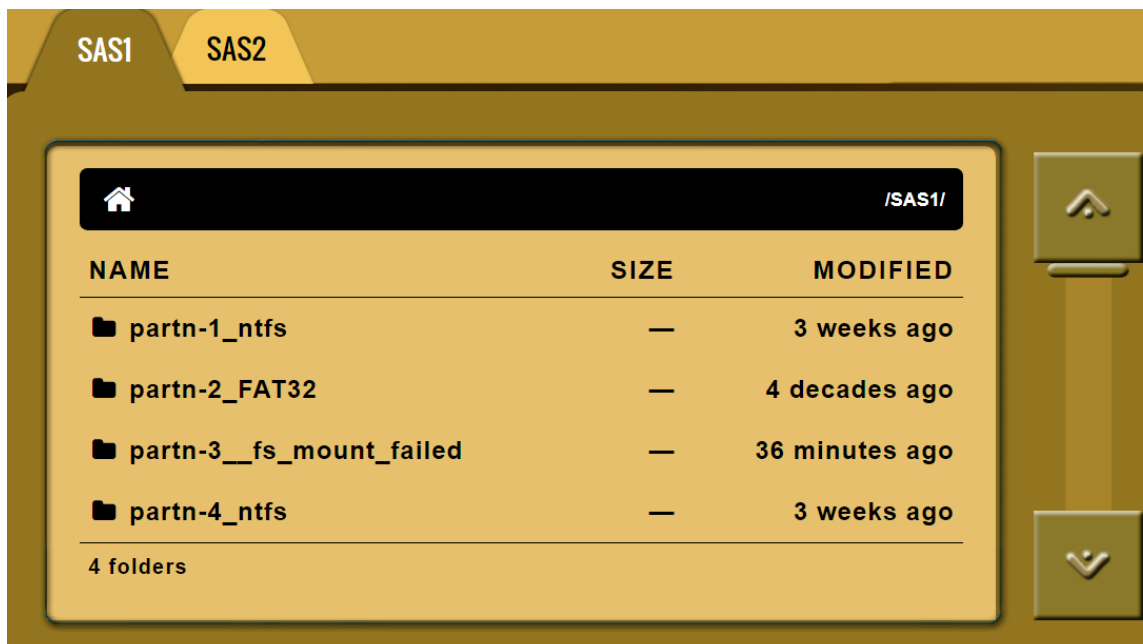
5.1.3 Exports

This screen has a **Re-Engage USB** button which resets the USB connection without having to physically disconnect and re-connect the USB cable between the WriteProtect and the computer.

5.2 File Browser



The contents of all connected drives can be previewed using the WriteProtect's file browser. The file browser will show the partitions and the contents of each partition. Files opened by the file browser will not alter the drive in any way. The file browser can be useful for file systems that cannot be recognized by the computer's Operating System.



If a file cannot be previewed, the following message will appear:

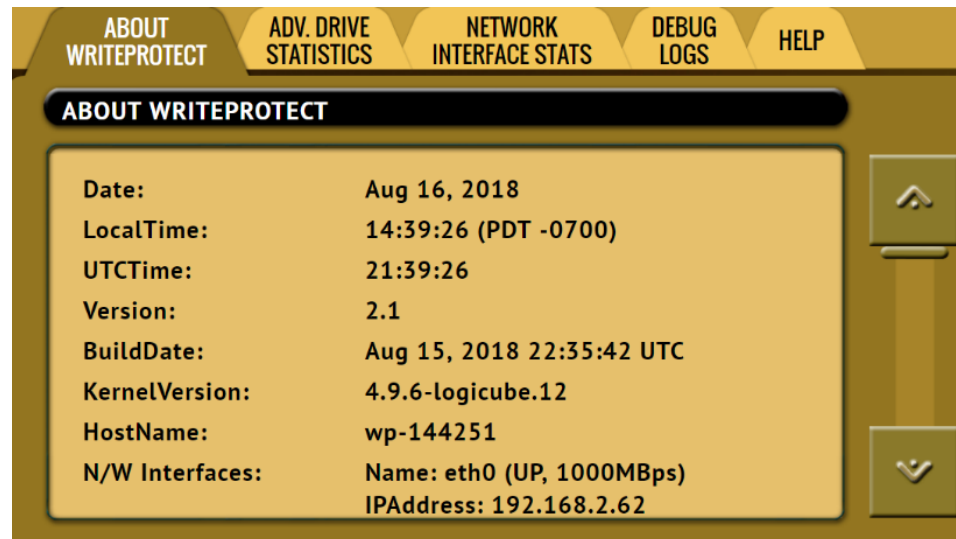
File viewer cannot view file type:

5.3 Write Protect Statistics



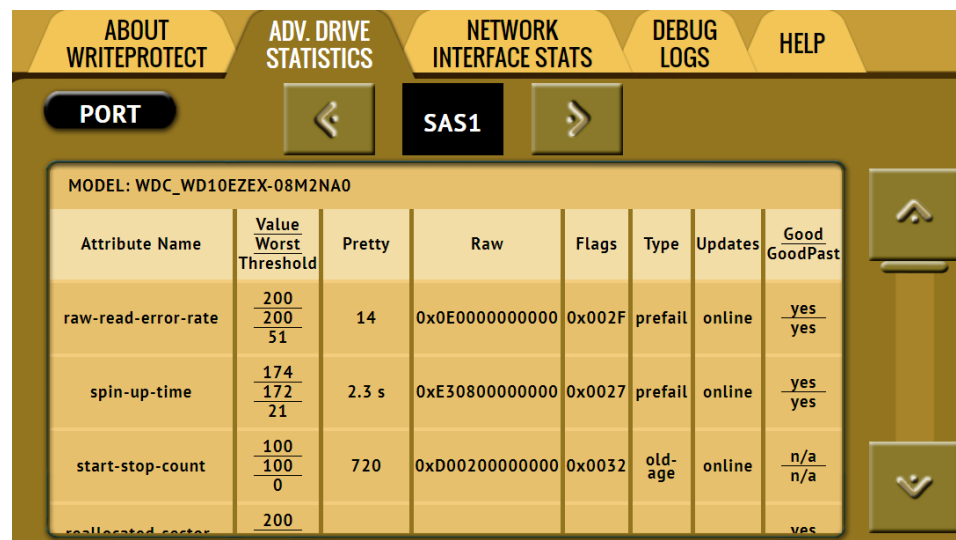
This will display the following tabs: **About**, **Adv. Drive Statistics**, and **Network Interface Stats**, **Debug Logs**, and **Help**.

5.3.1 About



The **About** screen will show information about the WriteProtect.

5.3.2 Adv. Drive Statistics



The **Adv. Drive Statistics** tab displays S.M.A.R.T. information for connect drives that support S.M.A.R.T.

5.3.3 Network Interface Stats

ABOUT
WRITEPROTECT

ADV. DRIVE
STATISTICS

NETWORK
INTERFACE STATS

DEBUG
LOGS

HELP

NETWORK INTERFACE STATS

Interface	Rx Bytes	Rx Packets	Rx Dropped	Rx Errors	Tx Bytes	Tx Packets	Tx Dropped	Tx Errors	Status
eth0	6827766	36768	1	0	18306162	21884	0	0	UP

Displays the Network Interface statistics (Receive and Transfer bytes, packets, drops, and errors, and the link status).

5.3.4 Debug Logs

There may be times when Logicube Technical Support will ask for debug logs. This tab allows the user to export the debug logs to a USB flash drive (connected to front USB port).

To export the debug logs:

1. Connect a formatted USB flash drive to the one the front USB ports.



The USB flash drive must be formatted in Windows using the NTFS, FAT32, or FAT file system.

2. From the Debug Logs screen, click **Export**.
3. The Debug Logs will be exported to the USB flash drive and can be emailed to Technical Support.

5.3.5 Help

The help tab contains a QR code that links to the user's manual online. There are several ways to view the manual through the QR code such as:

- From the touch screen (if the unit is connected to a network with Internet access), simply click the QR code.
- Through a web browser, click the QR code.
- Scan the QR code from a mobile phone or tablet that has internet access.

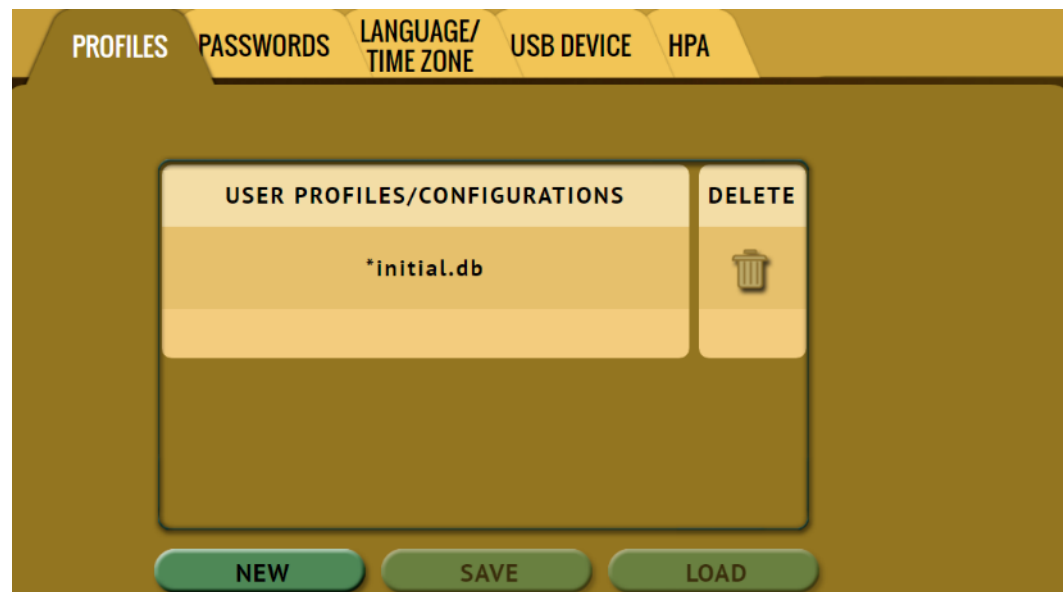
5.4 System Settings



The **System Settings** screen allows users to configure the following for the WriteProtect:

- Profiles
- Passwords
- Language/Time Zone
- USB Device
- HPA

5.4.1 Profiles



This screen shows all user profiles for the WriteProtect. There are three options in this screen:

- **New** – Allows the user to create a new profile name.
- **Save** – Saves the selected profile.
- **Load** – Loads the selected profile.

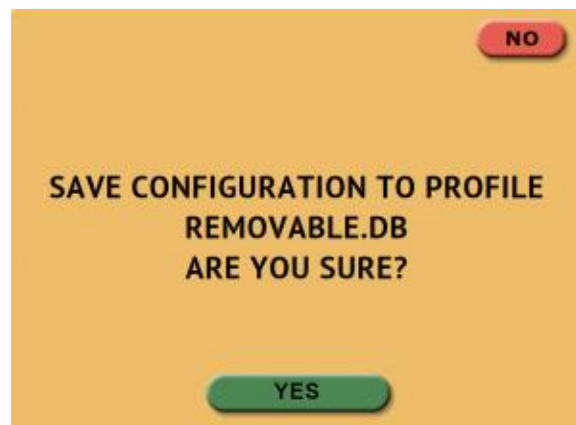


The WriteProtect will boot with the profile that has an asterisk (*) next to the name.

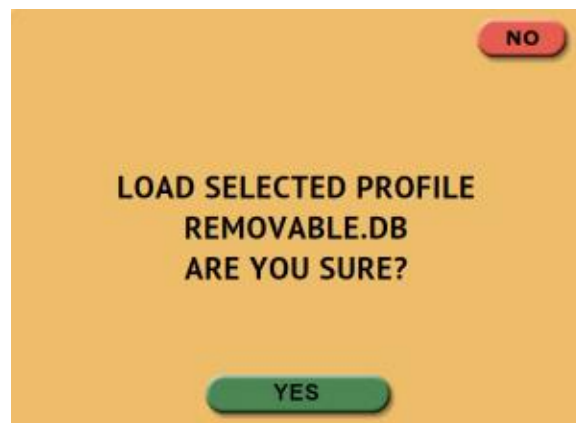
Profiles allow users to create different profiles. The profile can then be saved. When a profile is loaded using the **Load** icon, that profile will be used during its boot process.

For example, if the user wants to change the Export Type from Fixed Drive to Removable and have that setting be used every time the WriteProtect is turned on, the setting must be changed then a profile needs to be added, saved, and loaded:


1. Turn the WriteProtect off then back on. This will reset all settings to its default configuration. This is an important step to help ensure only the changes desired will be the changes saved.
2. Go to the **System Settings** tab and in the USB Device tab, set the **Export Type** to 'Removable'.
3. Go to **Profiles** tab and click the **New** icon.
4. Type a name for this profile. For example, **removable** and click the **OK** icon. The profile name should appear on the screen.
5. Click the newly saved profile and click **Save**. A confirmation screen will appear:



6. Click the **Yes** icon to save the profile.
7. Make sure the profile to be loaded (during the boot process) is highlighted (in this case, REMOVABLE.DB) and click the **Load** icon. A confirmation screen will appear:



8. The next time the WriteProtect is turned on it will load the REMOVABLE.DB profile.

To delete a profile, click the  (delete) icon. A confirmation screen will appear. Click the **Yes** icon to delete the selected profile.

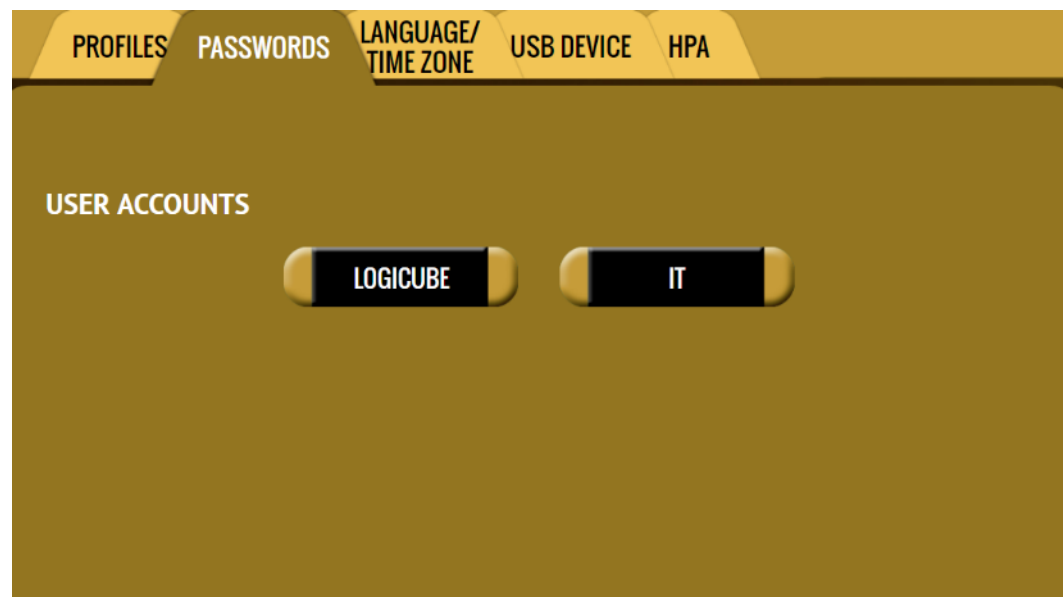


It is highly recommended that the WriteProtect is turned off then back on before making any changes to the profiles/configurations. This helps ensure that only the desired changes are saved.



Do not highlight and save over the INITIAL.DB configuration. This is the default configuration of the WriteProtect and is used to reset the device to the factory default settings.

5.4.2 Passwords



There are four passwords that can be set on the WriteProtect:

- **Key: Remote HTTP** – A password can be set to lock remote HTTP access (through a web browser). If this password is set, the WriteProtect will prompt for a password before allowing access through a web browser.
- **Key: Config Lock** – The WriteProtect can be configured to lock out any configuration changes. When this is enabled, changes to the different types of operations cannot be made without entering the correct key or password. Different types of operations can still be started.

For example, when the WriteProtect is locked, and it is configured for a 'Write Suppress' Export Mode, the user will be unable to change this mode to 'Read Only' without entering the correct key or password.

- **User Account: LOGICUBE** – Allows the user to change the **logicube** local account.
- **User Account: IT** – Allows the user to change the **it** local account.

5.4.2.1 Setting Key Passwords

To set a key for **Remote HTTP or Config Lock**, click one of the buttons. The following screen will appear.

Click the **Enable** icon to enter a password or key. The available characters are 0 through 9 and A through F.

Click the **Auto Lock** icon to set the time to automatically lock the configuration and require a password. By default, this is set to 1 minute.



The keys for **Remote HTTP** and **Config Lock** can be saved into a user profile and loaded each time the WriteProtect is turned on. See [Section 5.4.1](#) for more information on saving and loading a user profile.



Remember the Config Lock Key! If the WriteProtect is configured to load a user profile with the Config Lock set (enabled) and the password is forgotten, the only way to reset the Config Lock is load the INITIAL.DB profile using the Command Line Interface. See [Section 5.4.2.1.2](#) for more information.

If the INITIAL.DB has a Config Lock Key configured, and the password was forgotten, contact Tech Support assistance.

5.4.2.1.1 Config Lock Notes

A shortcut (and indicator) to the **config lock** can always be seen on the WriteProtect's screen. It is located on the top-right of the screen, next to the WriteProtect logo.

While in a locked state, the following operations will be affected as follows:

- **USB Device** – All functions in the USB Device screens are not affected by the Config Lock.
- **File Browser** – The file browser cannot be accessed without the Config Lock unlock key.

- **Statistics** – Since there are no settings or configurations for this operation, it is not affected by the Config Lock.
- **System Settings** – This entire section cannot be accessed without the Config Lock unlock key.
- **Network Settings** – This entire section cannot be accessed without the Config Lock unlock key.
- **Software Updates** – This entire section cannot be accessed without the Config Lock unlock key.
- **Power Off** – This entire section cannot be accessed without the Config Lock unlock key.



The WriteProtect can still be turned off without the unlock key by using the power button.

5.4.2.1.2 Forgotten password for any keys

If any of the keys is forgotten, the INITIAL.DB profile will need to be loaded using the Command Line Interface (CLI). See [Section 7.2](#) for more information on how to connect to the WriteProtect using the CLI.



This method will only work if the INITIAL.DB profile does not have a Config Lock Key saved. If the INITIAL.DB has a Config Lock Key configured, and the password was forgotten, contact Tech Support assistance.

Once connected to the Command Line Interface (CLI):

1. Login with the username "**it**" (without the quotes) and the password "**it**" (without the quotes).
2. From the main prompt, type **command**, then press the enter key.
3. Type **config** then press the enter key.
4. Type **db list** then press the enter key. This will show a list of profiles (or databases) saved. The WriteProtect has one default profile called **initial.db**. Any profiles added by users will appear in this list. The example below shows two databases (the default initial.db and lock.db). The db that shows an asterisk (*) before the name is the current database or configuration

being loaded each time the WriteProtect is turned on.

```
it@wp-144251(command-config)> db list
Number of DB's: 1
0: *initial.db

it@wp-144251(command-config)> █
```

5. Type **db load initial.db** then press the Enter key to load the default database. There should be a response showing "Command (DbManagement) Successful".
6. Type **db list** again and there should be an asterisk (*) on initial.db.
7. Turn the WriteProtect off using the power button, then close the Telnet/SSH application.
8. Turn the unit on. When the WriteProtect boots up, it will load the default profile (INITIAL.DB).

5.10.2.2 User Account Passwords

The WriteProtect comes with two built-in user accounts:

- **logicube**
- **it**

Both user account passwords can be changed in this screen. To change the password for either account, click either the **LOGICUBE** or **IT** button. A screen will appear:

The screenshot shows a web interface for changing passwords. It features a dark blue header bar with a close button (X) on the right. Below the header, there are three input fields labeled 'CURRENT PASSWORD', 'NEW PASSWORD', and 'CONFIRM PASSWORD'. Below these fields is a virtual keyboard with letters, numbers, and special characters. At the bottom of the screen is an 'OK' button.

1. Enter the current password.



The default password for each account is:

LOGICUBE: logicube

IT: it

2. Enter a new password.
3. Enter the new password again in the 'confirm password' box.
4. Click the **OK** icon when finished.

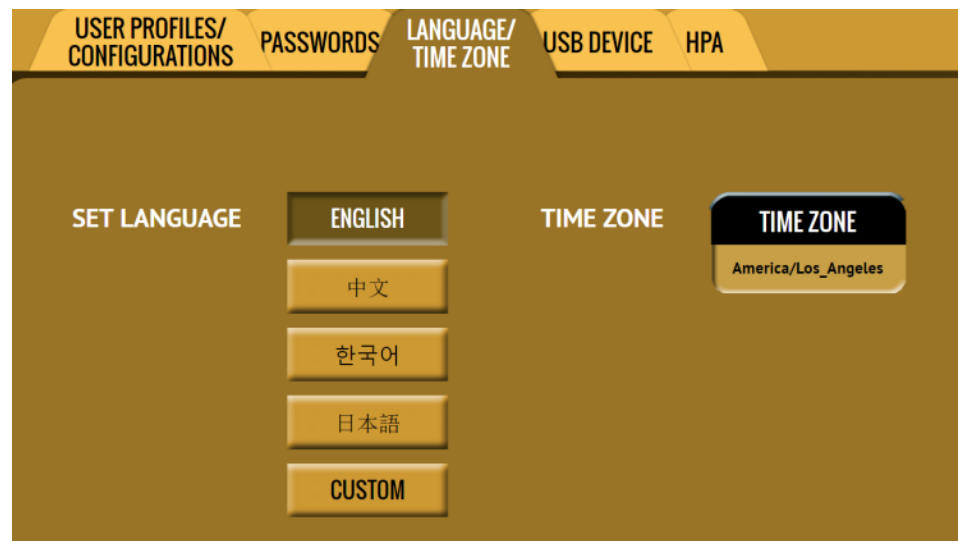


The **User Account Passwords** do not need to be saved into a user profile. Changing any of these two passwords will take effect immediately.

If the new User Account password is forgotten, contact Tech Support assistance.

5.4.3 Language/Time Zone

The WriteProtect menu's language can be changed along with the time zone setting.



5.4.3.1 Language

Four languages are available. Select English, Chinese (中文), Korean (한국어), or Japanese (日本語) to change the language displayed. As soon as the selection is made, the computer's Internet browser will automatically refresh and display the selected language.



The **Custom** button is reserved for future language releases.

5.4.3.2 Time Zone

The WriteProtect utilizes NTP (Network Time Protocol). Each time the unit is connected to a network with internet access, it will automatically check for the correct time using NTP and adjust the time as needed.

The WriteProtect also has a time zone setting. Click **Time Zone** to select the time zone region. Click the **OK** icon to continue.



After selecting the region, select the time zone and click the **OK** icon to set the time zone.



5.4.4 USB Device

The screenshot shows the 'USB DEVICE' configuration page in the Logicube WriteProtect BAY web interface. The page has a yellow header with five tabs: 'USER PROFILES/ CONFIGURATIONS', 'PASSWORDS', 'LANGUAGE/ TIME ZONE', 'USB DEVICE' (which is selected and highlighted), and 'HPA'. Below the tabs is a large light yellow box containing three configuration sections. The first section, 'EXPORT MODE', has two buttons: 'WRITE SUPPRESS' and 'READ ONLY'. The second section, 'EXPORT TYPE', has three buttons: 'FIXED DRIVE', 'REMOVABLE', and 'AUTO'. The third section, 'DCO PASSTHROUGH', has two buttons: 'ENABLED' and 'DISABLED'.

This section allows advanced configuration for the WriteProtect.

EXPORT MODE – This changes the behavior on how the computer's Operating System will interact with the connected drive.

- **WRITE SUPPRESS** – Will make it so that it looks like changes can be made, but no changes will occur. On rare occasions, this setting may need to be used for drives that are not properly detected (for example, Windows may show a notice that the connected drive needs to be formatted).
- **READ ONLY (Default)** – Sets the drive in a Read-Only state. Attempts to alter the contents of the drive will result in error messages or notices that the drive is Read-Only.

EXPORT TYPE – This setting changes the behavior on how the computer's Operating System will see the connected drive.

- **FIXED DRIVE** – Will make it so that the connected computer's Operating System sees the connected drive as a fixed drive (non-removable).
- **REMOVABLE** – The connected computer's Operating System will see the connected drive as a removable disk.
- **AUTO (Default)** – The WriteProtect will automatically choose based on the type of drive connected.

DCO PASSTHROUGH – Changes to DCO is persistent and may be permanent. Always proceed with caution when changing the DCO. By default, this is set to DISABLED, disallowing changes to the DCO. If changes need to be performed to the DCO, set this to ENABLED.

5.4.5 HPA

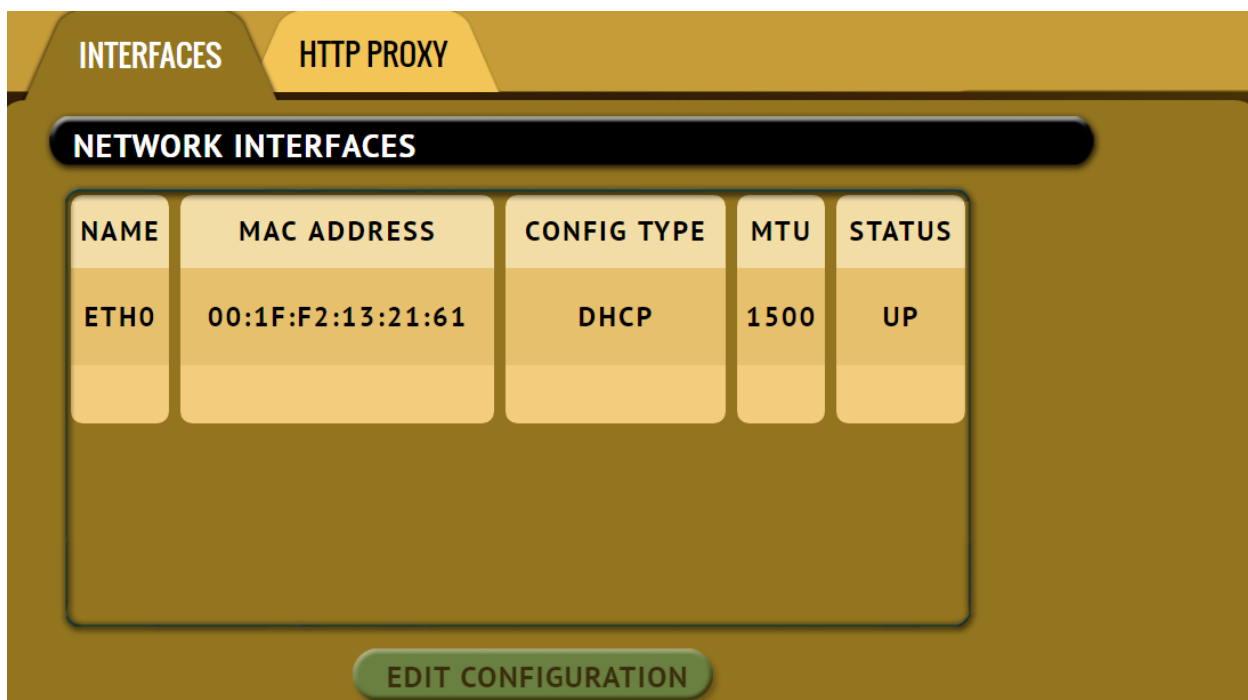
This screen allows the auto-removal of HPA to be enabled or disabled.



5.5 Network Settings



The Network settings screen has two tabs: **Interfaces** and **HTTP Proxy**. The **Interfaces** tab allows the configuration of the network interface which include setting a static IP (DHCP is set by default) and allows certain services to be enabled or disabled. There is also an **HTTP Proxy** tab where proxy server information can be entered.



5.5.1 Interfaces

The Interfaces tab displays the network interface information: MAC Address, Configuration type (DHCP or Static), MTU, and the status. This tab also allows enabling or disabling certain services. To edit the network interface configuration, click the Ethernet adapter name then click the **Edit Configuration** button. The configuration screen should appear:

EDIT NETWORK INTERFACE CONFIGURATION ETH0 [X]

TYPE	IP SETTINGS
DHCP	IP/NetMask: 192.168.2.12/22, Gateway: assigned by dhcp, DNS Server: assigned by dhcp

MTU	NETWORK SERVICES SETTING
1500	Enabled: SSH, Telnet, HTTP, CIFS/NetBIOS, iSCSI, iperf, ping Disabled:

[OK]

5.5.1.1 Configuring a Static IP address

The WriteProtect is DHCP enabled by default. Some networks do not support DHCP and require a static IP address. The WriteProtect can be configured with a static IP.

1. From the **Network Interface Configuration** screen (above), click the **Type** box and select **STATIC** then click the **OK** icon. The **IP SETTINGS** box should now be selectable.

EDIT NETWORK INTERFACE CONFIGURATION ETH0 [X]

TYPE	IP SETTINGS
Static	IP/NetMask: 192.168.2.128/22, Gateway: assigned by dhcp, DNS Server: assigned by dhcp

MTU	NETWORK SERVICES SETTING
1500	Enabled: SSH, Telnet, HTTP, CIFS/NetBIOS, iSCSI, iperf, ping Disabled:

[OK]

- Click the **IP SETTINGS** box to manually set the IP address, NetMask, Gateway, and DNS Server. When finished, click the **OK** icon.



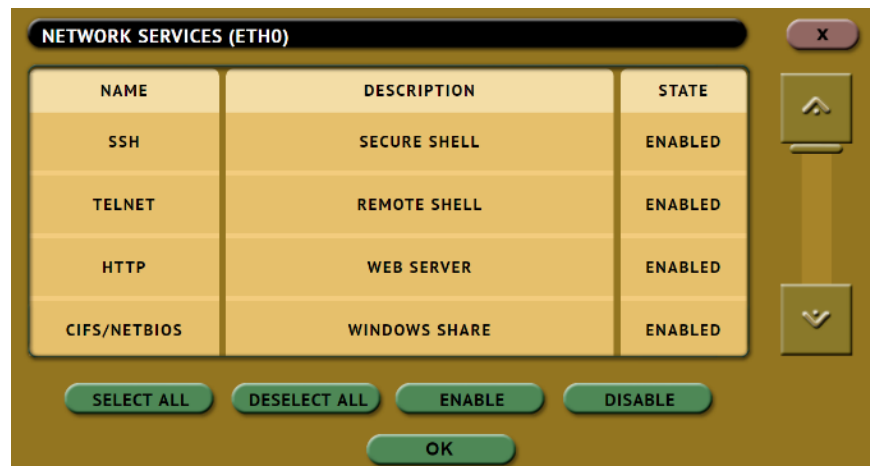
The IP SETTINGS dialog box has a title bar with "IP SETTINGS" and a close button (X). It contains three rows of input fields: "IP/NetMask" with the value "192 . 168 . 2 . 128 / 22", "Gateway" with four empty boxes, and "DNS Server" with four empty boxes. Below these is a numeric keypad with buttons for digits 0-9 and a back arrow. At the bottom is an "OK" button.



To save the settings so that the WriteProtect boots up with the static IP address, see [Section 5.4.1](#) for more information on saving and loading a user profile.

5.5.1.2 Enabling/Disabling Network Services

Network Services are enabled by default. To enable or disable specific network services, go to the **Network Interfaces Configuration Screen** and click **Network Services Setting**. The **Network Services** screen will appear:



The NETWORK SERVICES (ETH0) screen has a title bar with "NETWORK SERVICES (ETH0)" and a close button (X). It features a table with three columns: NAME, DESCRIPTION, and STATE. The table lists four services: SSH, TELNET, HTTP, and CIFS/NETBIOS, all of which are currently "ENABLED". To the right of the table are up and down arrow buttons. At the bottom are four buttons: "SELECT ALL", "DESELECT ALL", "ENABLE", and "DISABLE", followed by an "OK" button.

NAME	DESCRIPTION	STATE
SSH	SECURE SHELL	ENABLED
TELNET	REMOTE SHELL	ENABLED
HTTP	WEB SERVER	ENABLED
CIFS/NETBIOS	WINDOWS SHARE	ENABLED

Click each network service to be enabled or disabled then click the **Enable** or **Disable** icon.

There are 7 services that can be disabled (enabled by default):

- **SSH** – Disabling this will block Secure Shell (SSH) traffic.
- **Telnet** – Disabling this will block Telnet traffic.

- **HTTP** – Disabling this will block web browser connections to the WriteProtect.
- **CIFS/NETBIOS** – Disabling this will block any CIFS or NETBIOS connection to the WriteProtect (for example, Windows Explorer).
- **iSCSI** – Disabling this will block any iSCSI (Internet SCSI) traffic.
- **Iperf** – Disabling this will block Iperf traffic (a network tool to measure bandwidth performance).
- **Ping** – Disabling this will block ping access to the WriteProtect.

Disabling any of the services above will disallow the types of communication controlled by those services. For example, if HTTP is disabled, users will not be able to see the WriteProtect through a web browser over the network. If HTTP was disabled by accident, please contact Logicube support.



Please contact your Network or Systems Administrator before changing any of these services.

5.5.2 HTTP Proxy

If the network the WriteProtect is connected to uses an HTTP proxy server to access the Internet, proxy settings may need to be set for the WriteProtect to be able to update software from a network (over the internet). This typically includes a server (or IP address), a host port, a username and password.

The screenshot shows the 'HTTP PROXY' configuration page. At the top, there are two tabs: 'INTERFACES' and 'HTTP PROXY'. The 'HTTP PROXY' tab is selected. Below the tabs, there are two main configuration areas. The first area is labeled 'SERVER' and is currently empty. The second area is labeled 'USERNAME/PASSWORD' and contains the text 'Username:' and 'Password:'.

5.5.2.1 Server

Click the Server icon to set the IP address (or server name) and port of the proxy server.

5.5.2.2 Username/Password

If the proxy server requires a username and password for authentication, click the **Username/Password** icon to set this information.

5.6 Software Updates



New and improved software will be released from time to time. There are two ways to update the software on the WriteProtect: From the web via a network connection or from a USB drive.

See [Section 6.0 Updating/Loading/Re-loading Software](#) for step-by-step information on how to update the software and firmware.

5.7 Power Off



This screen allows the user to remotely turn off or reboot the WriteProtect.

6: Updating/Loading/Re-loading Software

6.0 Updating/Loading/Re-loading Software – Introduction

New and improved software will be released from time to time and will always be available on the WriteProtect support page. Browse to <http://www.logicube.com>. Point your mouse to Tech Support and select Product Knowledge Base or go directly to <https://www.logicube.com/knowledge/writeprotect>.

6.1 Updating/Loading/Re-loading Software Instructions

There are two methods of how to update the WriteProtect software:

- A. **FROM NETWORK** – Over the Internet through a network connection
- B. **FROM USB DRIVE** – Through a software file download onto a USB drive flash.



The actual software installation will take about 5 minutes. If **FROM NETWORK** was chosen, the total time can exceed 10 to 20 minutes (or longer) depending on Internet speeds and Internet traffic.



The most up-to-date instructions on updating the software can be found on the WriteProtect's support page.

6.1.1 From Network (Over the Internet)

The software can be updated/re-installed by connecting the unit to a network with internet access.

1. Connect the unit to a network with internet access and turn the unit on.
2. Using the Remote Connectivity feature (see [Section 4.0](#) for details on Remote Connectivity), connect to the WriteProtect.
3. From the main menu, locate and click the **Software Updates** icon on the left side.
4. Select **From Network**. The unit will check for software on Logicube's server. After a few seconds, one of the following messages will appear:
 - **Newer version available** – This message will appear if there is a newer software version found. Click the **OK** icon to continue.
 - **Up to date** – This message will appear if the software version found is the same as the version currently installed. Click the **OK** icon to continue.
 - **No new version found** – This message will appear if the unit does not have any internet access. Click the **OK** icon to continue. If this message is seen, make sure the unit is connected to a network with internet access and try step 3 again or try updating the software from a USB drive.

5. Click the **Update** icon to begin the update. The unit should begin the update process. Do not interrupt the update process. It may take several minutes. Once completed, a screen will appear stating the update is complete and will prompt you to turn the unit off then back on.
6. Turn the unit off. Wait at least 5 seconds then turn the unit back on.
7. Verify the software version is correct by going to the **Software Updates** screen.

6.1.2 From USB Drive (Through a software file download)

Aside from the network option, the latest software can also be downloaded from Logicube's website and be placed onto a USB flash drive to perform the update/re-install. It is recommended to use an empty USB flash drive.

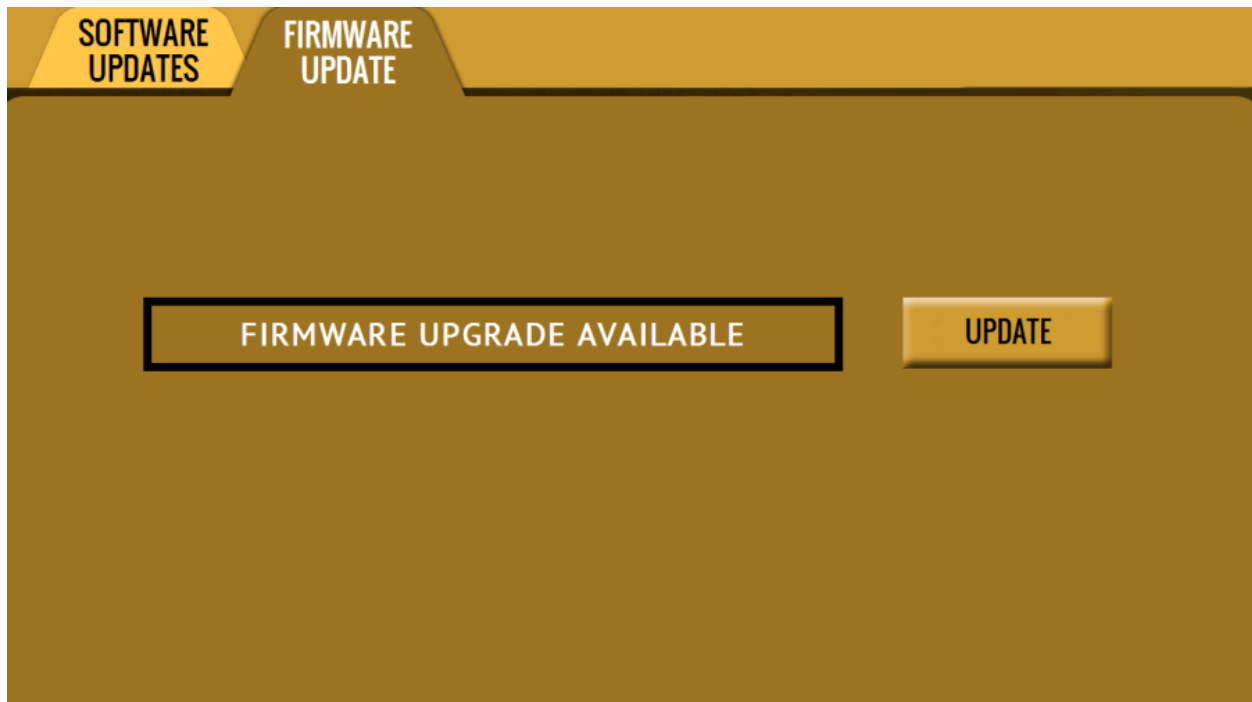
1. Download the latest software from the product support page at <https://www.logicube.com/knowledge/writeprotect>.
2. Extract the contents of the downloaded zip file to the root of the USB flash drive.
3. Turn the unit on. Using the Remote Connectivity feature (see [Section 4.0](#) for details on Remote Connectivity), connect to the WriteProtect.
4. When the main software screen appears, connect the USB flash drive (that has the extracted software from step 2 to the USB_S port.



For the WriteProtect Desktop, connect the USB flash drive to the USB port on the left side.
For the WriteProtect Bay, connect the USB flash drive to the USB port on the front.

5. From the main menu on the unit, locate and click the **Software Updates** icon on the left side.
6. Select **From USB Drive**. The unit then check for the version of the software on the USB drive. After a few seconds, one of the following messages should appear:
 - **Software found** – A software version is found on the USB flash drive. Click the **OK** icon to continue.
 - **No new version found** – The unit did not find any software on the USB flash drive. Double-check that the correct software was downloaded and that the files were extracted to the root of the USB flash drives (steps 1 and 2). Click the **OK** icon to continue and try step 6 again or try updating the software using the "From Network" option.
7. Click the **Update** icon to begin the update. The unit should begin the update process. Do not interrupt the update process. It may take several minutes. Once completed, a screen will appear stating the update is complete and will prompt you to turn the unit off then back on.
8. Turn the unit off. Wait at least 5 seconds then turn the unit back on.
9. Verify the software version is correct by going to the **Software Updates** screen.

6.2 Firmware Loading Instructions



Some software releases may contain a firmware upgrade. The steps below outline how to check if there is a firmware upgrade available:

1. After the software is updated the unit on then click the **Software Updates** icon.
2. Click the "Firmware Update" page. One of two screens will appear:
 - a. **FIRMWARE UPGRADE AVAILABE** – Click the **Update** icon. A message will appear: "FIRMWARE UPDATE COULD TAKE UP TO A FEW MINUTES TO COMPLETE; PLEASE DO NOT INTERRUPT POWER DURING THIS TIME. ON COMPLETION THE UNIT WILL AUTO-RESTART AND CONFIRM THE UPDATE." Click the **OK** icon to start the firmware update process.



When the **OK** icon is clicked, the screen may appear to do nothing. Do not keep clicking the **OK** icon. The firmware update will take no more than 120 seconds. When the firmware update finishes, the unit will reboot automatically.

- b. **FIRMWARE UPGRADE NOT AVAILABLE** – This message will appear if the device does not require a firmware update. No further action is necessary if this message appears.

7: Remote Operation

7.0 Remote Operation - Introduction

The WriteProtect comes with a gigabit network connection in the back of the unit. Connecting the WriteProtect to a network allows remote access to the WriteProtect from any computer within the same network.

The WriteProtect is configured for DHCP by default. See [Section 5.5.1.1](#) for instructions on how to configure the WriteProtect with a Static IP address.

The WriteProtect is setup with a Zero Configuration Network (Zeroconf). There are two ways to access the WriteProtect:

- Web interface – A graphical interface using an Internet browser where the screens are shown exactly the way they appear on the unit.
- Command Line Interface (CLI) – A text only command line interface that can be accessed one of two ways:
 - i. Telnet (via a network connection)
 - ii. SSH (Secure Shell via a network connection)



BROWSER COMPATIBILITY: Google Chrome and Mozilla Firefox are recommended. Other browsers may not display the Graphical User Interface (GUI) properly.

7.1 Web Interface

Using a web browser, go to the IP address or the host name of the WriteProtect. Both IP address and hostname can be found by going to the **Statistics** screen on the unit. For example, browse to <http://192.168.1.100> or <http://wp-XXXXXX> where XXXXXX is the 6-digit serial number of the WriteProtect. The unit's web interface will appear on the browser screen. All screens and operations available on the unit will be available on the browser.



On some browsers or Operating Systems, the WriteProtect will need to be accessed by browsing to <http://wp-XXXXXX.local>.

The WriteProtect can be controlled by clicking on the icons appearing on the browser window.

7.2 Command Line Interface (CLI)

The WriteProtect also has a CLI, or Command Line Interface. This interface has no graphical content and is all command line (text) based and is for advanced users who have knowledge of command line functions. This type of connection requires a Telnet or SSH client. There are several Telnet and SSH clients available from different software companies. Microsoft Windows also has a built-in Telnet client that can be used.



- Windows has a built-in Telnet client but may not be installed by default. Installing the Telnet client may require the assistance of a Network or Systems Administrator. Other third-party Telnet programs are available.
- All versions of Windows do not have a built-in SSH client.
- For assistance on the installation of any SSH or Telnet software (including Microsoft's Telnet client) please check with your IT administrator.

7.2.1 Connecting via Telnet

Once the Telnet client is installed, follow the steps below to connect using the Windows Telnet client.

1. Connect the unit to the network by attaching a network cable (CAT 6 type) to the RJ45 connector (network port).
2. Turn the unit on and allow it to boot up completely.
3. Open the Telnet client.
4. Type **open** followed by the IP address or hostname of the unit. For example: **open 192.168.1.100** or **open wp-XXXXXX** where XXXXXX is the 6-digit serial number of the unit, then press Enter. The unit's login screen should appear.
5. Login with the username **"it"** (without the quotes) and the password **"it"** (without the quotes). A command prompt should appear on the Telnet window.

The unit can now be configured or managed via the command line interface.

7.2.2 Connecting via SSH

Connecting to the unit using SSH (Secure Shell) is very similar to connecting using Telnet. Since Windows does not have a built-in SSH client, a third party SSH client will need to be downloaded and installed to connect via SSH. For instructions and support on how to use third party SSH clients, please contact the SSH client's manufacturer.

1. Connect the unit to the network by attaching a network cable (CAT 6 type) to the RJ45 connector (network port).
2. Turn the unit on and allow it to boot up completely.
3. Open the SSH client and select an SSH connection.
4. Connect to the unit either by IP address or by hostname. The name of the unit will be **wp-XXXXXX** where XXXXXX is the 6-digit serial number of the unit.



On some Operating Systems,
the unit will need to be accessed
by opening wp-XXXXXX.local.

5. Login with the username **"it"** (without the quotes) and the password **"it"** (without the quotes). A command prompt should appear in the SSH window.

The unit can now be configured or managed via the command line interface.

7.3 Zero Configuration Networking (Zeroconf)

The WriteProtect has the capabilities for Zero Configuration Networking (Zeroconf). Zeroconf allows devices to automatically create a usable computer network based on the Internet Protocol Suite (TCP/IP). For example, when the WriteProtect is connected (connected via a network cable) directly to a Windows based computer that is DHCP enabled, both the WriteProtect and the Windows based computer will automatically configure themselves to be seen by each other using TCP/IP with a 169.254.x.x IP address configuration.

Technical Support Information

For further assistance please contact

Logicube Technical Support:

by phone: **(+1) 818.700.8488 8 a.m. – 5 p.m. PT, M-F**
(excluding US legal holidays)

or by email: **techsupport@logicube.com**