ZClone™Xi User's Manual

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

Version: 2.2
Date: 04/08/2021
MAN-ZXi

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 8am – 5pm PT, Monday through Friday, excluding U.S. legal holidays.

Table of Contents

1: Introduction

1.0 Introduction to the Logicube ZCloneXi

The ZClone™Xi (also known as ZXi), delivers advanced features, secure drive wiping and blazing fast cloning speed at 24GB/min in a sleek flat-bed design. The unit can clone up to six targets (up to 10 targets with the optional expansion kit) when cloning from a ZXi created image repository. The ZXi supports SATA and USB3 and supports SAS drives with an optional software activation package. PCIe M.2 SSDs are supported with the optional PCIe Bridge adapter that connects to any of the 3 USB 3.0 ports on the ZXi. The laptop-cloning version of the ZXi allows users to clone up to six laptops (Windows or MAC x86 based) or tablets (Windows x86 based), without removing hard drives, simultaneously. The ZXi is perfect for hard drive imaging tasks including PC deployment, O/S upgrades and content/application distribution.

1.1 Features

- High-speed cloning. The ZCloneXi will clone at blazing speeds of 24GB/min*.
- The ZXi has built-in support for 3.5”/2.5” SATA hard drives. The SAS-ready drive stations support SAS hard drives with the purchase of an optional software activation package.
- 1.8”/2.5”/3.5” IDE and IDE ZIF drives, eSATA, micro SATA, mSATA and compact flash media are supported with optional adapters.
- Supports cloning PCIe M.2, PCIe and mini-PCIe cards using the optional PCIe Bridge and adapters. Connect multiple Bridges (a maximum of 3) to the ZXI’s USB ports to clone from a master drive or an image repository to multiple PCIe drives simultaneously.
- Supports cloning to and from USB enclosures and USB thumb drives. 3 USB 3.0 ports are available.
- Multi-target, volume cloning: Clone from 1 Master to 5 SATA target drives or 5 SAS (if SAS option is purchased) target drives, or clone from a ZXi-created image repository stored on an external USB enclosure or on a network repository to a total of 6 SATA/SAS target hard drives.
- Optional 4 drive expansion kit provides an additional 2 SAS/SATA and 2 SATA targets for a total of 9 SATA targets (7 SAS) when cloning from a master hard drive or a total of 10 SATA (8 SAS) targets when cloning from a network repository or from an external USB enclosure connected to the ZXi. SAS option required to clone to SAS target drives.
- Laptop Cloning Version – Customers can purchase a version of the ZXi (F-ZXI-LAPTOP) that is shipped with a factory-installed feature that provides support for cloning of 6 laptops (Windows or MAC x86 based) or tablets (Windows x86 based) and 6 hard drives simultaneously without removing hard drives from the laptops. Tablets require a docking station enabled with an Ethernet port.
- Supports multiple master/source and target drives. User can assign any drive connected to ZXi as a master/source or target drive.
- Network sharing. Allows network access (upload/download) to drive images and log files. Two Gigabit Ethernet ports are available.
- Multi-session capability. Allows user to perform multiple tasks, including cloning, wiping or hashing concurrently.
- Hash verification (SHA-1, SHA-256 or MD5) allows the user to clone and verify the exact replication of the master drive. Available with the purchase of an optional software activation package.
- Removable drive stations are field replaceable.
- Wipe feature. Sanitizes hard drives to DoD 7-pass specification, offers Secure Erase and custom pass settings.
- Bad sector handling. Scan for bad sectors on the master drive, abort or skip and log for review.
- Multiple cloning modes:
    - Mirror Copy (bit for bit copy). Supports all OS including Linux and Mac.

  - Clever Copy (copies only data areas, skips blank sectors, scales partitions to target). Supports FAT16/FAT32/NTFS and Linux (ext, ext2, ext3, ext4) file systems.
  - Multi-Image Master: Store multiple ZXi-created images in a repository on an attached drive, a USB enclosure connected to ZXi or on a shared network location and then clone to selected targets
  - Partition Cloning: For multiple partition drives, ZXi automatically selects the optimum cloning method (Clever or Mirror)
- Remote operation provides the ability to control all operations from a remote computer using a web browser or CLI interface.
- The Task Macro feature allows users to set specific tasks to be performed sequentially. For example, wipe then clone, then hash.
- Advanced administrative functions allow administrator to create/manage image repositories, manage network settings, create user profiles, save configurations, manage drive station assignments.
- Audit trail/log report provides detailed information on each completed task. Logs can be printed using a web browser and your PC. Includes a digital signature for authentication purposes.
- A color touch screen display provides an intuitive and easy to use interface.
- HPA/DCO support. Clone or wipe HPA/DCO areas of a drive.
- USB 2.0 host ports. Two USB 2.0 host ports are available for connecting a keyboard or mouse to the ZXi.

*Speed referenced was achieved using solid state drives and mirror mode. The specification and condition of hard drives and settings used may affect the achieved speed

1.2 In the Box

The complete ZXi system includes the following:

- The Logicube ZXi unit
- Power cable
- 6 SAS/SATA 5” cables
- CD-ROM with user’s manual

The ZXi-Laptop Cloning Version also includes these additional items:

- Cat6 Ethernet cables
- 2 Gigabit Ethernet switches (with AC adapter/power supply)
- 6 built-in USB cables

1.3 Options

The following options are available with the ZXi:

- SAS drive interface software option. Provides support for SAS hard drives on all drive stations on the base unit and 2 drive stations in the expansion kit.
- Verification/Hash software option. Use SHA1, SHA256 or MD5 to verify the exact duplication of the master drive.
- 4-target expansion kit (includes 2 SATA only drive stations, 2 SATA/SAS drive stations, drive tray, 4 SATA/SAS data/power cables).
- PCIe Bridge: PCIe to USB 3.0 adapter enables access to PCIe M.2 type4 drives, PCIe, and mini-PCIe cards. Requires PCIe adapter kit.
- PCIe adapter kit for M.2 PCIe, PCIe, and mini-PCIe cards.
- 2.5”/3.5” IDE to SATA adapter
- 1.8” IDE to SATA adapter
- 1.8” IDE ZIF to SATA adapter
- 1.8” micro SATA adapter, mSATA to SATA adapter
- eSATA 18” cable
- Flash card reader for compact flash media
- Extended warranties

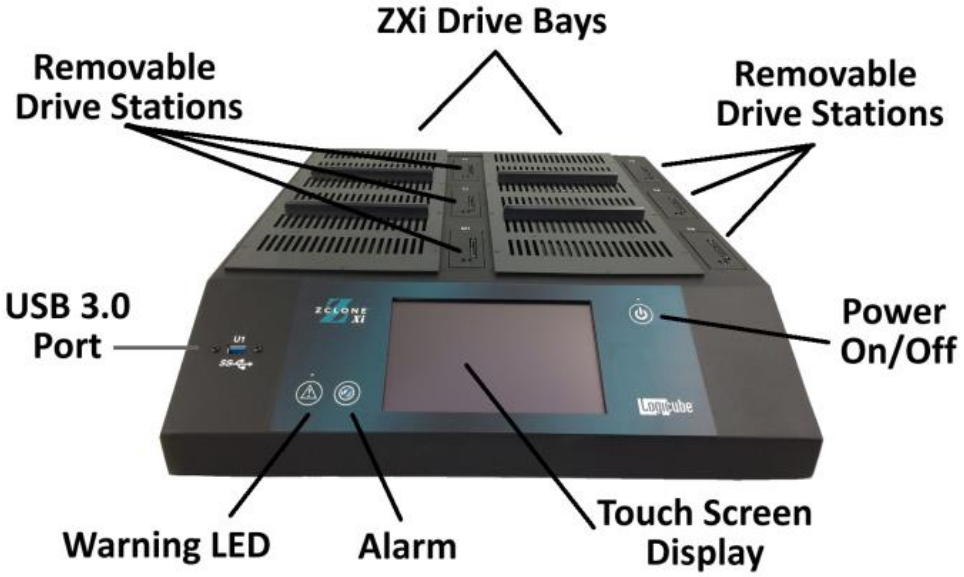
WARNINGS:

- Avoid dropping the Logicube ZXi or subjecting it to sharp jolts. When in use, place it on a flat surface.
- Keep the unit dry. If the ZXi 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 Logicube ZXi. Doing so may void the warranty. If the unit requires service, please contact Logicube Technical Support for assistance.

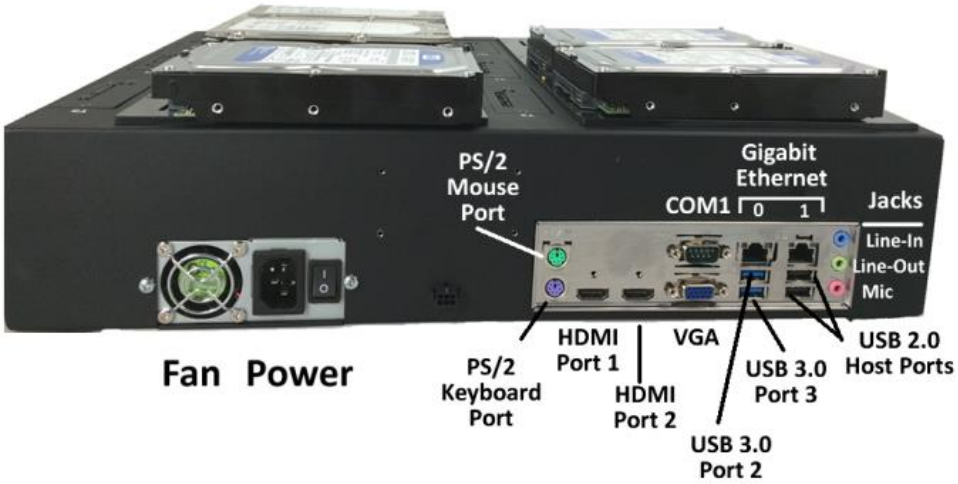
2: Getting Started

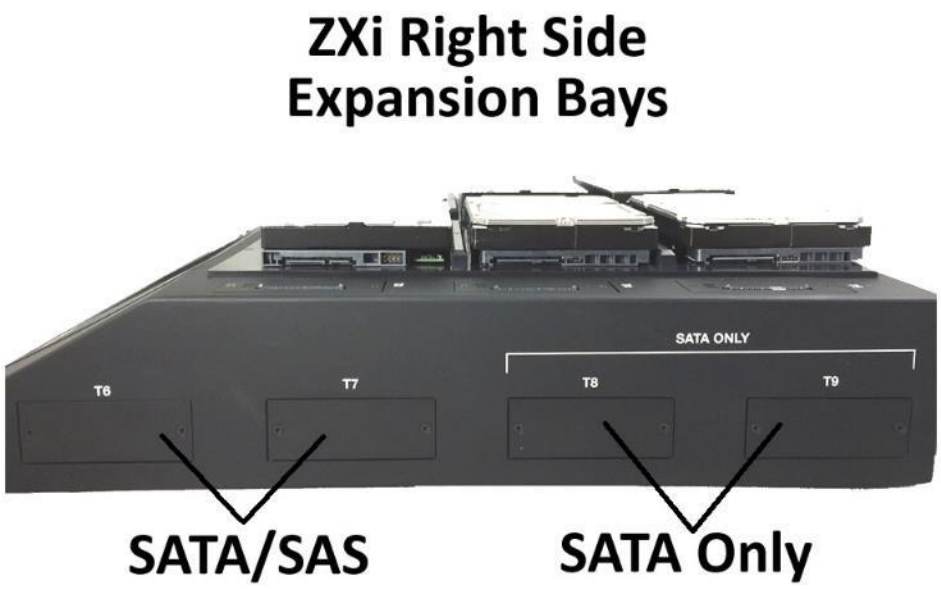
2.0 Overview of the ZXi

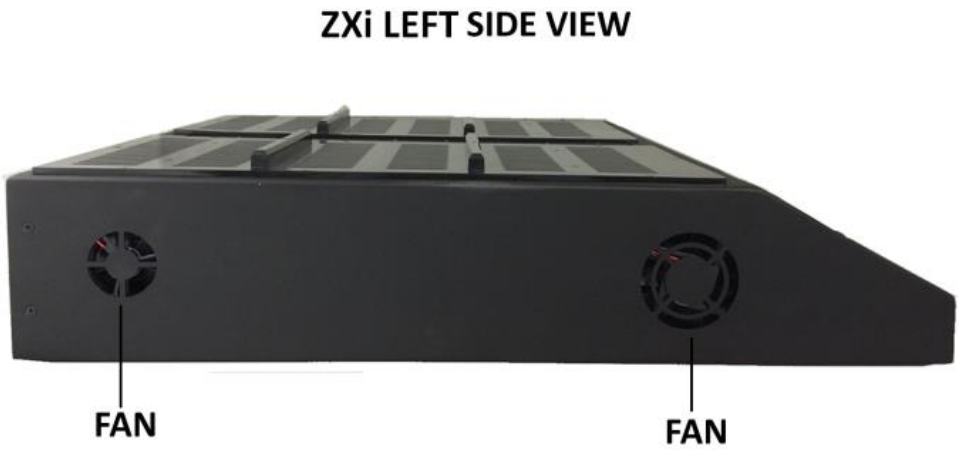
Special Icons – Throughout this manual, there are two icons that can be seen. Please pay close attention when any of these two icons are found. These icons highlight additional information or important warnings on specific topics.



ZXi Rear View







2.1 Turning the ZXi On and Off

The ZXi comes with a standard power cable that connects to the back of the device. Attach the included power cable the power connector in the back of the ZXi.

To turn the ZXi on, turn the power switch (located next to the power connector in the back of the ZXi) to the ON position. Press and release the power button on the front of the ZXi. The ZXi will turn on and start the boot process.

It is normal for the fans to either turn off or slow down after the initial start-up sequence.

To turn the ZXi off, use the Graphical User Interface (GUI) either on the touch screen or using a web browser through a remote connection. Navigate to the ***Power Off*** screen and tap or click the ***Power Off*** icon. Another way to turn the ZXi off is to press and release the power button located on the front of the ZXi.

It is not recommended to use the power switch located on the back to turn the ZXi off.

2.2 Connecting Various Drive Types

The ZXi comes standard with six SAS/SATA cables. One end of the cable has a male connector that connects to the ZXi. On the other end is a female connector that connects to a drive or Logicube adapter.

Support for SAS drives is optional. To verify if you have this feature installed, press the Statistics icon from the navigation menu on the left and select the "Options" tab. If you need to purchase the SAS option, contact our sales team at: sales@logicube.com

Cables and adapters are available for the following drive types:

- SAS
- SATA
- USB
- 1.8" microSATA (optional)
- 2.5" and 3.5" PATA/IDE (optional)
- 1.8" ZIF (optional)
- 1.8" PATA/IDE (optional)
- eSATA (optional)
- mSATA (optional)
- Flash Media (optional)

When drive adapters are being used, it is recommended to keep the drive connected to the adapter, then connect/disconnect the adapter to/from the SAS/SATA cable, or connect/disconnect the SAS/SATA cable from the drive bay.

The ZXi ports are hot swappable. Drives that are not being used in any task (clone, hash, wipe, etc.) can be disconnected any time.

Some drives, however, are not hot swappable. Please check with the drive manufacturer to find out if the drive being used does not support hot swapping.

When disconnecting drives, it is very important to make sure the drives are not being used on any task. Disconnecting drives while the ZXi is using the drive for a task may cause data loss.

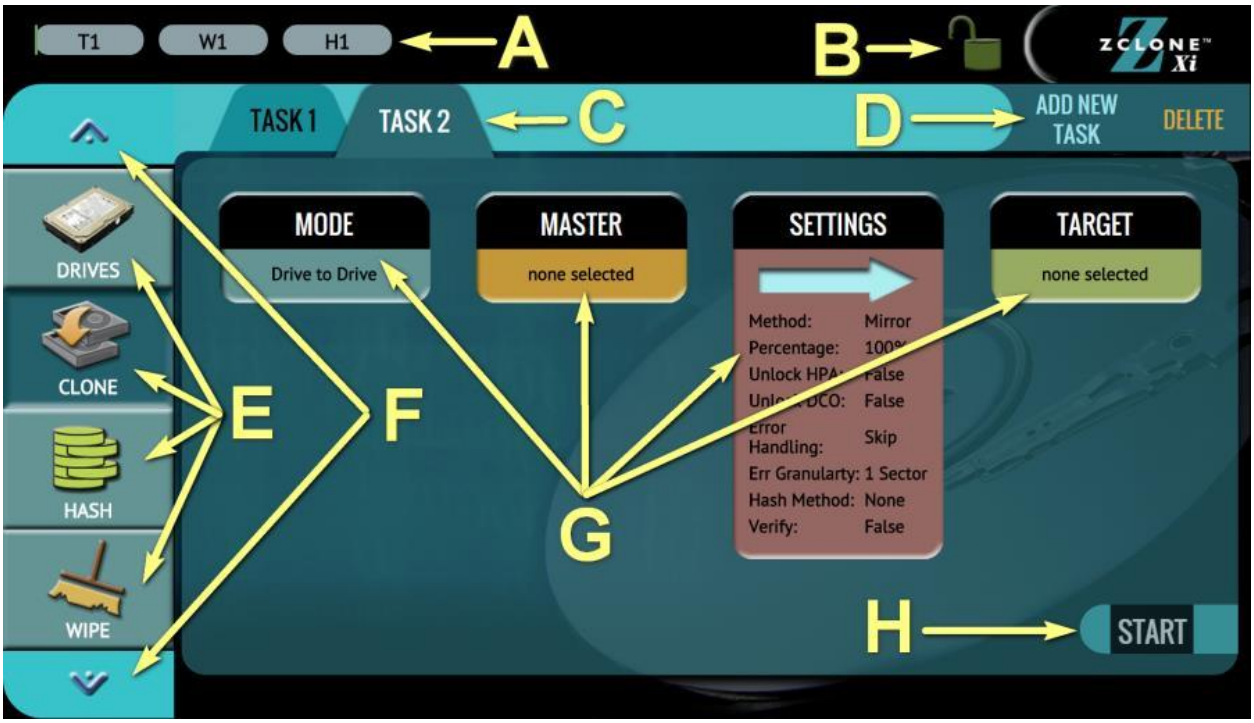
2.3 Drive Bay LEDs

Each bay has a DriveStation that has the following LEDs:

- Green LED
  - OFF – The ZXi is not detecting a connection and is not supplying power to that bay.
  - ON (Solid) – The ZXi is detecting a connection (drive or adapter) and is supplying power to that bay.
- Yellow/Amber LED
  - OFF – There is no activity to the drive/bay.
  - ON (Blinking) – There is activity on the bay. Typically, this means that data is being read from, written to, or the drive's information is being accessed. This is typically blinking when a drive is connected (while the ZXi is gathering drive information details) or during any clone, wipe, or hash task as the ZXi is either reading from the drive or writing to it.
  - ON (Solid) – This LED will turn solid if a drive that is being cloned to, hashed, or wiped stops working, alerting that there may be a problem with the drive.

2.4 The User Interface

The user interface (UI) has been designed to quickly and easily input commands. It is simple and intuitive showing common icons such as tasks, modes of operation, and scroll icons on the screen. The UI is designed to be easily followed, going from left to right across the screen.



A – Operations/Tasks currently running

B – Lock indicator/shortcut

C – Operations/Tasks

D – Add or delete tasks

E – Types of Operations

F – Up and down scroll arrows

G – Operation options and settings

H – Start icon

2.5 Touch Screen

The ZXi features a 7" color LCD capacitive touch screen that allows the user to quickly input commands. The screen is bright and easy to read.

2.6 HDMI

The ZXi has two HDMI ports located in the back panel. Simply connect an HDMI cable from the ZXi to an external display that supports HDMI and the ZXi will automatically show the display on both the ZXi and the external display.

To change the display resolution on the external display:

1. Connect a wired USB keyboard to one of the back USB 2.0 host ports.
2. Press ALT+R. An on-screen display should appear on the external display that allows the display resolution to be changed.

2.7 Operating System and ZXi Application Software

The ZXi has an embedded storage drive that contains the operating system and ZXi software. This drive does not store any data from master drives or target drives.

3: Quick Start

3.0 Quick Start Guide

This chapter gives a basic overview and steps on how to perform different types of operations using the ZXi (Clone, Hash, Wipe, etc.). Complete details on each operation, menu, or selection, and the different screens can be found in **Chapter 4: Cloning** and **Chapter 5: Types of Operation**.

The ZXi can perform up to five (5) concurrent types of operation at the same type (specifically Clone, Hash, and/or Wipe).

It is highly recommended to change the passwords for the built-in accounts. Instructions on how to change the passwords to the two built-in accounts can be found in ***Chapter 10***.

The ZXi clone, hash, and wipe speeds are determined by several factors including the following:

- The manufacturer specifications of the drive(s) being used
- The age of the drive (manufactured date)
- How often that drive has been used

For example, a 2 TB drive with 64MB of cache produced by the manufacturer 2 years ago is most likely slower than a 2 TB drive that the same manufacturer just released this year, even though they are both 7200RPM with 64MB of cache and are both SATA III.

3.1 Drives

This screen shows the status of all drive bays. Each drive bay will be listed whether there is a drive connected or not.

If there is a drive connected, the model of the drive will appear in the Drive Information column and will have a ✔ symbol in the Drive Connected column. If no drive is detected, the bay will have a ✗ symbol.

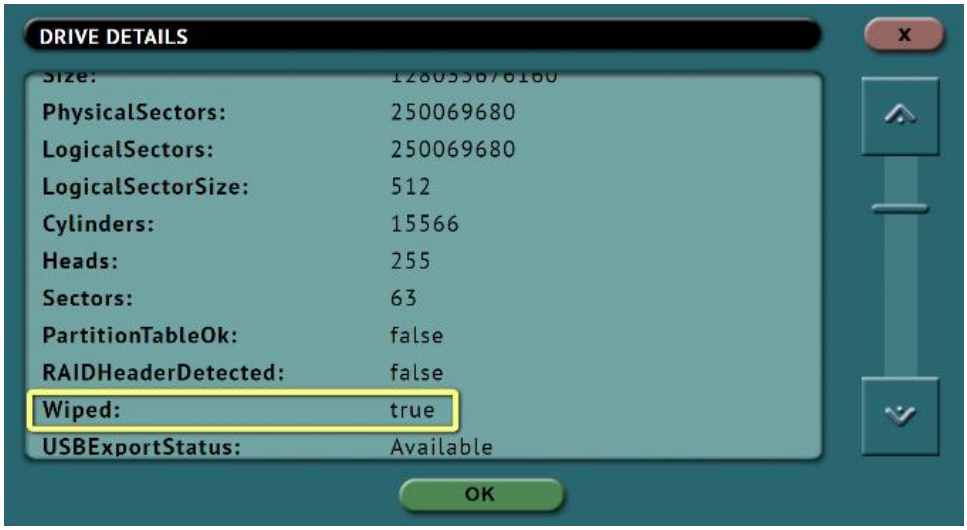
Additional drive information can be viewed by tapping the more info icon.

3.1.1 Blank Disk Check

A blank disk check can be performed to see if a drive has been wiped by the unit. This check will not be accurate if Secure Erase or Pattern Buffers was used to wipe the drive. To perform a blank disk check:

1. Connect a drive to the unit.

2. Choose Clone, Hash, or Wipe/Format.
3. Go to Drives to see the list of connected drives.
4. Tap the ***More Info*** icon to the right of the drive to display information about the drive.
5. Tap or click the down arrow located to the right of the screen to scroll down to the second page of information.
6. Locate the line that shows "Wiped". This will either show ***True*** (drive is blank) or ***False***.



3.2 Clone

This type of operation allows the imaging of a Master drive to one or more Targets. There are three different imaging modes and several settings to choose from. Drives can be cloned using ***Mirror*** (bit-for-bit copy) or ***Clever*** (copies only data areas, skips blank sectors, and partitions can be resized to fit larger capacity drives). These selections should be performed in order from left to right.

Details on the different screens found in the Imaging operation can be found in ***Chapter 4: Cloning***.

For details on cloning drives to a smaller capacity Target, see ***Section 4.0.1***.

- **Drive to Drive** – Performs a bit-for-bit copy of the Master producing an exact duplicate of the Master drive. This is also known as a native copy or mirror copy.
- **Image to Drive –** Restores an image created by the ZXi to one or more Target drives.
- **Drive to Image –** Creates a Logicube ZXi image file to a Target drive or Repository. This image file can be restored to drives using the Image to Drive mode.

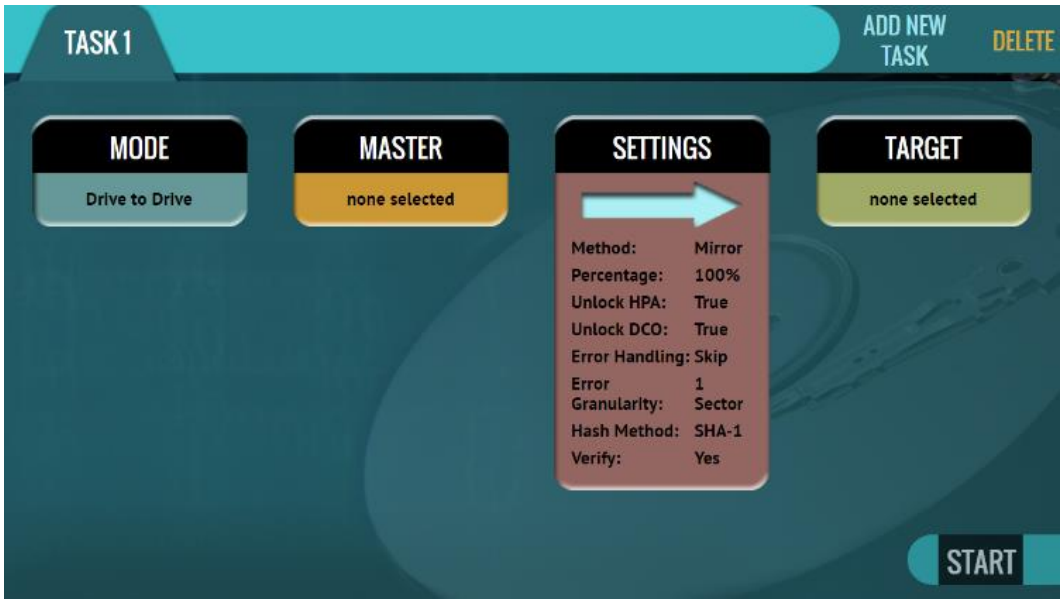
One or more Master drives can be cloned to one or more Target drives by using additional cloning tasks. Any drive bay can be configured as a Master, Target, or both Master and Target. Details on how to change the bay roles can be found in ***Section 5.9.4***.

The ZXi clone, hash, and wipe speeds are determined by several factors including the following:

- The manufacturer specifications of the drive(s) being used
- The age of the drive (manufactured date)
- How often that drive has been used

For example, a 2 TB drive with 64MB of cache produced by the manufacturer 2 years ago is most likely slower than a 2 TB drive that the same manufacturer just released this year, even though they are both 7200RPM with 64MB of cache and are both SATA III.

3.2.1 Step-By-Step Instructions – Clone



1. Select ***Clone*** from the types of operation on the left side.
2. Tap ***Mode*** and select ***Drive to Drive, Image to Drive, or Drive to Image*** then tap the ***OK*** icon.
3. Tap the ***Master*** (or ***Image File***) icon and choose the Master from the list of connected drives then tap the ***OK*** icon.
4. Tap the ***Settings*** icon and adjust the settings as needed (***Job Info***, ***Clone Method Settings, HPA/DCO***, ***Error Handling***, ***Hash/Verification Method***, ***etc.***) then tap the ***OK*** icon.

The Settings screen may be different in each of the modes. Details on the different Settings screens can be found in ***Chapter 5: Types of Operations***.

Log file names can be set in ***Settings*** in the ***Job Info*** screen by entering a Job Name. See ***Section 4.3.1*** for more information.

5. Tap the ***Target*** (or ***Image File***) icon and select the Target or Image File then tap the ***OK*** icon.

For ***Drive to Image***, the ZXi must be used to format drives. If the Target drive is not formatted by the ZXi, the ***Format*** icon will appear in the Format column. Tap the ***(Format)*** icon to format the Target drive.

6. Tap the ***Start*** icon to start the cloning task.
7. A progress bar will appear at the bottom of the screen showing the bytes processed, the rate (speed), elapsed time, and time remaining.
8. When finished, the status will show "COMPLETED". At this point, it is recommended to tap ***Reset Task*** to reset the task, so the drive bays properly reset and not show as being used or assigned for other tasks.

The number of bytes shown on the progress bar is not the actual size of the drive. This is the actual bytes being processed. When 'Verify' is set to "Yes", the reported number will double in size.

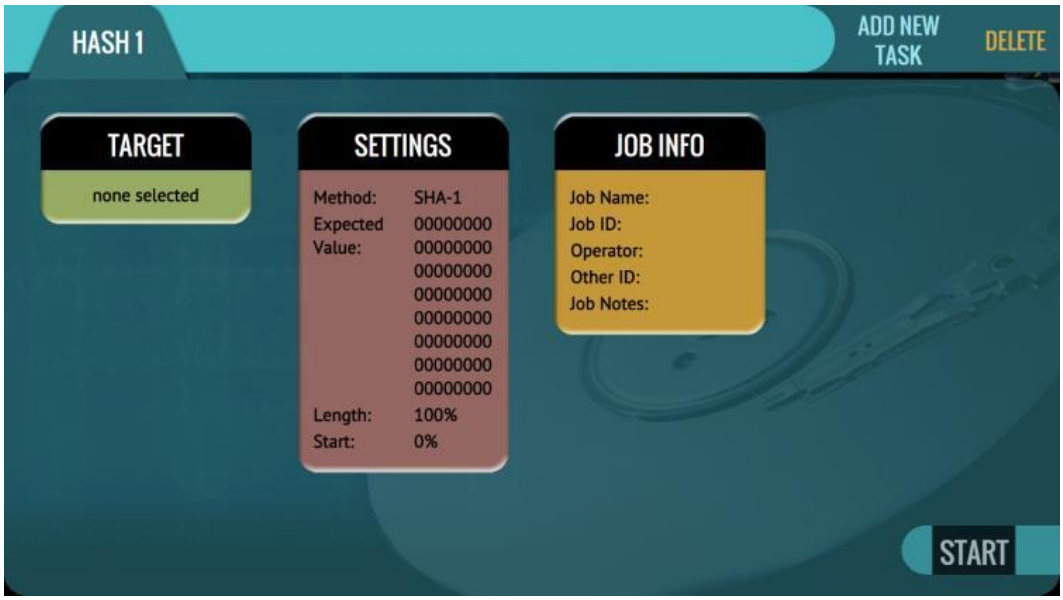
3.3 Hash

A hash or operation can be performed to any connected drive. Performing a hash task will instruct the unit to calculate the hash for the specified drive or validate the hash value for that drive.

Details on the different screens found in the Hash operation can be found in ***Section 5.3: Hash***.

This mode will hash any connected drive on an active Master or Target port. This mode is Logical Block Address (LBA) based and will hash drives based on the number of LBAs. If multiple drives are selected to be hashed, the unit will hash up to the LBA value of the smallest capacity drive. If drives with different capacities need to be hashed, it is recommended to start one task per drive.

3.3.1 Step-By-Step Instructions – Hash



1. Select ***Hash*** from the types of operation on the left side.
2. Tap the ***Target*** icon and select the drive(s) to be hashed then tap the ***OK*** icon.
3. Tap the ***Settings*** icon to choose the different settings based on the Mode. Details for every setting can be found in ***Section 5.3.2***.
4. Change any of the optional settings (LBA settings or percentage of the drive to be hashed) if needed.
5. Optional: Tap Job Info to set the Job Name, Job ID, Operator, Other ID, or Job Notes.
6. Tap the ***Start*** icon to start the hash task.
7. When finished, the status will show "COMPLETED". At this point, it is recommended to tap ***Reset Task*** to reset the task, so the drive bays properly reset and not show as being used or assigned for other tasks.

3.4 Wipe / Format

Drives connected to bays that are configured as Target (or both Master and Target) can be wiped or formatted. Unless formatted (with the ZXi), when a drive is wiped, there will be no file system on the Target drive. The following methods are available in the Wipe menu:

Details on the different screens found in the Wipe operation can be found in ***Section 5.4: Wipe / Format***.

- ***Secure Erase*** – Sends a command to the drive instructing it to wipe the drive based on the hard drive manufacturer's specifications for the Secure Erase command.

Contact the hard drive manufacturer for Secure Erase specifications for each model/type of hard drive.

Secure erase will not work on drives connected through the USB, Thunderbolt, or rear expansion ports.

- ***Wipe Patterns*** – Allows the user to set a specific pattern to use for wiping the drive. The number of passes is customizable (up to 7 passes) along with the type of data written for each pass. In addition, a 7-pass DoD wipe can be set with pre-selected pass values.
- ***Format*** – Formats a drive. Supported file systems are: ***EXT4*** and ***NTFS***.

The unit can perform one, two, or all three methods on the same drive, using the same task. Each method will be performed in order (Secure Erase, Wipe Patterns, then Format) depending on which methods are chosen. For example, if both Secure Erase and Wipe Patterns are selected, the unit will perform a Secure Erase first then a Wipe Patterns wipe.

3.4.1 Step-By-Step Instructions – Wipe / Format

1. Select ***Wipe*** from the types of operation on the left side.
2. Tap the ***Target*** icon and select one or more drives then tap the ***OK*** icon.

   It is recommended to use the same capacity drives per task. When smaller capacity drives are wiped together with larger capacity drives, the smaller drives will finish first. However, the ports will not be available until the entire task is finished.

3. Tap the ***Settings*** icon and choose the type of wipe to be performed (Secure Erase and/or Wipe Patterns). If Wipe Patterns is selected, choose the type of Wipe Pattern to perform (DoD or Custom).
4. If the drive has an HPA or DCO area that needs to be wiped, tap the ***HPA/DCO*** icon and select ***Yes*** to wipe the HPA/DCO area of the drive.

5. Tap the ***Passes*** icon to edit the number of passes and what gets written on each pass.
6. If the drive needs to be formatted, tap the ***Settings*** icon to change the Format settings then tap the ***OK*** icon.

- **FORMAT –** Select ON to format the drive.
- **FILE SYSTEM –** Select which file system will be used to format the drive.

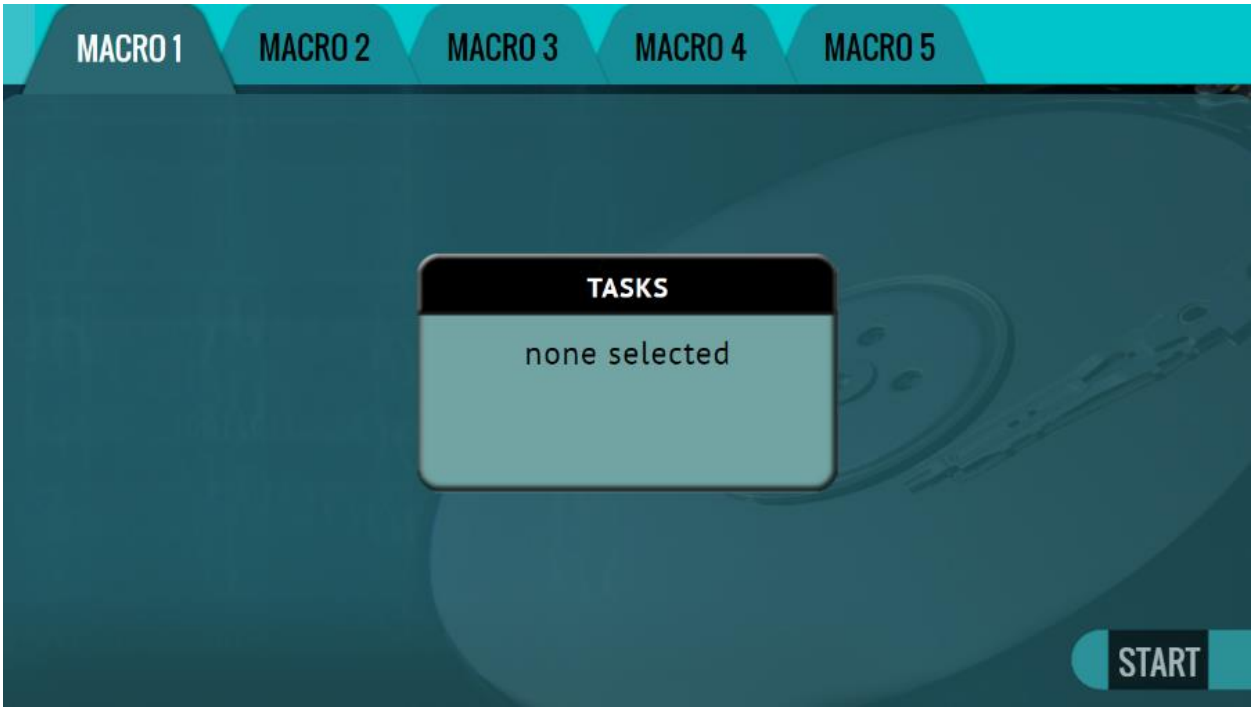
7. Optional: Tap Job Info to set the Job Name, Job ID, Operator, Other ID, or Job Notes.
8. Tap the ***Start*** icon to start the wipe task. A Secure Erase will be performed first (if selected), then a Wipe Pattern (if selected), then finally a Format (if selected).
9. When finished, the status will show "COMPLETED". At this point, it is recommended to tap ***Reset Task*** to reset the task, so the drive bays properly reset and not show as being used or assigned for other tasks.

3.5 Task Macros

This operation allows up to five (5) macros that can be set. Each macro can run up to nine (9) tasks sequentially (one after another). For example, a macro can be set to perform these tasks in order: Wipe then Clone.

Details on the different screens found in the Task Macro operation can be found in ***Section 5.5: Task Macros***.

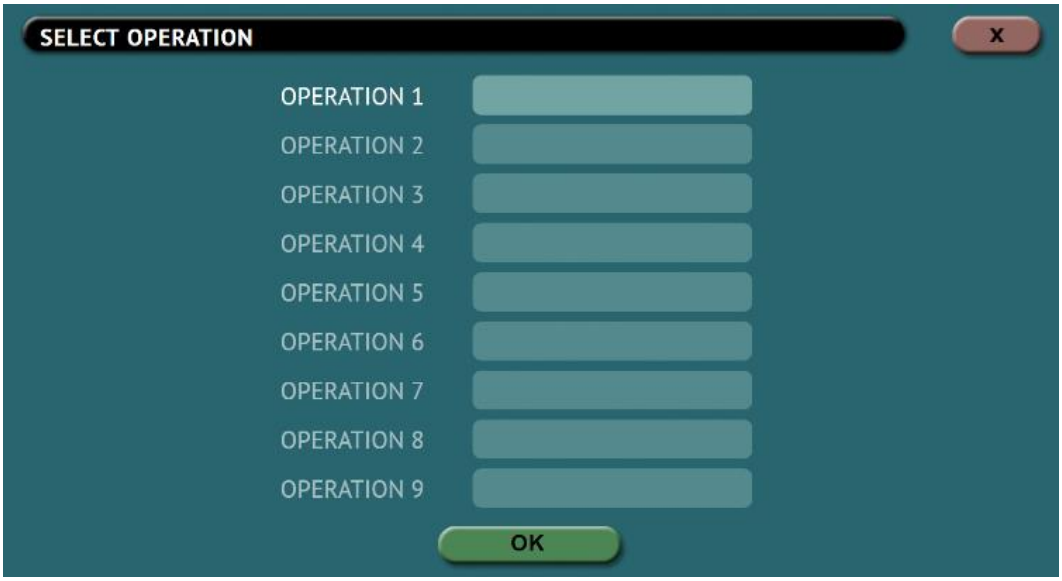
Each of the five macros can be set by tapping on the Macro number as seen in the next picture:



Each task or operation must be set up before setting up the macro. For example, to set up a Task Macro that will perform a wipe, then clone, users must first set up both the wipe and clone tasks. Once the wipe (for example, Wipe 1) and clone (for example, Image 1) has been set up, the Task Macro can be set.

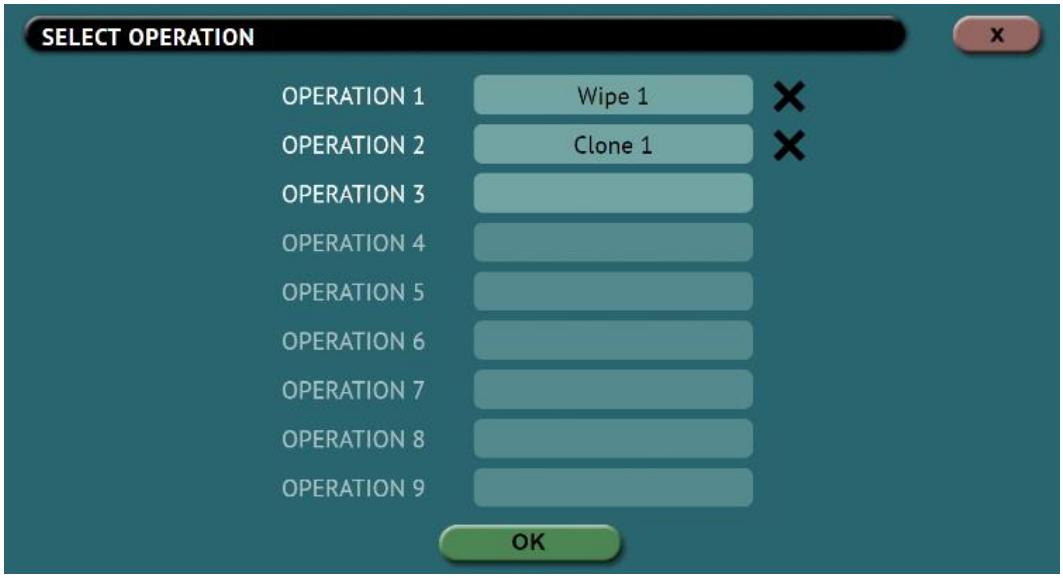
3.5.1 Step-By-Step Instructions – Task Macro

Tapping this icon allows the user to set specific tasks for each macro. The following window will appear:



Tap ***Operation 1*** to set the first operation in the macro. The following screen will appear allowing the user to choose the task. Tap the ***OK*** icon to continue.

Continue adding operations desired. Each operation added will appear on the list. To delete an operation, tap the ***X*** to the right of the operation.



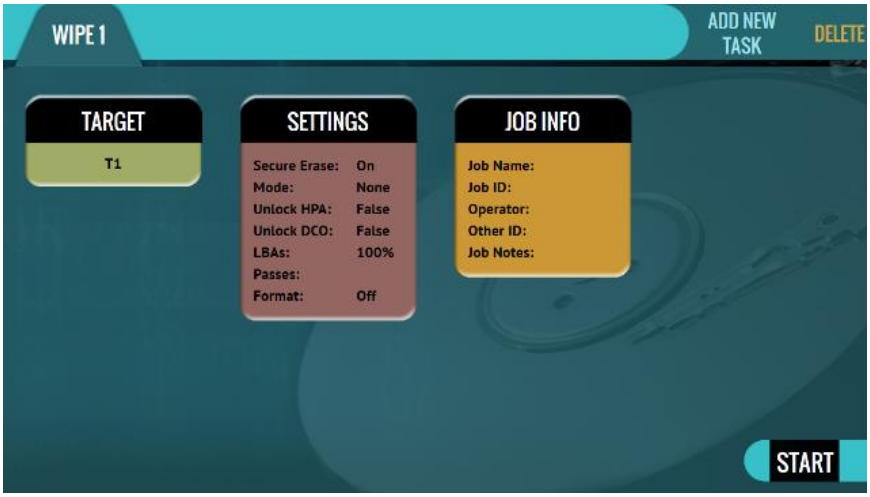
When finished, tap the ***OK*** icon. A summary of the macro will be seen:

To start the macro and have the unit perform all the operations on the task list, tap the ***Start*** icon in the Task Macro screen.

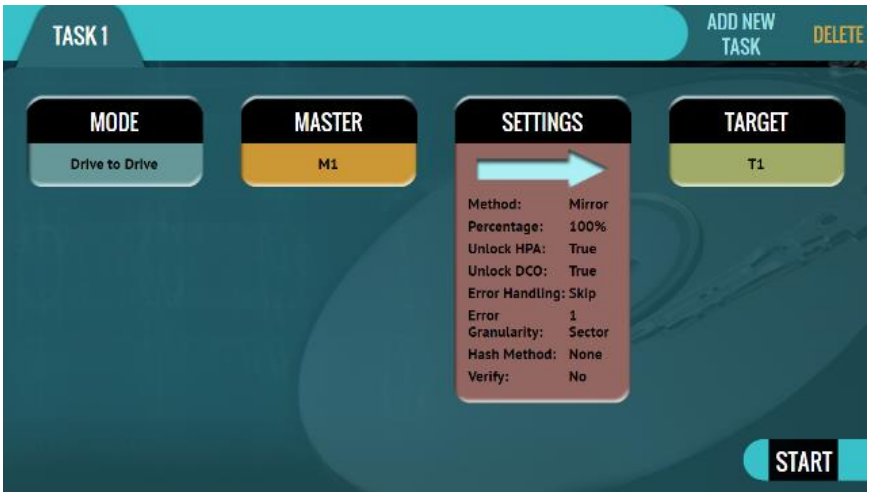
Example: Setting up a Macro for a Wipe to Secure Erase then perform a Drive to Drive Clone

To set a macro to perform a Wipe using Secure Erase on T1, immediately followed by performing a Drive to Drive Clone from M1 to the newly wiped (secure erased) drive on T1, the Wipe and Clone Tasks first need to be set up.

1. First, set the Wipe task. Select T1 as the Target and change the setting to perform a Secure Erase (Wipe Patterns and Format set to off). Do not start this task.



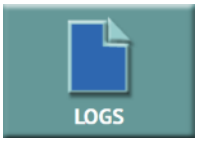
2. Next, set the Clone task. Select Drive to Drive as the Mode. Select M1 as the Master. Change the settings as needed. Select T1 as the Target. Do not start this task.



3. Choose ***Task Macro*** from the list of operations on the left side.
4. Tap the ***Tasks*** icon to select the different tasks for the macro.
5. Tap the field next to ***Operation 1*** to set the first operation. Since the first task to be run is the Wipe task, select ***Wipe 1*** then tap ***OK***.
6. Tap the field next to ***Operation 2*** to set the second operation. Since the second task to be run is the Drive to Drive Clone task, select ***Clone 1*** then tap ***OK***.
7. The screen should now show ***Wipe 1, Clone 1*** as the Tasks for the macro.

8. Tap the ***Start*** icon to begin the macro. The macro will run the Wipe 1 task first, then Clone 1.

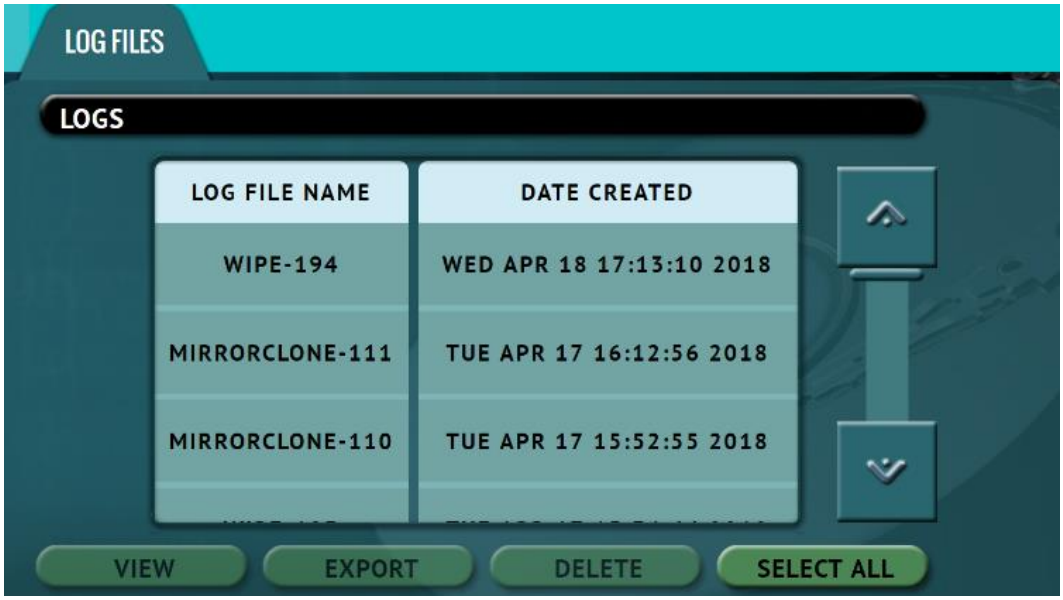
3.6 Logs



Logs of all clone, hash, and wipe operations are stored and saved on the unit. Logs can be viewed directly on the unit or from a computer's browser (if the unit is connected to a network). In addition to viewing, the logs can be exported to an external USB location such as a USB flash drive. Logs are exported in PDF, HTML and XML format.

Details for the Logs screen can be found in ***Section 5.6: Logs***.

3.6.1 Step-By-Step Instructions – Viewing or Exporting Logs



1. Select ***Logs*** from the types of operation on the left side. A list of log files will appear sorted by date (newest on top).
2. Select the log file to view by tapping the name of the log file. This will highlight the log file chosen.
3. Tap the ***View*** icon to view the log file on-screen. The log files can also be exported to a USB drive. To export the log files:

    a. Connect a formatted USB flash drive to one of the USB 2.0 ports located in the back panel of the unit. Disconnect any other drive connected to the USB 2.0 ports.

    The USB flash drive connected to the USB 2.0 port must be formatted in Windows using the NTFS, FAT32, or FAT file system.

    b. Tap the ***Export*** icon to export the log file to a USB flash drive. The log will be exported/copied to the attached USB drive and will be in HTML, PDF, and XML formats.

    Repeat steps 2 and 3 if other log files need to be exported or viewed. Alternatively, all the log files can be exported by tapping the ***Select All*** button to select all the log files. Once all log files are selected, they can be exported in a single operation.

    Log files can also be accessed over the network. See ***Section 3.6.3*** for details.

    To print the log files, it is recommended to use the web interface as described in ***Chapter 7: Remote Operation*** and click the print icon on the upper-right corner of the screen. The browser's print menu will appear, and the log can be printed to an available printer on configured on the computer.

3.6.2 Deleting Log Files

Log files can be deleted one at a time or all at once.

- To delete a single log file, tap the log file to highlight the log file to be deleted. Tap the ***Delete*** icon to delete the selected log file.
- To delete all the log files, tap the ***Delete All*** icon.

A log file deletion password can be set to add a layer of security when deleting log files. If a password was set, log files cannot be deleted without entering the correct password.

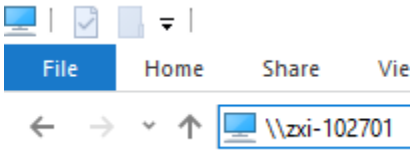
- If a log file deletion password was not created, a confirmation screen will appear confirming to delete the single log file or all log files.
- If a log file deletion password was created, a screen will appear prompting to enter the log file deletion password. Enter the log file deletion password. Tap the ***OK*** icon to delete the single log file or all the log files (depending on which was selected).

The password can be set in the ***Systems Settings***. More information about the log file deletion password can be found in ***Section 5.9.2***.

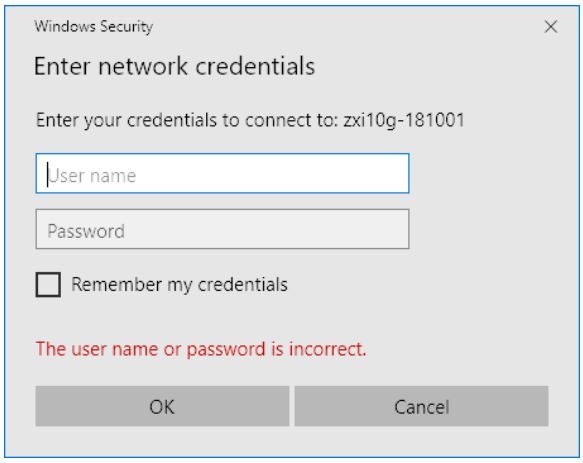
3.6.3 Accessing the Logs Over a Network

The log files can also be accessed through a network on a computer if the unit is connected on the same network.

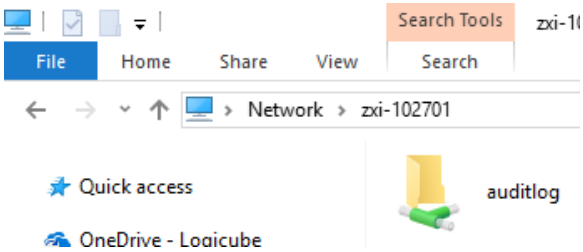
1. Open Windows Explorer or a similar window and browse to the hostname or the IP address found in the Statistics screen. See ***Section 5.7*** for more information on the Statistics screen.



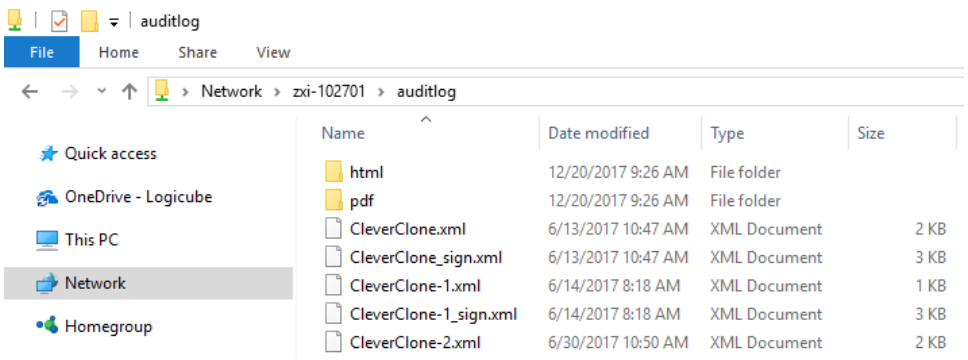
2. A Windows security screen will appear prompting to enter a User name and Password to connect to the unit. Login with the following credentials:
   - User name: ***it***
   - Password ***it***



3. Once connected, an ***auditlog*** folder will appear. Open the ***auditlog*** folder.



4. The auditlog folder contains the HTML, PDF, and XML files for each of the log files. There will be two folders (html and pdf) that contain either the HTML or PDF versions of the log files. The XML files can be used with any XML viewer which allows for some customization on how the information can be viewed.



3.7 Statistics

This will display the following tabs: ***About***, ***Adv. Drive Statistics***, ***I/O Ports***, ***Options***, and ***Network Interface Stats***.

Details on the different Statistics screens can be found in ***Section 5.7: Statistics***.

- **About** – This screen will show information about the unit including the current software installed.
- ***Adv. Drive Statistics* –** Displays S.M.A.R.T. information taken directly from what the drive is reporting.
- ***I/O Ports* –** Displays a diagram of the input and output ports located in the back of the unit.
- **Options –** Displays which optional software is available and what is installed.
- **Network Interface Stats –** Displays the Network Interface statistics (Receive and Transfer bytes, packets, drops, and errors, and the link status).

3.8 Manage Repositories

Repositories can be added to the unit in this operation. Repositories can be drives connected to the Target ports of the unit (automatically shown) or shared folders over a network. SMB, CIFS, NFS, and iSCSI protocols are supported.

Details on the different Manage Repositories screens can be found in ***Section 5.8: Manage Repositories***.

3.9 System Settings

The ***System Settings*** screen allows users to configure different settings for the unit:

Details on the different System Settings screens can be found in ***Section 5.9: System Settings***.

- Profiles
- Passwords
- Language/Time Zone
- Bay Roles

3.10 Network Settings

There following tabs are seen in the Network settings:

Details on the different Network Settings screens can be found in ***Section 5.10: Network Settings***.

- ***Services –*** The network settings screen allows certain network services to be enabled or disabled.
- ***Interfaces –*** Allows the configuration of the network interface which include setting a static IP address and allows certain network services to be enabled or disabled.
- ***HTTP Proxy –*** For the unit to be able to update software from a network (over the internet), proxy settings may need to be set. Networks that have a proxy server for internet access will require proxy settings for devices like this to connect to the Internet. This typically includes a server (or IP address), a host port, a username and password.

3.11 Software Updates

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

Details on how to perform a software update, software re-load, or firmware update can be found in ***Chapter 8: Updating/Loading/Re-loading Software***.

3.12 Power Off

The following tabs can be found in the Power Off screen:

Details on the different Network Settings screens can be found in ***Section 5.13: Power Off***.

POWER OFF – The unit can be remotely turned off or restarted by going to this tab. Additionally the unit's screen can be refreshed.

DRIVE POWER – Inactive drives connected to the unit can be set to go to standby mode in this tab. The default is set to 0 minutes (OFF).

4.0 Cloning

This type of operation allows the cloning of a Master drive to one or more Targets (other drives or a repository). There are three different imaging modes and several settings to choose from. These selections should be performed in order from left to right. ***Mirror*** (Performs a bit-for-bit copy of the Master drive or image) or ***Clever*** (Clones only sectors with data, skips blank sectors, and can expand partitions depending on the settings used) can be used.

There are four selections when performing a clone:

- Mode
- Master/Image File
- Settings
- Target/Image File

4.0.1 Cloning to Smaller Capacity Drives

Regardless of the Operating System, Target drives should be at least the same capacity or larger than the Master drive. Specifically, each Target drive must have the same number of sectors (or Logical Block Addresses/LBAs) or a larger number of sectors or LBAs than the Master.

If the Master drive is larger in capacity than any Target drive, it is still possible to clone the drive, but there are some adjustments that will need to be made to the Master drive. The following applies to any Operating System:

- The total partition sizes on the Master drive need to be adjusted to be less than the capacity/size of the smallest Target drive.
- The partitions on the Master drive need to be adjusted so that the free/unallocated space is at the end of the drive.

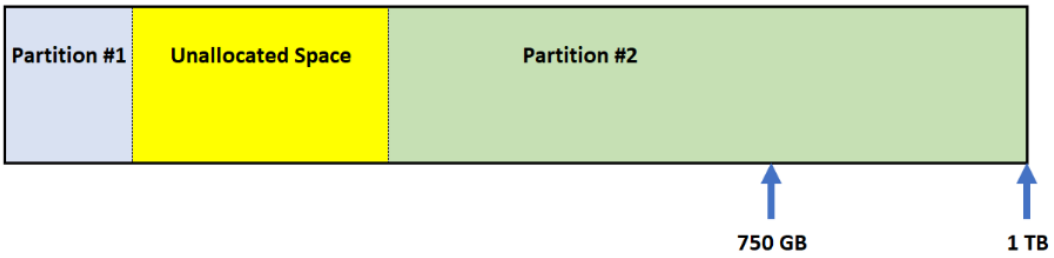
Before making any changes to the Master drive, it is highly recommended to make a backup copy of the Master drive by performing a Mirror copy of the drive to make sure there is an exact duplicate backup of the Master drive.

Logicube cannot provide support on how to re-size, shrink, or move partitions. There are several articles and software/utilities/tools available on the internet on how to re-size, shrink, or move partitions.

Sample original drive (1 TB drive):

Sample of a properly adjusted drive (from a 1 TB drive to fit a 750 GB drive):

Sample of an adjusted drive that will not work (from a 1 TB drive to fit a 750 GB drive):



Once the partitions have been adjusted to properly fit the Target drive, it can be cloned using any of the cloning methods. Depending on the Operating System and cloning method used, there may be limitations to cloning the drive.

4.0.2 BIOS, UEFI, Partitioning Schemes, and Sector Sizes

The ZXi supports the following:

- **BIOS & UEFI –** Drives that come from devices that use BIOS or UEFI are supported.
- **MBR & GPT –** Both partitioning schemes are supported.
- **512 & 4096 (4K) Sector Size Drives –** Drives with these two common sector sizes are supported. The Target drive(s) must be the same sector size as the Master drive.

4.0.3 Mirror Copy Limitations

Mirror Copy method performs a bit-for-bit copy of the Master drive, producing an exact duplicate of the Master drive. There are very few possible limitations when using Mirror Copy (e.g., sector size, drive health, etc.). There is one other possible limitation when using the Mirror Copy method:

The Target drives should be the same capacity or larger. If the Target drive is smaller in capacity, please see ***Section 4.0.1***, then set the Clone Method Setting to the proper percentage of the drive (for example, if the Target drive is 750 GB and the Master is 1 TB, clone no more than 75% of the drive), or set the number of blocks (LBAs) to match the Target drive's number of blocks (LBAs).

4.0.4 Clever Copy Limitations

Clever Copy method copies only data sectors and fills the rest of the drives with zeroes (blank space) and can expand partitions to fill the rest of the drive or a percentage of the drive. If one of the partitions (file systems) is not supported by Clever Copy, the Logicube device will automatically use Mirror Copy for that partition. Here are some limitations when using the Clever Copy method:

- For Windows, all System Restore, Recovery, and OEM partitions should not be expanded.
- The Target drives should be the same capacity or larger. If the Target drive is smaller in capacity, please see ***Section 4.0.1***.

4.0.5 Cloning BitLocker Encrypted Drives

Drives that are encrypted with BitLocker can be cloned. BitLocker only encrypts partitions (not the entire drive). Depending on the cloning method, the following behavior is expected:

Mirror – Since Mirror is a bit-for-bit clone of a drive, the Target drive (including the BitLocker encrypted partition) will be an exact duplicate of the Master drive.

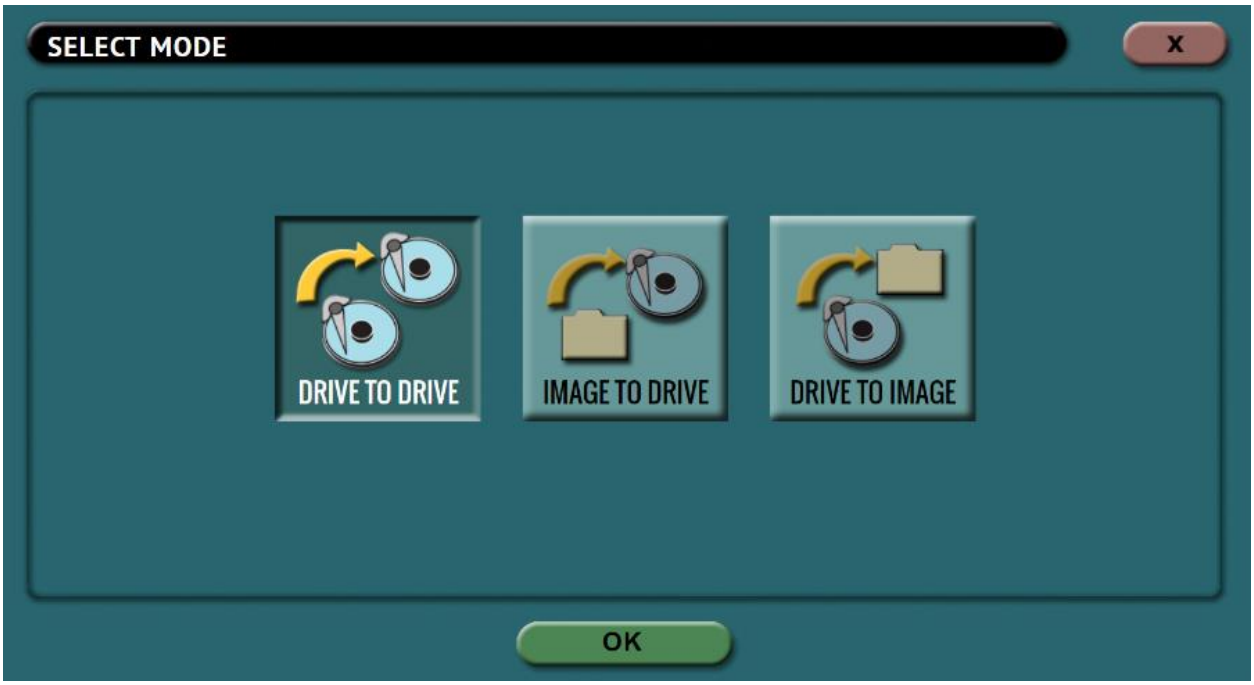
Clever – Using Clever, partitions can be resized. However, when cloning BitLocker encrypted drives, it is highly recommended to keep the BitLocker encrypted partition size the same as the Master (do not resize the BitLocker encrypted partition).

If a BitLocker encrypted partition is resized, the partition will be resized (as seen in Disk Management) but the actual volume size (drive letter) will remain the same as the Master drive's volume size.

Another option is to first decrypt the drive before cloning. This will completely remove all key protectors from the drive. Once decrypted, the drive can be cloned using Mirror Copy or Clever Copy. If Clever Copy is used, the partition can be resized to a larger size.

4.1 Mode

Tap this icon to choose between the following imaging modes:



- **Drive to Drive –** Clones one Master drive to one or more Target drives.
- **Image to Drive –** Restores a ZXi created image file to one or more drives.
- **Drive to Image –** Creates an image file from the Master drive. The image file can be written to a drive or a network repository.

4.2 Master/Image File

When ***Drive to Drive*** or ***Drive to Image*** mode is selected, the Master window will show all drives connected to the bays or ports configured as Master (or both Master and Target).

When ***Image to Drive*** mode is selected, the Image File window will list all available drives that may contain ZXi image files.

The ***(More Info)*** icon displays more information on the drive. The drive details window will appear showing information about the drive.

4.3 Settings

Tap the ***Settings*** icon to change the image settings. Depending on the selected mode, different screens will appear.

- **Job Info –** Available in all modes (See ***Section 4.3.1***).
- **HPA/DCO –** Available in the following modes (See ***Section 4.3.2*****:**
    - Drive to Drive
    - Drive to Image
- **Error Handling –** Available in all modes (See ***Section 4.3.3***).
- **Hash/Verification Method –** Available in all modes (See ***Section 4.3.4***). Hash Method is not available in Image to Drive.
- **File Image Method Settings –** Available in Drive to Image mode (See ***Section 4.3.5*****)**.
- **Clone Method Settings –** Available in the following modes (See ***Section 4.3.6***):
    - Drive to Drive
    - Image to Drive

4.3.1 Job Info

Job Info is available in all cloning modes and allows users to enter information about the job. Job Info is not required to start a clone operation. Information entered here will appear in the logs.

Tap any of the boxes and an on-screen keyboard will appear allowing information to be entered. After entering the information, tap the ***OK*** icon to go back to the previous screen.

Log names and file names can be customized by entering a ***Job Name***. if a clone operation is performed, and the Job Name is set to ***TestJob***, the log name and file name will be called ***TestJob***.

Subsequent Job Names that are the same will be identified with a dash, then the next image number. For example, TestJob-1, TestJob-2, etc.

The unit will convert any non-POSIX portable characters used in ***Case/File Name*** field to underscores "_" when creating the log or file names.

POSIX portable characters are:

Uppercase A to Z	Period (.)
Lowercase a to z	Underscore (_)
Numbers 0 to 9	Hyphen/Dash (-)

4.3.2 HPA/DCO

HPA/DCO is available in the following modes: ***Drive to Drive*** and ***Drive to Image***.

An HPA or DCO configuration on a hard drive is designed to change drive characteristics such as drive capacity, speed and other settings as they are reported to the computer's BIOS.

The HPA/DCO setting allows the user to set whether a drive's HPA or DCO is to be unlocked and imaged. Select ***YES*** to unlock and image a Host Protected Area (HPA) or Device Configuration Overlay (DCO).

HPA and **DCO** – Host Protected Area and Device Configuration Overlay are reserved areas on a drive designed to store information in such a way that it cannot be easily modified, changed, or accessed by the user, BIOS, or the OS.

4.3.3 Error Handling

Error Handling is available in all modes. When bad sectors are encountered on the Master drive, the unit can either ***skip*** the bad sectors or ***abort*** the imaging operation. This allows flexibility on what to do when bad sectors are found on the Master drive.

When bad sectors are encountered, and error handling is set to ***Skip***, the unit will write a zero on the corresponding sector or position in the Target drive.

There is also has a setting for error granularity. There are 3 options:

- 1 sector (512 Bytes)
- 4096 Bytes (8 sectors)
- 64 KIB (128 sectors)

When a bad sector on the Master drive is found, by default, it will skip that sector. Changing the granularity allows more sectors to be skipped.

A cluster size represents the smallest amount of disk space that can be used to hold a file. The most common cluster size for an NTFS volume, for example, is 4KB (4096 Bytes). This means that the smallest amount of space that will be used for a file is 4096 Bytes.

As an example, if 4096 Bytes is chosen, and one of the 8 sectors in that cluster size contains a bad sector, the unit will skip the entire cluster (or 4096 bytes or 8 sectors).

4.3.4 Hash/Verification Method

The Hash/Verification method screen is available in all modes. Hash is not available in ***Image to Drive*** but is available in other modes. Verification is available in all modes.

The Hash Method selection is shown in ***Image to Drive*** but is not selectable. The unit will automatically use the hash method that was selected when the image was created (using Drive to Image).

Hash – Will hash the Master drive with the selected method. There different hash algorithm options available, depending on which Imaging mode is selected:

- **None –** No hash of the Master will be performed. This is available only when using the following mode:
  - Drive to Drive
- **SHA-1 –** Uses the SHA-1 algorithm to hash the Master. This is available when using the following modes:
  - Drive to Drive
  - Drive to Image
- **SHA-256 –** Uses the SHA-256 algorithm to hash the Master. This is available when using the following modes:
  - Drive to Drive
  - Drive to Image
- **MD5 –** Uses the MD5 algorithm to hash the Master. This is available when using the following mode:
  - Drive to Drive

Verification Method/Verify – Available selections are **YES** or **NO**. Select ***YES*** to hash the Target and verify that hash with the hash calculated from the Master.

The Verify feature is an option. To verify if this option is installed, press the ***Statistics*** icon from the navigation menu on the left and select the ***Options*** tab. To purchase the SAS option or verification option, contact our sales team at: sales@logicube.com.

4.3.5 File Image Method Settings

The File Image Method Settings screen allows the user to select a file image output mode. The output modes available are:

- **Mirror –** Creates a bit-for-bit image of the Master.
- **Clever –** Copies only sectors containing data and compresses the image file.

4.3.6 Clone Method Settings

When ***Drive to Drive*** or ***Drive to Image*** mode is selected, ***Clone Method Settings*** will appear on the top-right of the Settings screen. Depending on the cloning method chosen, the Clone Method Settings screen has can have different settings:

Mirror – If mirror is selected or used, the following settings are available:

- **Length –** Set the percentage or number of blocks to clone. By default, this is set to 100% of the Master.
- **Master Start –** Set the percentage or number of blocks from the start of the Master. By default, this is set to 0%, or the beginning of the Master.
- **Target Start –** Set the percentage or number of blocks from the start of the Target. By default, this is set to 0%, or the beginning of the Target.

The specific number of blocks can be set for each of the options by tapping the ***(edit)*** icon.

This screen also displays an option to select whether the Master drive is a part of a RAID configuration or a NON-RAID configuration.

When cloning from drives from a RAID configuration, the Target drives may need to be initialized through the computer's RAID controller before being cloned to.

Clever – If clever is selected or used, the following settings are available:

- **Partition Resize –** This screen will show the number of partitions found on the Master drive and for each supported partition, a resize percentage setting will be shown.

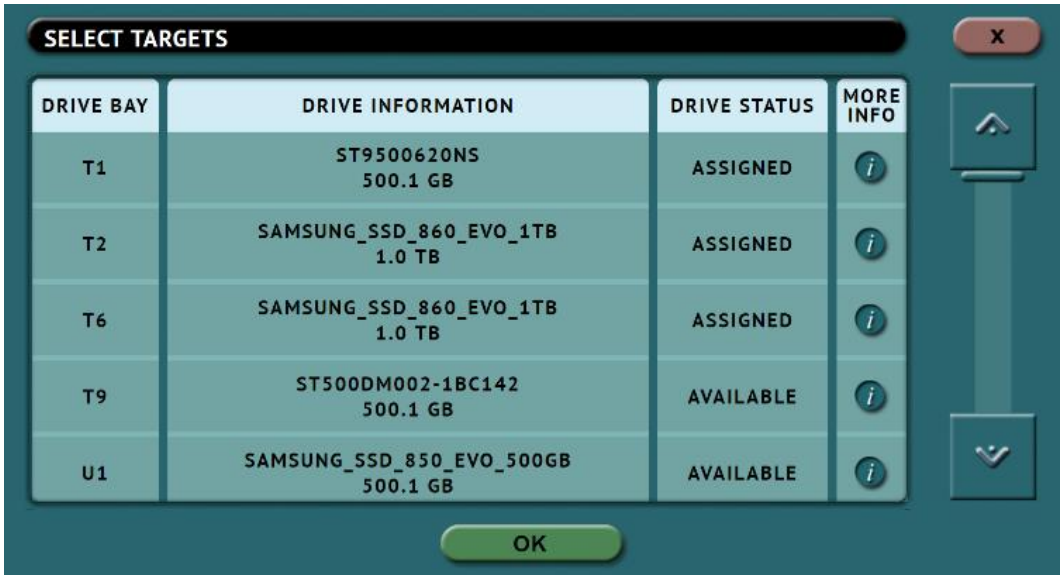
It is recommended that all System Restore, Recovery, and OEM partitions should not be expanded. Setting the slider/percentage to 0% will instruct the unit to keep the same partition size. The percentage value, when set from 1 to 100 will determine what percentage of the Target drive(s) will be used. For example, setting the percentage value to 100% would instruct the unit to use the entire remainder of the Target drive for that partition.

4.4 Target/Image File

Tap the ***Target*** or ***Image File*** icon to select which drive(s) will be used as the Target drive or which image file will be used as the image. When ***Drive to Drive*** or ***Image to Drive*** is chosen from the Mode settings, this will show the different drives connected to the ZXi. When ***Drive to Image*** is chosen from the Mode settings, this will show the repository screen which contains the different images located on the ZXi's repository drive.

4.4.1 Selecting Target Drives or Images

If ***Drive to Drive*** or ***Image to Drive*** was chosen as the mode, the following screen will appear. This will allow the selection of one or more Targets. It will display all available drives that are connected and set as a Target (or Both Master/Target).

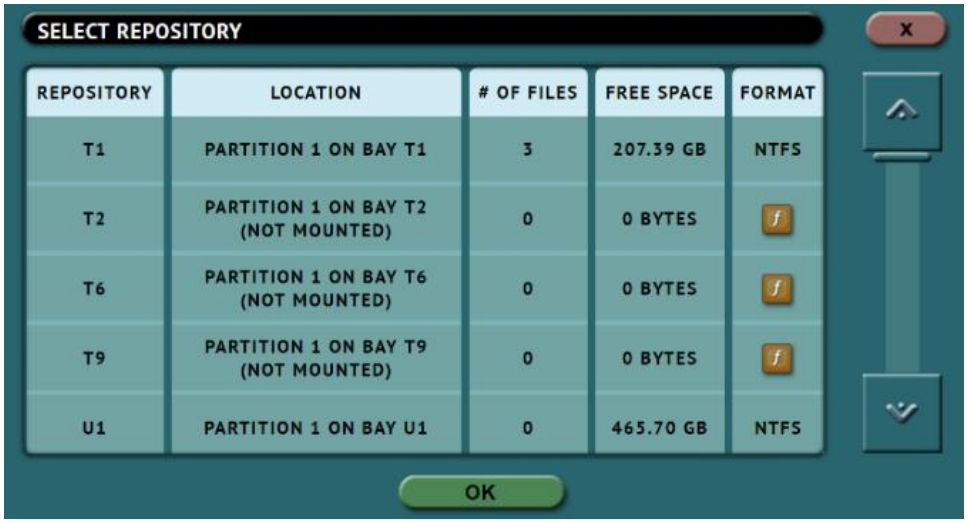


The ***(More Info)*** icon displays more information on the drive. The drive details window will appear showing information about the drive.

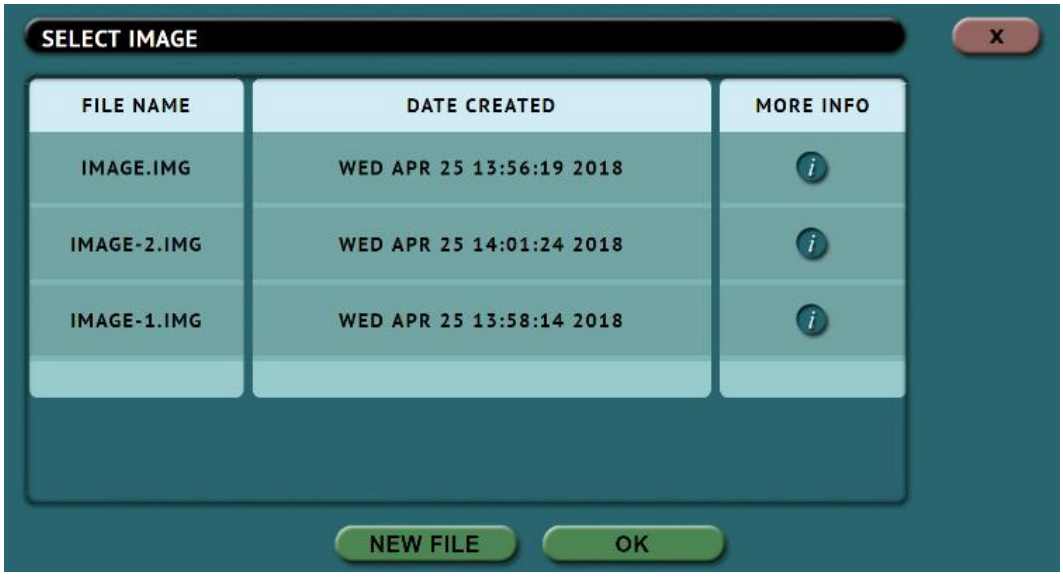
If 'DRIVE TO IMAGE' was chosen as the mode, the following screen will appear. This allows the selection of a repository.

The example below shows the following:

- An unformatted drive on T2, T6, and T9 that can be formatted to be used as a repository to store images (the ZXi can format a drive using EXT4 or NTFS for repository purposes)
- A formatted drive on T1 and U1 that can be used as a repository



Once a repository is selected, a new image file can be created by tapping the ***New File*** icon. An image name can be auto-generated, or user specified.

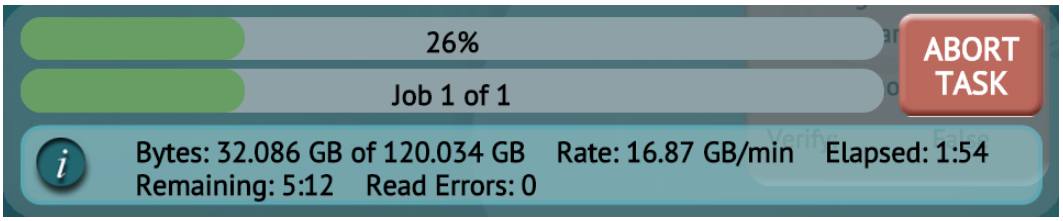


The ***More Info*** icon is available to see more information about the image. When selected, a screen will appear showing details on the selected image file.

4.5 Starting the Cloning Operation

Once all the settings and options have been selected or set, tap the ***Start*** icon to begin the Cloning operation. A confirmation screen will appear. Tap the ***Yes*** icon to continue.

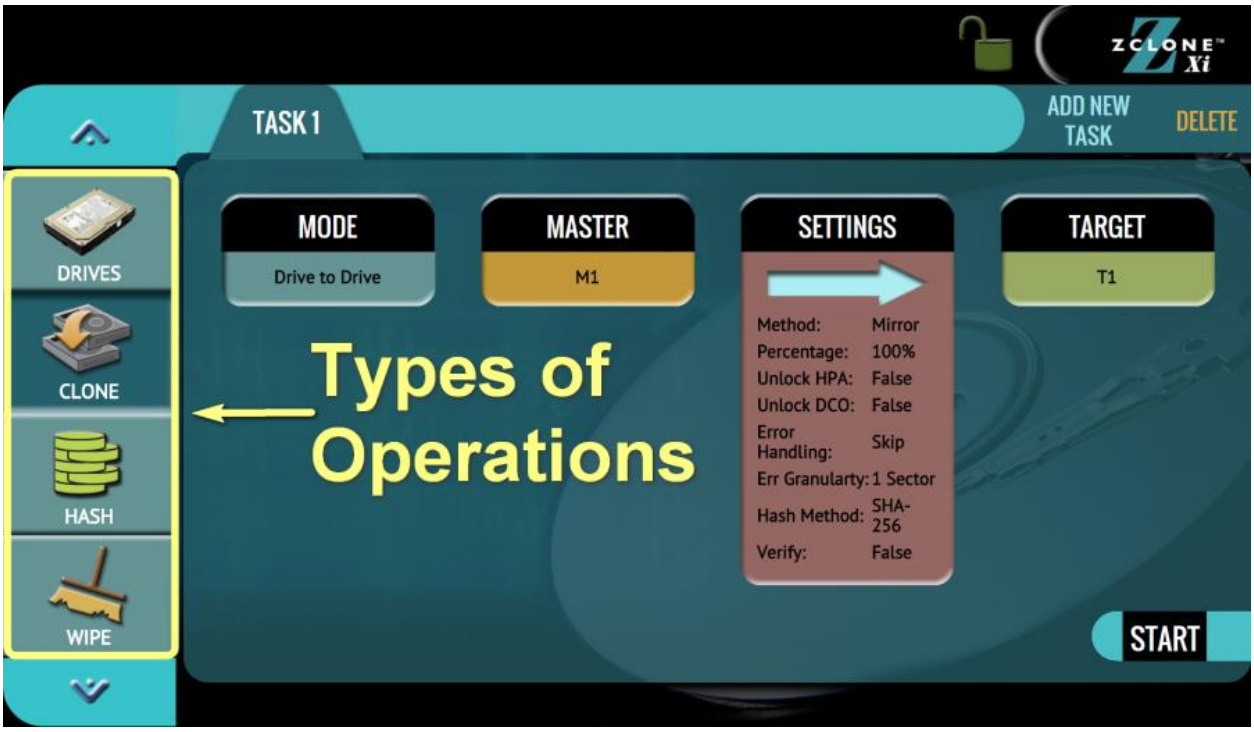
A progress bar will appear at the bottom of the screen showing the bytes processed, the rate (speed), elapsed time, time remaining, and bad sectors (on the Master drive, if any).



When finished, the status will show "COMPLETED". At this point, it is recommended to tap ***Reset Task*** to reset the task, so the drive bays properly reset and not show as being used or assigned for other tasks.

5.0 Types of Operations

There are twelve (12) types of operation available. The left side of the screen shows the different operation types that can be set. Detailed information on all the different operations and their screens can be found in this section.



1. **DRIVES –** This screen shows the status of all drive bays. Each drive bay will be listed and will show any drive connected.
2. **CLONE –** There are three cloning modes available. Drives can be cloned using ***Mirror*** (bit-for-bit copy) or ***Clever*** (copies only data areas, skips blank sectors, and partitions can be resized).
    a. **Drive to Drive –** Performs a bit-for-bit copy of the Master producing an exact duplicate of the Master drive.
    b. **Image to Drive –** Restores an image created by the ZXi to one or more Target drives.
    c. **Drive to Image –** Creates a Logicube ZXi image file to a Target or Repository. This image file can be restored to drives using the Image to Drive mode.

    Details on the different screens found in the Imaging operation can be found in ***Chapter 4: Cloning*.**

3. **HASH –** Perform a SHA1, SHA-256, or MD5 hash of a drive. This can also verify the hash of the drive by entering an "expected value" for the hash.
4. **WIPE / FORMAT –** This type of operation is used to erase, wipe, and/or format drives. The following wipe or format methods are available:
    - **Secure Erase –** Sends a command to the drive instructing it to perform a secure erase based on the drive manufacturer's specifications.
    - **Wipe Patterns –** Allows the user to set a specific pattern to use for wiping the drive. The number of passes is customizable (up to 7 passes) along with the type of data written for each pass. In addition, a 7-pass DoD wipe can be set.
    - **Format –** Formats the Target using any of the following file systems:
        - EXT4
        - NTFS
5. **TASK MACRO –** Set up to nine (9) different tasks to perform sequentially (one after another). For example, a macro can be set to perform these tasks in order: Wipe then Clone.
6. **LOGS –** Display logs of each task that has been performed on the unit.
7. **STATISTICS –** This will display tabs that include:
    - **About** – This screen will show information about the unit including the current software installed.
    - ***Adv. Drive Statistics* –** Displays S.M.A.R.T. information taken directly from what the drive is reporting.
    - ***I/O Ports* –** Displays a diagram of the input and output ports located in the back of the unit.
    - **Options –** Displays which optional software is available and what is installed.
    - **Network Interface Stats –** Displays the Network Interface statistics (Receive and Transfer bytes, packets, drops, and errors, and the link status).
8. **MANAGE REPOSITORIES –** Allows the user to add a network location as a repository that can be used as a Target for cloning. This will display tabs that include:
    - **Add/Remove –** Allows the user to add, remove, or edit networked repositories.
    - **iSCSI –** Allows the user to set ISCSI protocol settings.
9. **SYSTEM SETTINGS –** This mode allows changes to the system settings which include the following:
    - **Profiles –** Allows the user to create, save, apply, or delete user profiles.
    - **Passwords –** Allows the user to set passwords to lock the unit from any access or configuration changes.
    - **Language/Time Zone –** Sets the language on the menu and change the system's Time Zone.
    - **Bay Roles –** Allows the user to configure each bay to be a Master, Target, or both Master and Target.

10. **NETWORK SETTINGS –** Allows the editing of various network configurations. The following tabs are available:
    - **Services –** Set certain network services to be enabled or disabled.
    - **Interfaces –** Edit TCP/IP configuration.
    - **HTTP Proxy –** Set proxy settings (if required by the user's network).
11. **SOFTWARE UPDATES –** Perform software and firmware updates on the unit. Software can be updated over an internet connection (from network) or from a USB flash drive. Two tabs are available:
    - **Software Updates –** This is the screen where users can check for new software and update or reload the software.
    - **Firmware Update –** Firmware for the unit (if available) can be updated on this screen.
12. **POWER OFF –** Turn the unit off, restart the unit or refresh the Graphical User Interface (GUI) and set a drive timeout, powering down drives when not in use. The following tabs are available:
    - **Power Off –** The unit can be restarted or turned off on this screen. This can be useful when using the web interface. The User Interface can also be refreshed in this screen.
    - **Drive Power –** Drives can be powered down automatically when not in use.

5.1 Drives

This screen shows the status of all drive bays. Each drive bay will be listed whether there is a drive connected or not.

If there is a drive connected, the model of the drive will appear in the Drive Information column and will have a ✔ symbol in the Drive Connected column. If no drive is detected, the bay will have a ✗ symbol.

Additional drive information can be viewed by tapping the ⓘ more info icon.

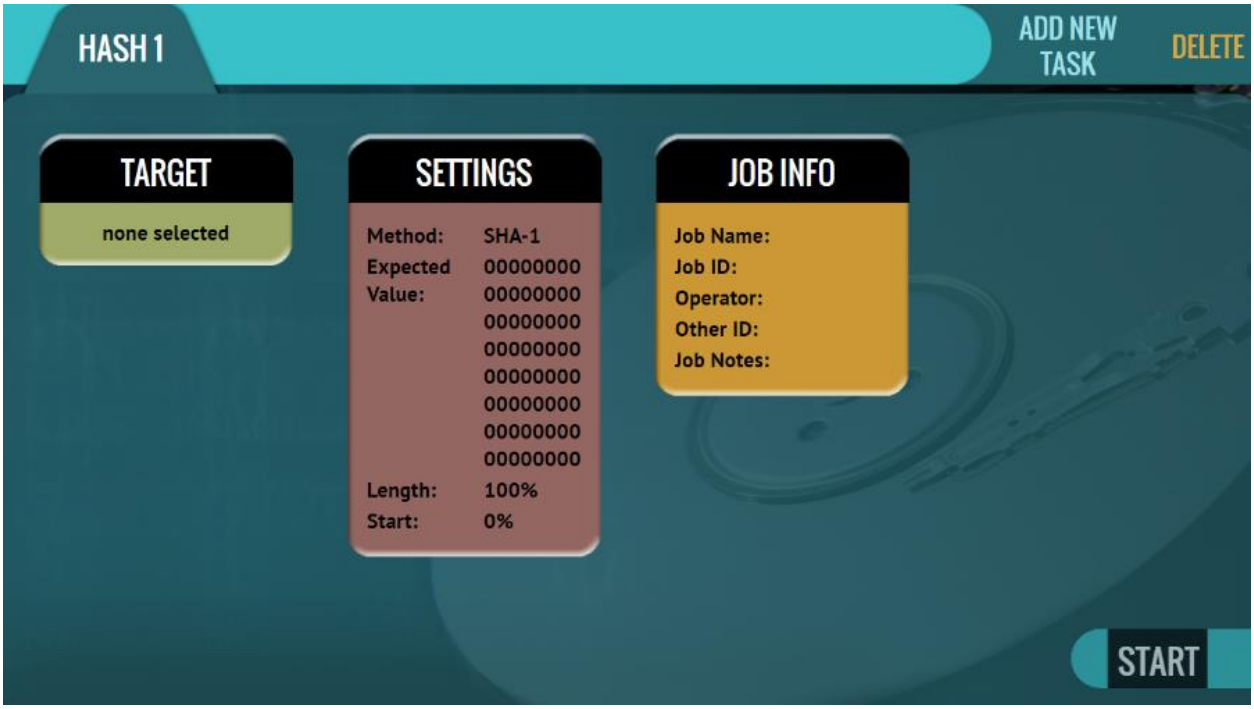
5.2 Clone

This type of operation allows the cloning of a master to one or more Targets. There are three different imaging modes and several settings to choose from. These selections should be performed in order from left to right.

In-depth details on the different screens found in the Clone operation can be found in ***Chapter 4: Cloning***.

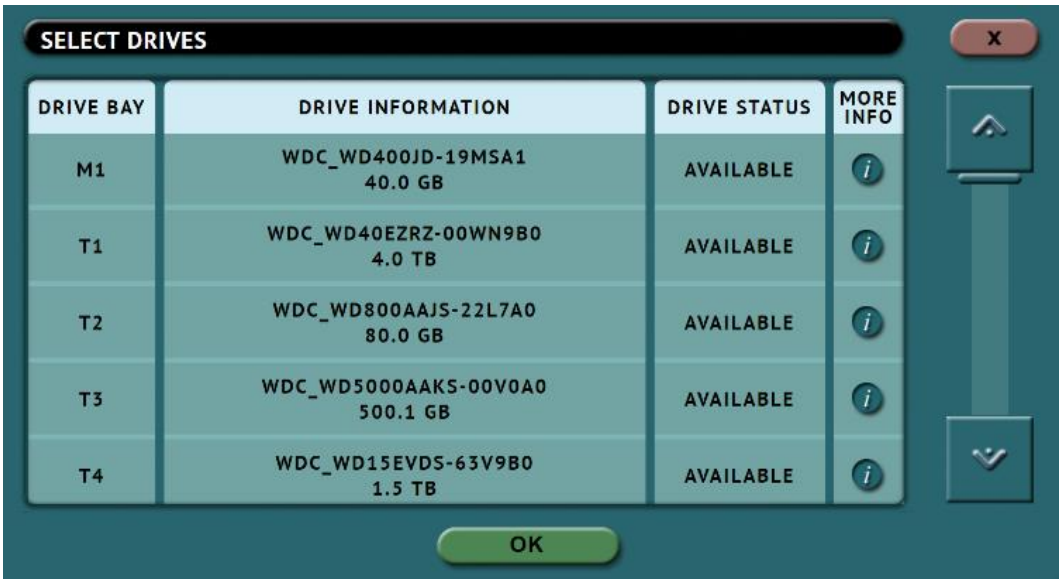
5.3 Hash

This type of operation can be performed to any drive connected to the unit to hash using one of the following algorithms: ***SHA-1***, ***SHA-256***, or ***MD5***



5.3.1 Target

Tap this icon to select which drive(s) will be hashed. The unit will show all connected Master and Target drives. Tap the drive(s) to be hashed then tap ***OK***.



5.3.2 Settings

Tap this icon to choose a drive to adjust the hash settings.

5.3.2.1 Hash Settings

Tap the ***Hash Values*** icon to set the hash method (SHA-1, SHA-256, or MD5) and to set the expected hash value (if desired). Setting the expected hash value instructs the unit to hash the drive then verify the hash with the expected value set.

Each hash task is Logical Block Address (LBA) based and will hash drives based on the number of LBAs. If multiple drives are selected to be hashed, the unit will hash up to the LBA value of the smallest capacity drive.

5.3.2.1.1 Hash Method

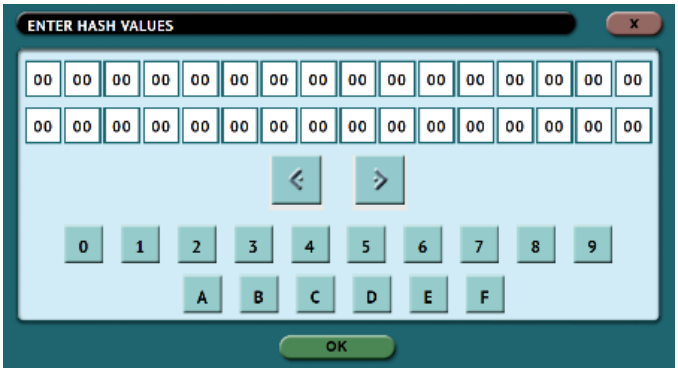
Select one of the following hash methods:

- **SHA-1**
- **SHA-256**
- **MD5**

5.3.2.1.2 Hash Values

By default, this value will have 0s (zeros). If this is not changed, or no value is entered, this will instruct the unit to hash the drive using the selected algorithm in the previous step. The result of the hash will be used as the expected value. If a value is entered, the unit will hash the selected drive and verify hash with the value entered/edited.

To set the expected value, tap the ***edit*** icon. The on-screen keyboard will appear, and the expected hash value can be set.



There is a ***Clear All*** button to easily clear all values.

5.3.2.1.3 LBA

The LBA icon will bring up the LBA settings screen. The user can adjust the percentage or the number of blocks of the drive to hash and where to start the hash. By default, the length is set to 100% (whole drive) and the starting percentage is set to 0% (start of the drive).

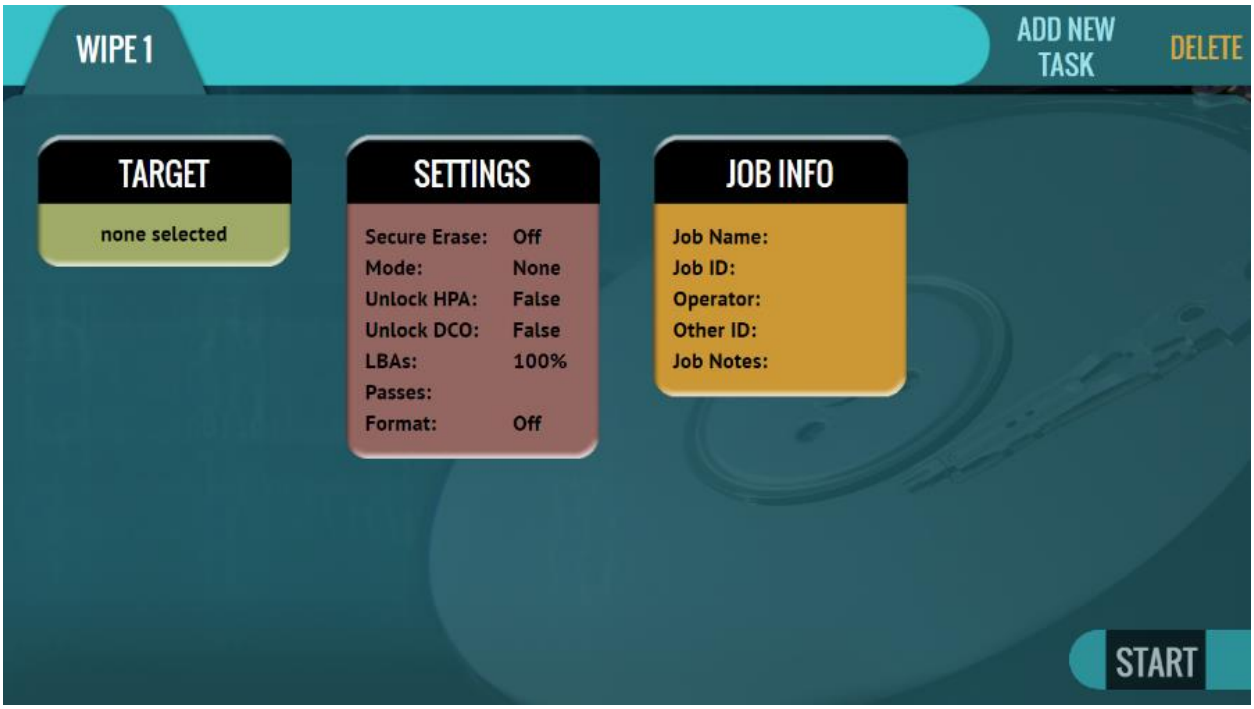
5.3.3 Job Info

The Job Info setting allows users to enter some information about the job. Job Info is not required to start a Clone, Hash, or Wipe/Format operation.

Information entered here will appear in the logs. More information on the Job Info screen can be found in ***Section 4.3.1***.

5.4 Wipe / Format

This type of operation allows the user to erase, wipe, and/or format one or more Target drives. The following wipe or format methods are available: Secure Erase, Wipe Patterns, and Format.



- **Secure Erase –** Sends a command to the drive instructing it to perform a secure erase based on the drive manufacturer's specifications for the secure erase command.
- **Wipe Patterns –** Allows the user to set a specific pattern to use for wiping the drive. The number of passes is customizable (up to 7 passes) along with the type of data written for each pass. In addition, a 7-pass DoD wipe can be set with pre-selected pass values.
- **Format –** Formats the Target drive with one of the following user selectable file systems (with or without encryption): EXT4 or NTFS.

The following selections are available when performing a wipe:

- Target
- Settings
- Case Info

5.4.1 Target

Tap this icon to choose a drive to erase, wipe, and/or format.

A screen will appear, allowing the selection of one or more targets. Tap the drive(s) to be erased, wiped, and/or formatted then tap ***OK***.

5.4.2 Settings

Tap this icon to choose a drive to set the wipe settings. The Wipe Settings screen will appear.

The following wipe or format methods are available: ***Secure Erase***, ***Wipe Patterns***, and ***Format***.

Each setting will be performed sequentially. For example, if Secure Erase is set to ON, a Wipe Pattern mode is specified, and Format is set to ON, the unit will first secure erase the drive, then wipe the drive according to the mode specified, then format the drive.

5.4.2.1 Secure Erase

Choose ***ON*** to Secure Erase the selected Target drive(s). Most drives support this function. Secure Erase will send a command to the drive instructing it to reset itself to the specifications the drive manufacturer has set.

Secure erase will not work on drives connected through the USB ports.

For SAS (Serial Attached SCSI) drives, Secure Erase sends a 'Format' command. For SATA (Serial-ATA) drives, Secure Erase sends a 'Security Erase Unit' command. For SATA drives that support 'Enhanced Security Erase Unit' commands, the enhanced command will be sent. For questions on how each drive supports these features, or what the drive will do with these commands, please contact the drive manufacturer.

5.4.2.2 Wipe Patterns

This setting allows the user to set a specific wipe pattern or patterns to use for wiping the drive. The number of passes is customizable (up to 7 passes) along with the type of data written for each pass. In addition, a 7-pass DoD wipe can be set with pre-selected pass values.

There are 4 selections when setting a wipe pattern:

- MODE
- HPA/DCO
- LBAS
- PASSES

It is recommended to use the same capacity drives per task. When smaller capacity drives are wiped together with larger capacity drives, the smaller drives will finish first. However, the ports will not be available until the entire task is finished.

5.4.2.2.1 Mode

Selecting ***Mode*** will open the Wipe Mode screen showing the following options:

- **NONE –** Choosing this will instruct the unit not to perform a wipe using Wipe Mode.
- **DOD –** Choosing this will instruct the unit to perform a 7-pass wipe conforming to the DoD 5220.22-M standards.
- **CUSTOM –** Choosing this will allow the user to specify how many wipe passes will be performed and what values each pass will be written on each of the passes selected.

5.4.2.2.2 HPA/DCO

The ***HPA/DCO*** button will open the HPA/DCO option for wiping. If the drive to be wiped has HPA and/or DCO that needs to be wiped, select ***Yes*** for the corresponding option.

5.4.2.2.3 LBA

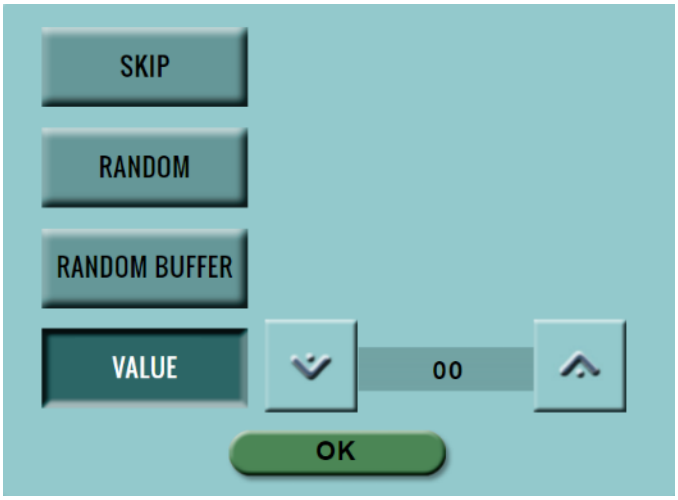
By default, this is set to 100% which will wipe all Logical Block Addresses (LBAs) and will wipe the entire drive (100%). The LBA count can be adjusted by tapping the ***edit*** icon.

5.4.2.2.4 PASSES

This Wipe Setting will change depending on the Wipe Pattern ***Mode*** selected.

- If ***None*** was selected, this is not selectable.
- If ***DoD*** was selected, all 7 passes will be pre-filled. Users can edit the pass values by tapping the ***edit*** icon. The default values are: 00, 01, 00, FF, F6, 00, XX (random).
- If ***Custom*** was selected, one pass will be pre-filled with a random value. Users can edit the pass values if desired by tapping the ***edit*** icon. The default value for a custom pass is 00.

Editing one or more of the passes in DOD or CUSTOM mode will bring up this screen:



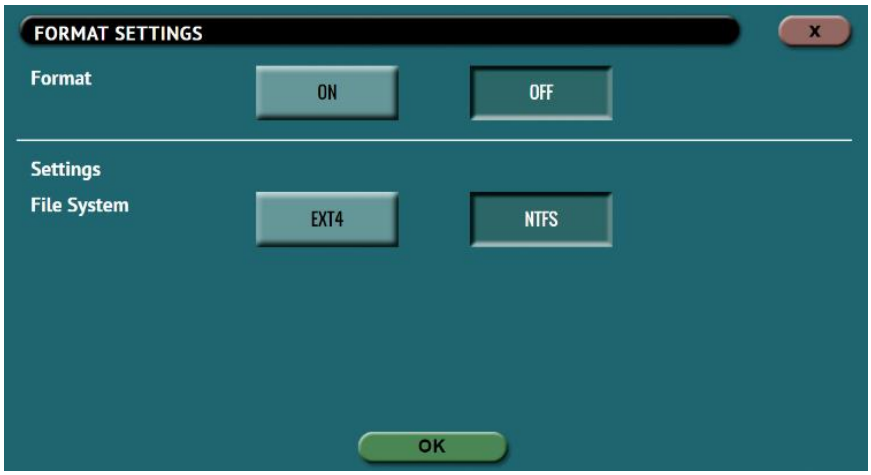
- **SKIP –** Instructs the unit to skip the pass.
- **RANDOM –** Writes one random hexadecimal value (from 00 - FF) to all the selected Logical Block Addresses.

- **RANDOM BUFFER –** The unit will create an 8MB block filled with random values (each byte in the 8MB block will contain a random value). The 8MB block will be written repeatedly to fill the entire drive.
- **VALUE –** Instructs the unit to use the specified hexadecimal value to be written for the pass. The values can range anywhere from 00 to FF.

5.4.2.3 Format

Formats the Target using the EXT4 or NTFS file system.

These settings are available:



- **Format –** When set to ***ON***, the Target drive will be formatted. The drive will be formatted with the user's choice of file system (EXT4 or NTFS). When set to ***OFF***, the Target drive will not be formatted.
- **File System –** Select the file system to be used to format the Target drive. Users can select EXT4 or NTFS.

5.4.3 Job Info

The Job Info setting allows users to enter some information about the job. Job Info is not required to start a Clone, Hash, or Wipe/Format operation.

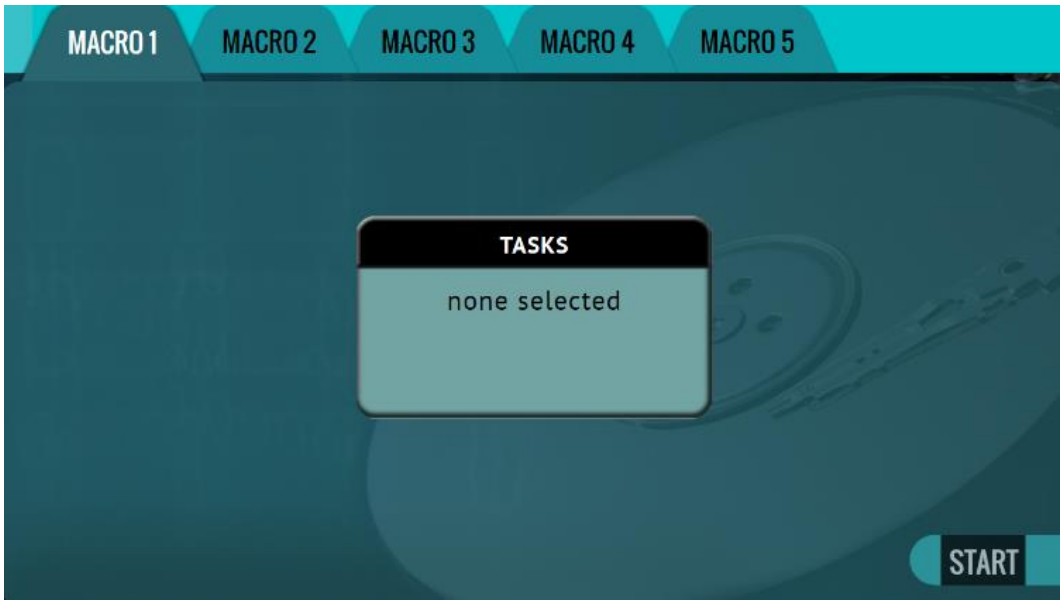
Information entered here will appear in the logs. More information on the Job Info screen can be found in ***Section 4.3.1***.

5.5 Task Macro

This operation allows up to five (5) macros that can be set. Each macro can run up to nine (9) tasks sequentially (one after another). For example, a macro can be set to perform these tasks in order: Wipe then Clone.

Each of the five macros can be set by tapping on the Macro number on the top of the screen. Each task or operation must be set up before setting up the macro. For example, to set up a Task Macro that will perform a wipe, then clone, users must first set up both the wipe and clone tasks. Once the wipe (for example, Wipe 1) and clone (for example, Clone 1) has been set up, the Task Macro can be set.

5.5.1 Tasks



Tapping this icon allows the user to set specific tasks for each macro.

Tap ***Operation 1*** to set the first operation in the macro. The following screen will appear allowing the user to choose the task. Tap the ***OK*** icon to continue.

Example: Setting up a Macro for a Wipe using Secure Erase then perform a Drive to Drive Clone

To set a macro to perform a Wipe using Secure Erase on T1, immediately followed by performing a Drive to Drive Clone from M1 to the newly wiped (secure erased) T1, the Wipe and Imaging Tasks first need to be set up.

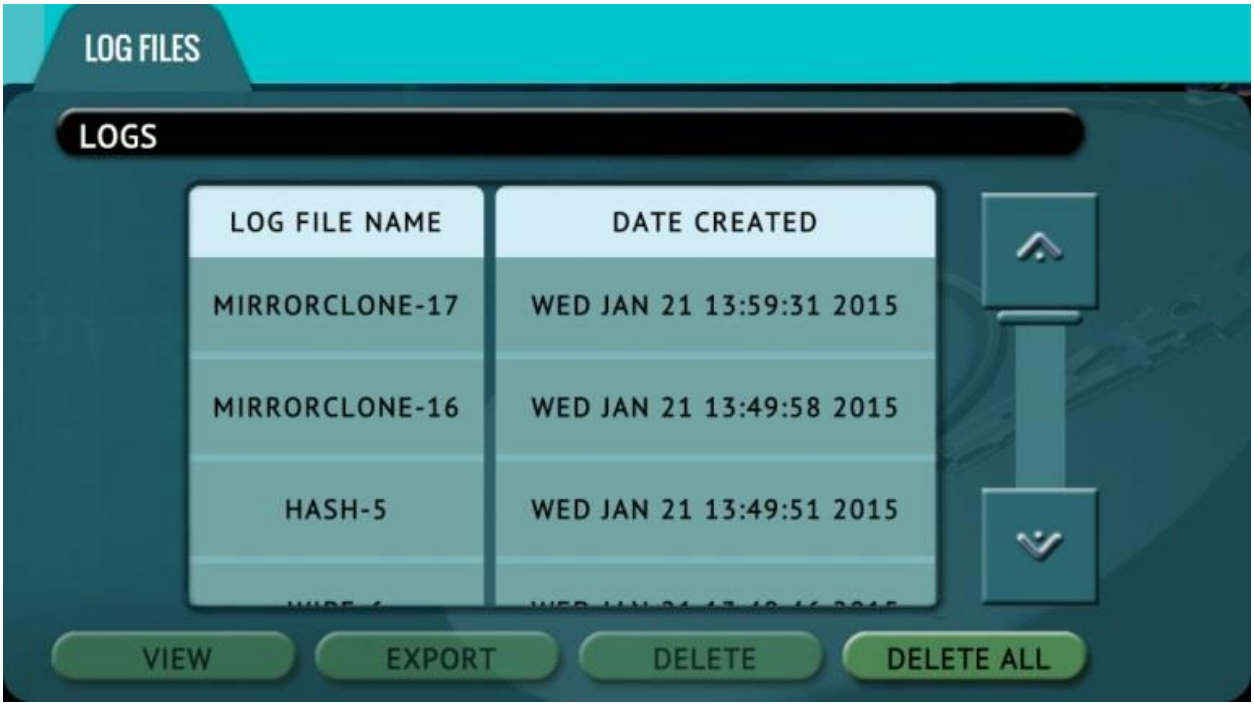
1. First, set the Wipe task. Select T1 as the Target and change the setting to perform a Secure Erase (Wipe Patterns set to off). Do not start this task.
2. Next, set the Clone task. Select Drive to Drive as the Mode. Select M1 as the Master. Change the settings as needed. Select T1 as the Target. Do not start this task.
3. Choose ***Task Macro*** from the list of operations on the left side.

4. Tap the ***Tasks*** icon to select the different tasks for the macro.
5. Tap the field next to ***Operation 1*** to set the first operation. Since the first task to be run is the Wipe task, select ***Wipe 1*** then tap ***OK***.
6. Tap the field next to ***Operation 2*** to set the second operation. Since the second task to be run is the Drive to Drive Imaging task, select ***Clone 1*** then tap ***OK***.
7. The screen should now show ***Wipe 1, Clone 1*** as the Tasks for Macro 1.
8. Tap the ***Start*** icon to begin the macro. The macro will run the Wipe 1 task first, then Clone 1.

5.6 Logs

Logs are kept from all imaging, hash, and wipe operations. Logs can be viewed directly on the unit or from a computer's browser (if connected to a network).

For wipe operations, logs are kept if secure erase or wipe patterns is selected. If the drive is just formatted (without secure erase or wipe patterns), no log will be created.



In addition to viewing, the logs can be exported to an external USB location such as a USB flash drive. Logs are exported in PDF, HTML and XML format.

Log files can be deleted one at a time or all at once.

The log file may contain several sections, depending on what settings and options were chosen during the operation, including:

- Information on the unit and its settings
- Job info (if entered)

- Master and Target hashes

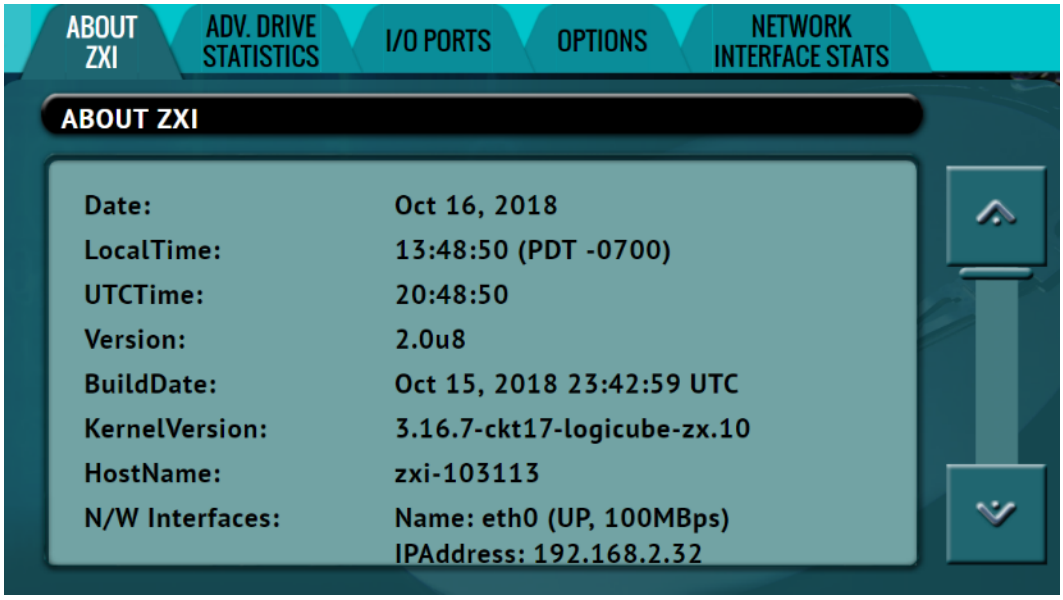
> See ***Section 3.6.1*** for instructions on how to export the log files.
>
> See ***Section 3.6.2*** for instructions on how to delete the log files.
>
> See ***Section 3.6.3*** for instructions on how to access the logs over a network.

5.7 Statistics

This screen shows several different tabs of information which include: ***About***, ***Adv. Drive Statistics***, ***I/O Ports***, ***Options***, and ***Network Interface Stats***.

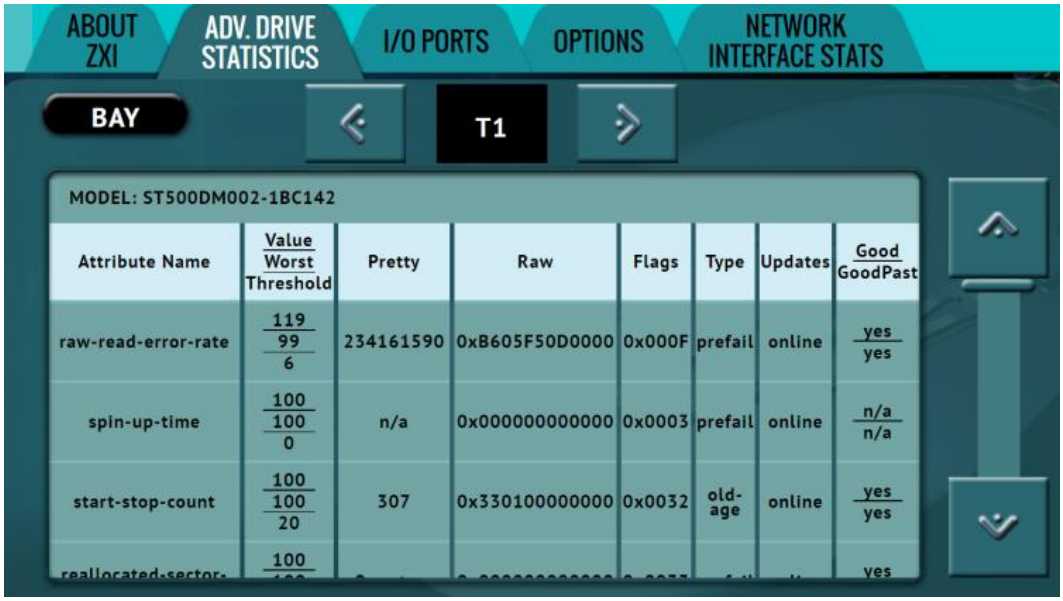
5.7.1 About Screen

The ***About*** screen will show information about the unit including the current software installed.



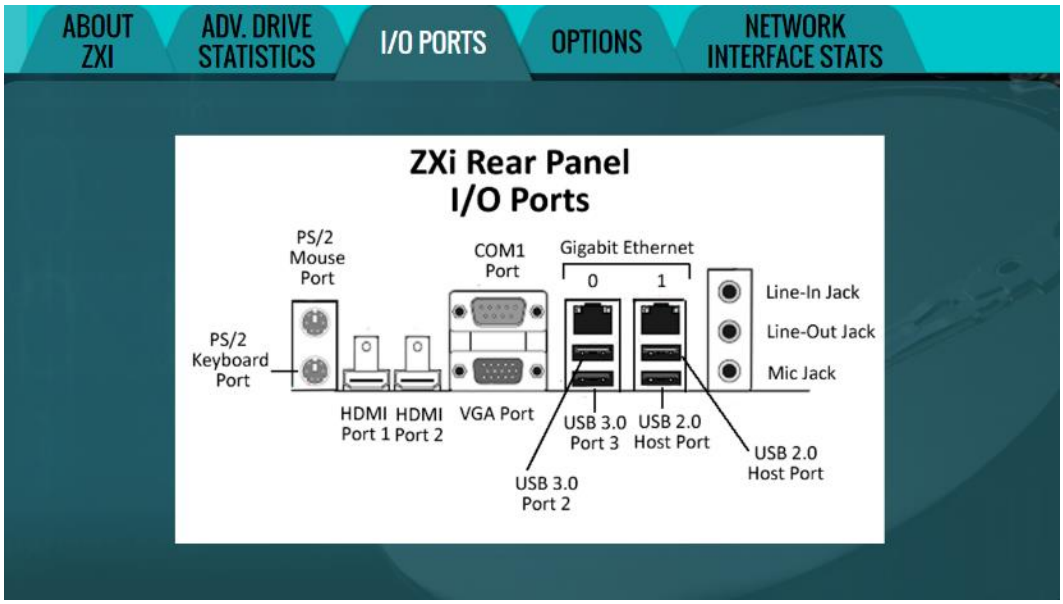
5.7.2 Adv. Drive Statistics

The ***Adv. Drive Statistics*** tab shows S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology) information taken directly from what the drive is reporting. Navigate between drives by using the left and right scroll arrows. The up and down scroll arrows scroll through the different information. The information shown is the raw value tracked by the drive and is not translated.



5.7.3 I/O Ports

The ***I/O Ports*** tab displays a diagram of the input and output ports located in the back of the ZXi.

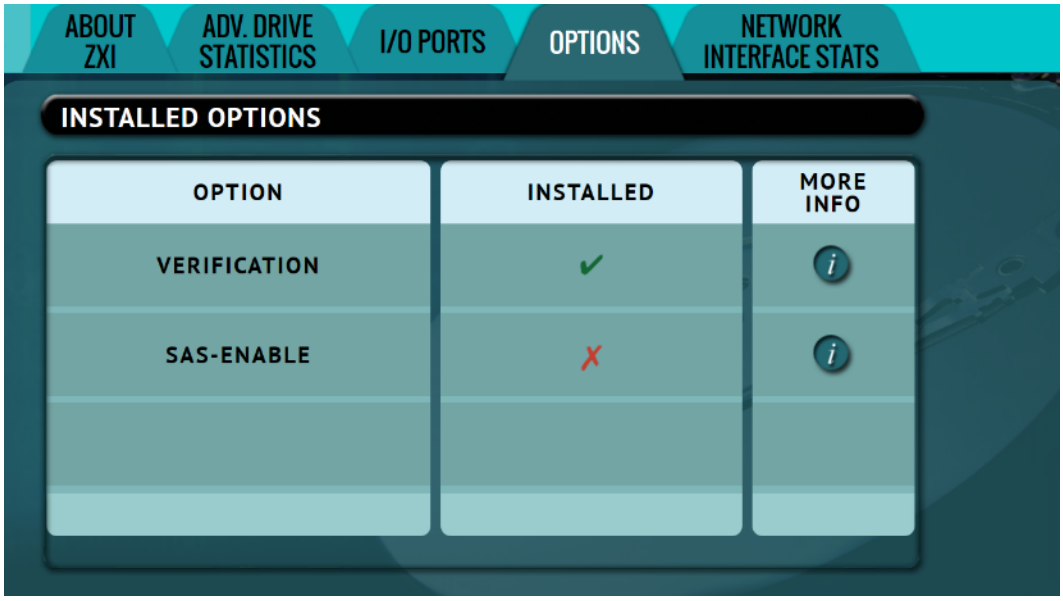


5.7.4 Options

The ***Options*** tab displays available software options and which options are installed on the unit.

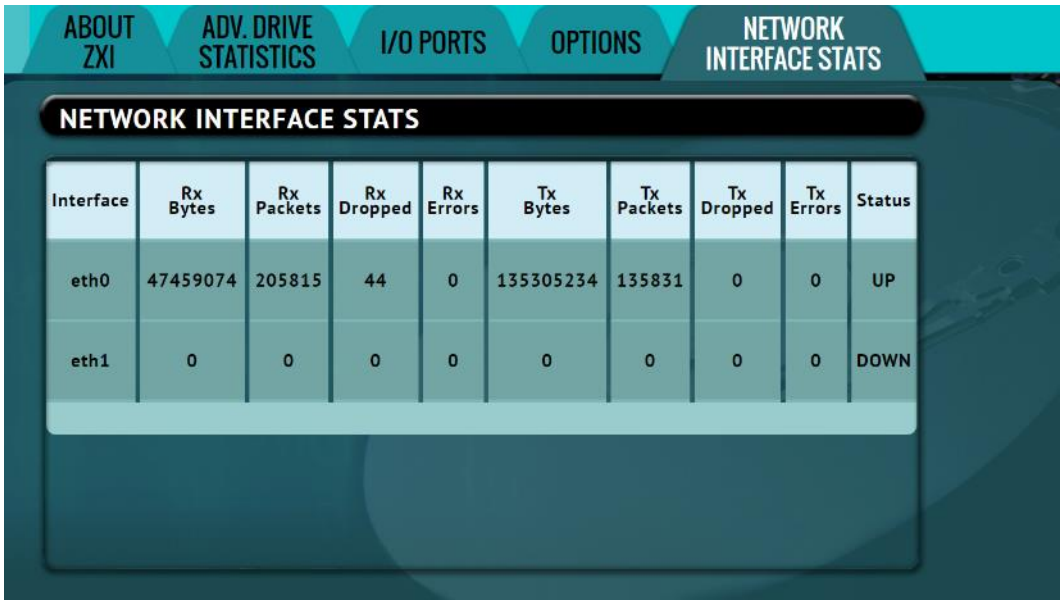
To purchase an option, please contact Logicube Sales: sales@logicube.com.

If an option has been purchased but is not showing as installed, please contact Logicube Technical Support: support@logicube.com.



5.7.5 Network Interface Stats

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



5.8 Manage Repositories

Networked repositories can be added using this operation.

When ***Manage Repositories*** is selected, the following tabs are available at the top of the screen:

- Add/Remove – Adds a repository using using the SMB, CIFS, or NFS protocol.
- iSCSI – Adds a repository using the iSCSI (Internet Small Computer System Interface) protocol.

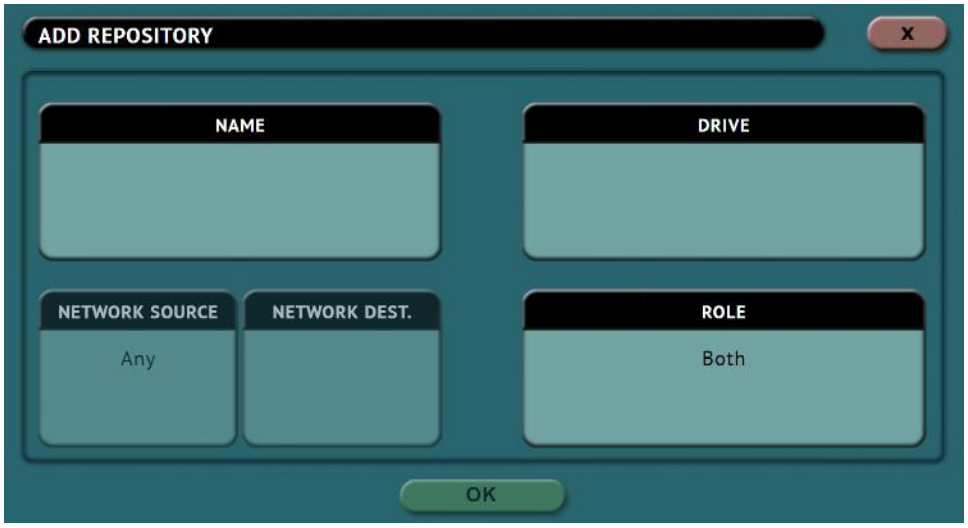
Networks are configured differently and may require the assistance of a Network or Systems Administrator to ensure proper configuration for sharing.

5.8.1 Add/Remove

A list of repositories will be shown. The user has the option of adding or deleting a repository. This will include all drives attached to bays that are set to Target (or Master/Target) and any networked repository.

If a repository location shows ***(NOT MOUNTED)***, it is because the drive attached is not formatted by the unit or the unit cannot connect to the shared network resource.

Tap ***Add Repository*** to add a repository. The Add Repository window will appear.



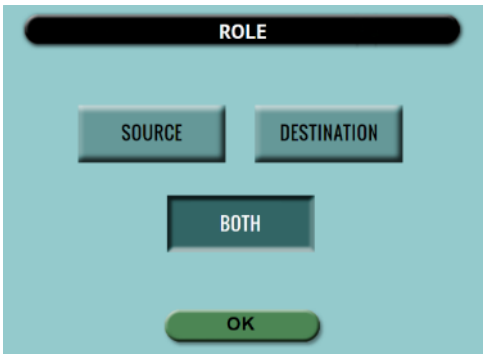
Tap ***Name*** to set the name of the repository. Tap the ***OK*** icon when finished.

Tap ***Drive*** to select ***network share*** to set as a repository. Tap the ***OK*** icon when finished.

Tap ***Network Settings*** to enter the network settings. See the example below. Tap the ***OK*** icon when finished.

For the ***Path***, make sure the forward slash (/) is used and not the backslash symbol (\ ).

OPTIONAL: Tap ***Role*** to select the role for this repository. By default, it is set to "Both" Source (Master) and Destination (Target). Tap ***OK*** when finished.



To delete a repository, tap the ***delete*** icon. A confirmation screen will appear. Tap ***Yes*** to permanently delete the repository from the list.

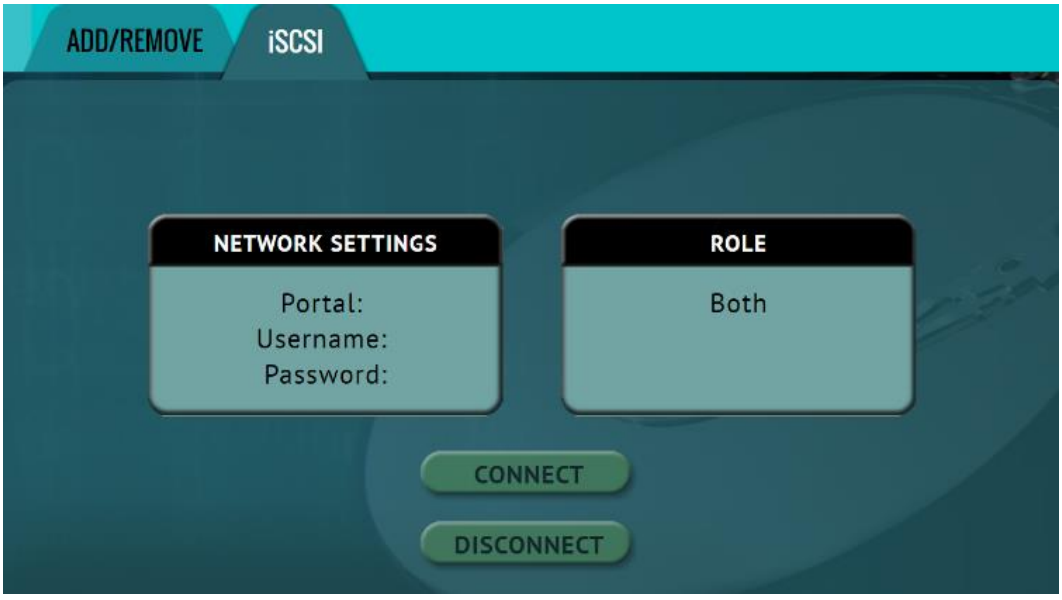
In order for a repository to remain configured when the unit is turned off, the changes must be saved and loaded to a profile. Details on profiles can be found in ***Section 5.9.1***.

5.8.2 iSCSI

This screen allows a user to add a repository using the iSCSI protocol.

To add a repository using the iSCSI protocol, an iSCSI Target must be setup on the remote system. Since networks are configured differently, a Systems Administrator or Network Administrator may be needed to set up the iSCSI protocol.

Once the iSCSI Target has been setup, click ***Settings***.



Input the iSCSI target portal, username and password. Tap the ***OK*** icon when finished.

Tap ***Role*** and input the role for the iSCSI server then tap ***OK***.

5.9 System Settings

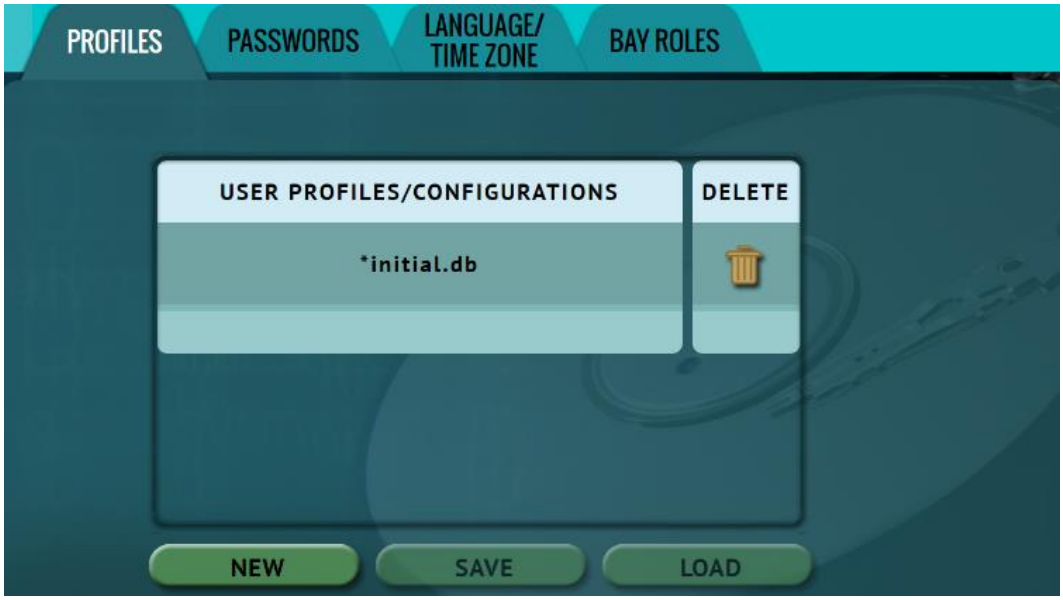
System Settings screen allows users to configure several different settings which include: ***Profiles***, ***Passwords***, ***Language/Time Zone***, ***Bay Roles***.

5.9.1 Profiles

Do not highlight and save over the INITIAL.DB profile. This is the default profile of the unit and is used to reset the unit to the factory default settings.

This screen shows all user profiles. The following selections are available in this screen:

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



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

The Profiles tab allows users to create, save, and load different profiles with different configurations. When a profile is loaded using the ***Load*** icon, the unit will load that profile during its boot process.

For example, if the user wants the unit to always boot up with the default Clone mode of ***Image to Drive***:

1. Turn the unit off then back on. This will reset all settings to the loaded profile. This is an important step to help ensure only the changes desired will be the changes saved.

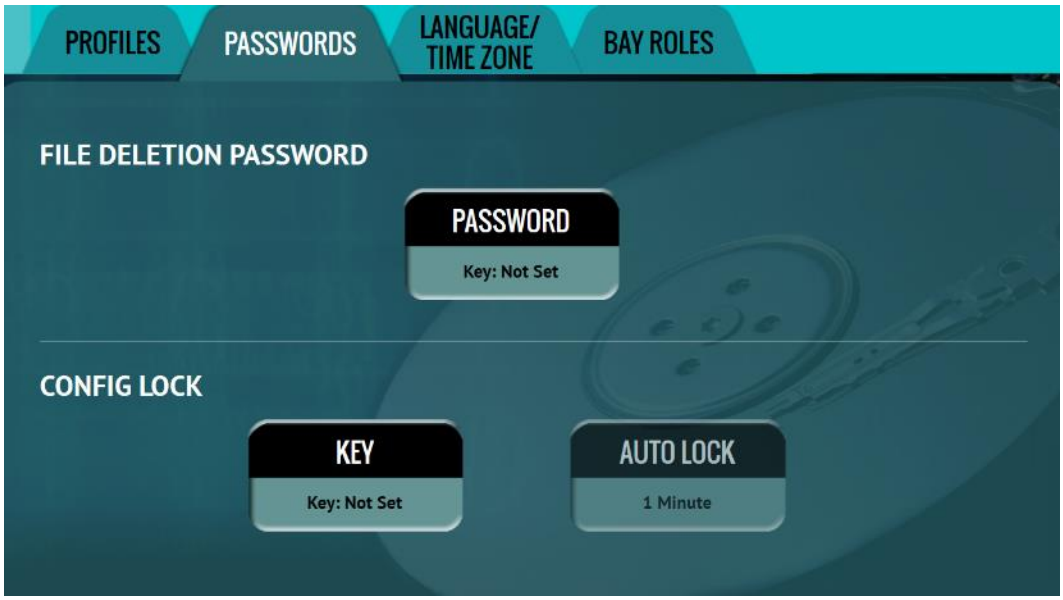
2. Go to the ***Clone*** screen and set the ***Mode*** to 'Image to Drive'.
3. In the ***System Settings***, go to ***Profiles*** and tap the ***New*** icon.
4. Type a name for this profile. For example, ImageToDrive and tap the ***OK*** icon. The profile name should appear on the screen.
5. Tap the newly saved profile and tap ***Save***. A confirmation screen will appear.
6. Tap the ***Yes*** icon to save the profile.
7. Make sure the profile to be loaded (during the boot process) is highlighted (for example ImageToDrive.DB) and tap the ***Load*** icon. A confirmation screen will appear.
8. The next time the unit is turned on it will load ImageToDrive profile.

To delete a profile, highlight the profile to be deleted then tap the delete icon. A confirmation screen will appear. Tap the ***Yes*** icon to delete the selected profile.

When loading a profile, the it may take several seconds to completely load the different profile.

5.9.2 Passwords

The following are keys or passwords that can be set or changed.



- **Log File Deletion Password –** A password can be set as an extra layer of protection when deleting log files. If this password is set, ZXi will prompt for the password before any log files can be deleted.
- **Config Lock –** The ZXi 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, if the Config Lock key is set, and the IMAGE task is configured for Drive to Drive cloning, the user will be unable to change the mode to Drive to Image but can start the Drive to Drive task.

Tap ***Password*** or ***Key*** to enter a log file deletion password or a config lock key. The following screen will appear.

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

Tap 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 ***Log File Deletion***, ***Local HTTP***, ***Remote HTTP***, and ***Config Lock*** can be saved into a user profile and loaded each time the unit is turned on. See ***Section 5.9.1*** for more information on saving and loading a user profile.

Remember the Config Lock Key! If the unit 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 5.9.2.1.2*** for more information.

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

5.9.2.1 Config Lock Notes

A shortcut (and indicator) to the ***config lock*** can always be seen on the top-right of the screen next to the logo.

 or 

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

- **Drives –** Since there are no settings for this screen, it is not affected by the Config Lock.
- **Clone –** A clone task can be started, but no settings can be changed. Additionally, no new task can be added, and no task can be deleted without the Config Lock unlock key.
- **Hash –** A hash task can be started, but no settings can be changed. Additionally, no new task can be added, and no task can be deleted without the Config Lock unlock key.

- **Wipe / Format –** A wipe / format task can be started, but no settings can be changed. Additionally, no new task can be added, and no task can be deleted without the Config Lock unlock key.
- **Task Macro –** A task macro can be started, but no settings can be changed. Additionally, no new macro can be set or edited without the Config Lock unlock key.
- **Logs –** Logs are not affected by Config Lock.
- **Statistics –** Since there are no settings or configurations for this operation, it is not affected by Config Lock.
- **Manage Repositories –** A managed repository cannot be added, edited, or deleted without the Config Lock unlock key.
- **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 unit can still be turned off without the unlock key by using the power button located on the front of the unit.

5.9.2.2 Forgotten Password or Config Lock Key

If the Log File Deletion password or Config Lock key is forgotten, the ZXi will need to be reset using the Command Line Interface (CLI). See ***Section 7.2*** for more information on how to connect to the ZXi 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 unit 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 profile being loaded each time the unit is turned on.

```
it@zxi-103113(command-config)> db list
Number of DB's: 2
0: *lock.db
1: initial.db
```

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 unit off using the power button, then close the Telnet/SSH application.
8. Turn the unit on. When the unit boots up, it will load the default profile (INITIAL.DB).

5.9.3 Language/Time Zone

The menu system's language can be changed. The available languages are English, Chinese (**中文**), Korean (한국어), and Japanese (日本語).

This screen also allows the time zone to be set.

5.9.3.1 Language

To change the language displayed. As soon as the selection is made, the screen (or the computer's Internet browser) will automatically refresh and display the selected language.

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

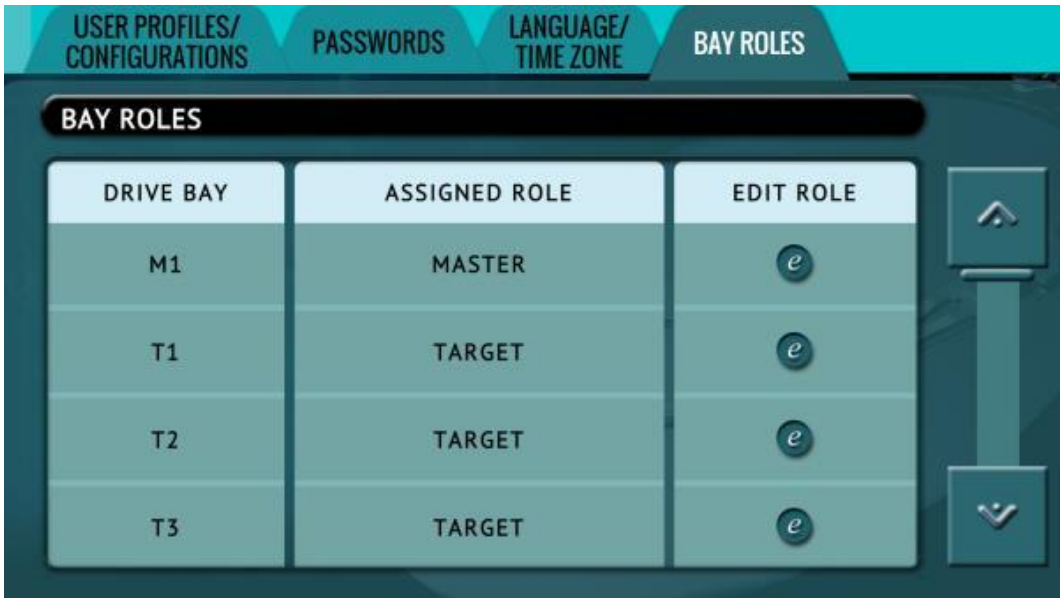
5.9.3.2 Time Zone

The unit utilizes NTP (Network Time Protocol). Each time it 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 unit also has a time zone setting. Tap ***Time Zone*** to select the time zone region. Tap the ***OK*** icon to continue.

After selecting the region, select the desired time zone. Tap the ***OK*** icon to set the time zone.

5.9.4 Bay Roles



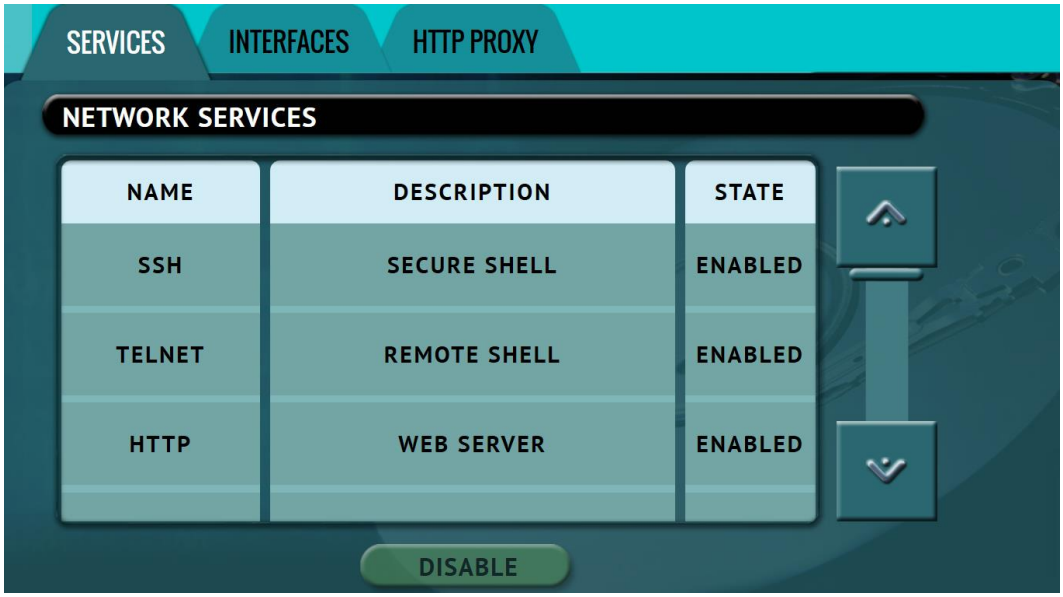
Each of the drive bays can be configured as a Master, Target, or both Master/Target. Tap a drive bay, then tap the ***Edit Role*** icon to assign the specific drive bay

After changing the bay role, it is highly recommended to save the settings into a profile, load that profile, then reboot. See ***Section 5.9.1*** for more information on saving and loading a profile.

5.10 Network Settings

The Network settings screen has the following tabs: ***Services***, ***Interfaces*** and ***HTTP Proxy***. The ***Services*** tab allows certain services to be enabled or disabled. 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.

5.10.1 Services



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

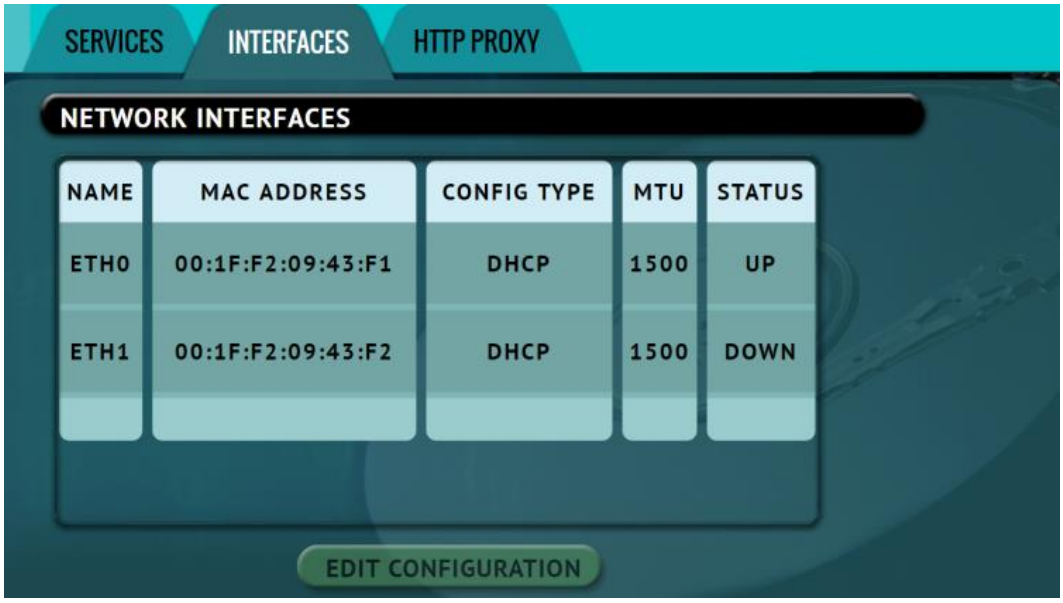
- **SSH –** Disabling this will block Secure Shell (SSH) traffic.
- **Telnet –** Disabling this will block Telnet traffic.
- **HTTP –** Disabling this will block web browser connections to the unit.
- **CIFS/NETBIOS –** Disabling this will block any CIFS or NETBIOS connection to the unit (for example, 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 unit.

  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 unit through a web browser over the network.

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

5.10.2 Interfaces

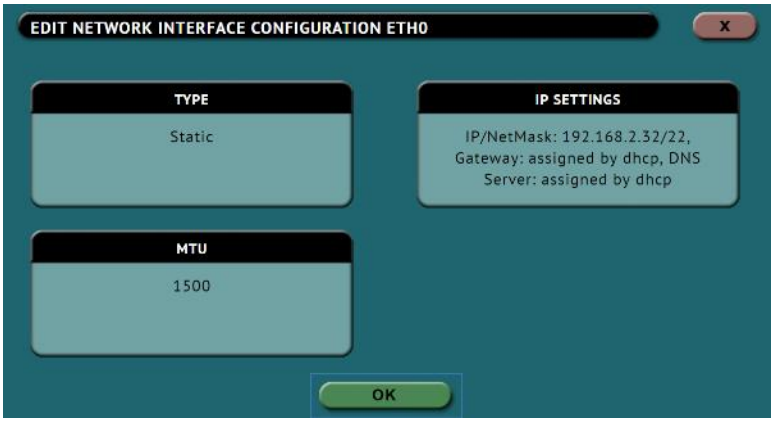
The Interfaces tab displays the network interface information (MAC Address, Configuration type (DHCP or Static), MTU, and the status. To edit the network interface configuration, tap the Ethernet adapter name then tap the ***Edit Configuration*** button. The configuration screen should appear:



5.10.2.1 Configuring a Static IP Address

DHCP is enabled by default. Some networks do not support DHCP and require a static IP address. The steps below outline how to configure the unit with a static IP address.

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



2. Tap the ***IP SETTINGS*** box to manually set the IP address, NetMask, Gateway, and DNS Server. When finished, tap the ***OK*** icon.

To save the settings so that the unit boots up with the static IP address, see ***Section 5.9.1*** for more information on saving and loading a user profile.

5.10.3 HTTP Proxy

If the network the unit is connected to uses an HTTP proxy server to access the Internet, proxy settings may need to be set for 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.

5.10.3.1 Server

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

5.10.3.2 Username/Password

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

5.11 Software Update

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

For the latest step-by-step instructions on how to update the software, please read the ***ZX Software readme*** file located on the ZXi Support page on the Logicube website at https://www.logicube.com/knowledge/zclonexi.

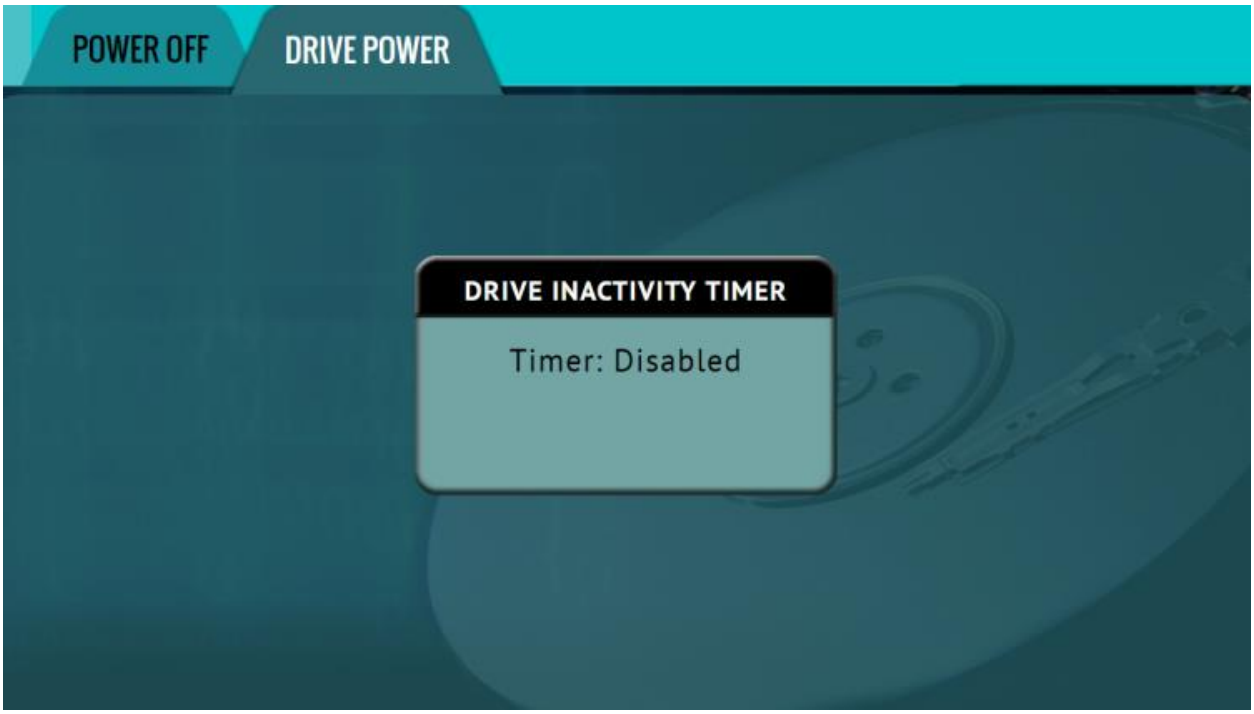
In-depth information on updating the ZXi software can be found in ***Chapter 8: Updating/Loading/Re-loading Software***.

5.12 Power Off

The following tabs are available in the ***Power Off*** screen:

POWER OFF – The unit can be remotely restarted or turned off by going to this tab. Additionally, the Graphical User Interface (GUI) can be refreshed.

DRIVE POWER – Connected, inactive drives can be set to go to standby mode in this tab. The default is set to 0 minutes (Off/Disabled).



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 ZXi's 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/zclonexi.

6.1 Updating/Loading/Re-loading Software Instructions

There are two methods of how to update the ZXi 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 may 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 ZXi'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. From the main menu, locate and tap the ***Software Updates*** icon on the left side.
3. 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. Tap 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. Tap the ***OK*** icon to continue.
    - ***No new version found –*** This message will appear if the unit does not have any internet access. Tap 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.

4. Tap 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 to turn the unit off then back on.
5. Turn the unit off. Wait at least 5 seconds then turn the unit back on.
6. 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 the Logicube 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/zclonexi.
2. Extract the contents of the downloaded zip file to the root of the USB flash drive.
3. Turn the unit on. When the main software screen appears, connect the USB flash drive (that has the extracted software from step 2) to the U1 port (the front USB port).
4. From the main menu on the unit, locate and tap the ***Software Updates*** icon on the left side.
5. 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. Tap 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). Tap the ***OK*** icon to continue and try step 5 again or try updating the software using the "From Network" option.
6. Tap 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 to turn the unit off then back on.
7. Turn the unit off. Wait at least 5 seconds then turn the unit back on.
8. 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 tap the ***Software Updates*** icon.
2. Tap the "Firmware Update" page. One of two screens will appear:
    a. ***FIRMWARE UPGRADE AVAILABE –*** Tap 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." Tap the ***OK*** icon to start the firmware update process.

> When the ***OK*** icon is tapped, the screen may appear to do nothing. Do not keep tapping 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

Two Gigabit Ethernet network connections are available in the back of the unit. Connecting the unit to a network allows remote access from any computer within the same network.

DHCP is enabled by default. See ***Section 5.10.2.1*** for instructions on how to configure a Static IP address.

Zero Configuration Network (Zeroconf) is also available. There are two ways to access the unit:

- Web interface – A graphical interface using an Internet browser where the screens are shown exactly the way they appear on the unit's touch screen.
- Command Line Interface (CLI) – A text only command line interface that can be accessed one of two ways:
    i. Telnet (Using a Telnet client over a network connection)
    ii. SSH (Using a Secure Shell Client over 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 hostname of the unit. Both IP address and hostname can be found by going to the ***Statistics*** screen. For example, browse to http://192.168.1.100 or http://zxi-XXXXXX where XXXXXX is the 6-digit serial number of the unit. The web interface will appear on the browser screen. All screens and operations available on the unit's screen will be available on the browser.

On some browsers or Operating Systems, the unit will need to be accessed by browsing to http://zxi-XXXXXX.local.

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

7.2 Command Line Interface (CLI)

A CLI or Command Line Interface is also available. 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 using 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 to any of the network ports in the back of the unit.
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 zxi-XXXXXX***
   where XXXXXX is the 6-digit serial number of the unit, then press Enter. A login 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 through the command line interface.

7.2.2 Connecting using SSH

Connecting 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 using 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 to any of the network ports in the back of the unit.
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 will be **zxi-*XXXXXX*** where XXXXXX is the 6-digit serial number of the unit).
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 through the command line interface.

7.3 Zero Configuration Networking (Zeroconf)

Zero Configuration Networking (Zeroconf) allows devices to automatically create a usable computer network based on the Internet Protocol Suite (TCP/IP). For example, when the unit is connected (connected through a network cable) directly to a Windows based computer that is DHCP enabled, both the unit 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.

8: Options

8.0 Options - Introduction

The ZXi has several available additional options including software options and additional accessories. For a complete list of available options, please visit https://www.logicube.com/shop/zclonexi. This section lists the following options:

- 4 Drive Expansion
- Serial Attached SCSI (SAS) Capability
- Hash Verification
- PCIe Bridge

To purchase one or more of these options or adapters, please contact Logicube Sales department at sales@logicube.com.

8.1 4 Drive Expansion

The optional expansion kit provides an additional 2 SAS/SATA and 2 SATA only targets for a total of 9 SATA (7 SAS) targets when cloning from a master drive or 10 SATA (8 SAS) targets from a network repository or from a repository stored on an external USB enclosure connected to the ZXi.

If the SAS option is installed and the Drive Expansions are installed, bays T6 and T7 will be able to detect and use SAS drives.

If the SAS option is ***not*** installed and the Drive Expansions are installed, bays T6 and T7 will only be able to detect other supported drives except for SAS drives.

8.1.1 Attaching the removable ZXi DriveStation

Follow these steps to attach the removable ZXi DriveStations to the ZXi's expansion slots:

1. Remove the cover on one of the expansion ports (T6 through T9) using a Phillips head screw driver. There are two screws on the cover (one on each side). Set the two screws aside as they will be used for the ZXi DriveStation.
2. Connect the ZXi DriveStation to the open port from step 1. When inserted properly, the ZXi DriveStation should not be protruding or sticking out.
3. Use the two screws set aside from step 1 to tighten and set the ZXi DriveStation in place.

8.2 Serial Attached SCSI (SAS) Option

This option, when activated, allows the ZXi to detect Serial Attached SCSI (SAS) drives. When this option is purchased, an updated license file will need to be installed/re-installed along with the ZXi software. See ***Chapter 6*** for details on how to load or reload the software.

8.3 Verification Option

This option, when activated, allows the ZXi to verify a clone's hash in one task (during the cloning task) and works with both Mirror or Clever. When this option is purchased, an updated license file will need to be installed/re-installed along with the ZXi software. See ***Chapter 6*** for details on how to load or reload the software.

8.4 PCIe Bridge

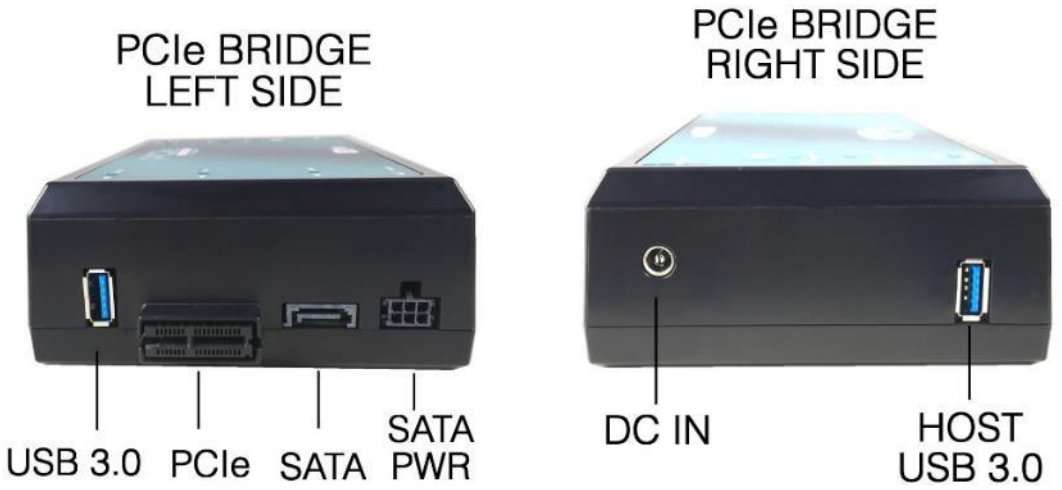
The Logicube PCIe Bridge is a hardware option that provides PCIe drive support on the ZXi. The PCIe Bridge can be purchased as a single device or as a kit (Part number F-ADP-PCIE-BRG-KT) which includes the PCIe adapter kit. The PCIe adapter kit (Part number F-ADP-PCIE-T-KT) includes 4 adapters.

The PCIe Bridge can support SSDs with the standard PCIe connector (Standard PCIe HHHL, FHHL, and FHFL).

The PCIe adapter kit includes adapters that provide support for the following drive types:

- M.2 PCIe NVMe SSDs
- M.2 PCIe AHCI SSDs
- mPCIe (Mini PCIe) SSDs
- mSATA SSDs

8.4.1 PCIe Bridge Overview



DRIVE LEDs (USB 3.0, PCIe, SATA) – For USB, PCIe, and SATA

- **On –** Detects a drive connected on the corresponding port
- **Blinking –** Detects activity on the corresponding port
- **Off -** No drive is detected on the corresponding port

HOST – Detects a link connection between the PCIe Bridge and the ZClone Xi

- **On –** Detects an active link between the PCIe Bridge and the ZClone Xi
- **Off –** There is no active link between the PCIe Bridge and the ZClone Xi

ALERT – 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

POWER – Power LED

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

8.4.2 PCIe Bridge Instructions

To use the PCIe Bridge:

1. **Make sure the PCIe Bridge is turned OFF.**

The PCIe port is not hot-swappable. Always turn the PCIe Bridge OFF when connecting or disconnecting drives through the PCIe port.

2. Connect a drive to the PCIe Bridge's PCIe port.

Connect only one drive to the PCIe Bridge. The PCIe Bridge only works with one drive connected at any time.

3. Connect the USB 3.0 A Male to A male cable to one of the ZXi's USB 3.0 ports and the other end of the cable to the PCIe Bridge's host port (on the right side).
4. Connect the AC adapter/power supply to a power source and the PCIe Bridge.

Logicube has qualified and included a 3-foot USB 3.0 A Male to A Male cable.

5. Press and release the power button located on the top of the PCIe Bridge. The Power LED will start blinking as the device turns on. The boot sequence may take about 30 seconds and when finished, the Power LED will stop blinking and turn on solid.

To disconnect or change drives, turn the PCIe Bridge OFF by pressing and releasing the power button. Wait for the Power LED to turn OFF. Once the PCIe Bridge is turned off, it is safe to disconnect or change drives. The ZXi does not need to be turned off.

9: ZXi-Laptop Cloning Version

9.0 ZXi-Laptop Cloning Version – Introduction

The ZXi-Laptop Cloning Version comes shipped with the ability to clone up to 6 laptops or computers (as Master or Target) without removing the drives inside the laptops/computers.

If your previously purchased ZXi is not the ZXi-Laptop Cloning Version and you would like to get the laptop cloning ability described in this chapter, please contact Logicube Sales at sales@logicube.com.

Using the ZXi-Laptop Cloning Version requires the laptop or computer to have a wired Ethernet connection and an available USB 2.0 or 3.0 Type A receptacle/port.

The ZXi-Laptop Cloning Version will be shipped with the following:

- Eight (8) Cat6 Ethernet cables.
- Two (2) Gigabit Ethernet switches (with AC adapter/power supply).
- Six (6) built-in USB cables located in the back of the ZXi.

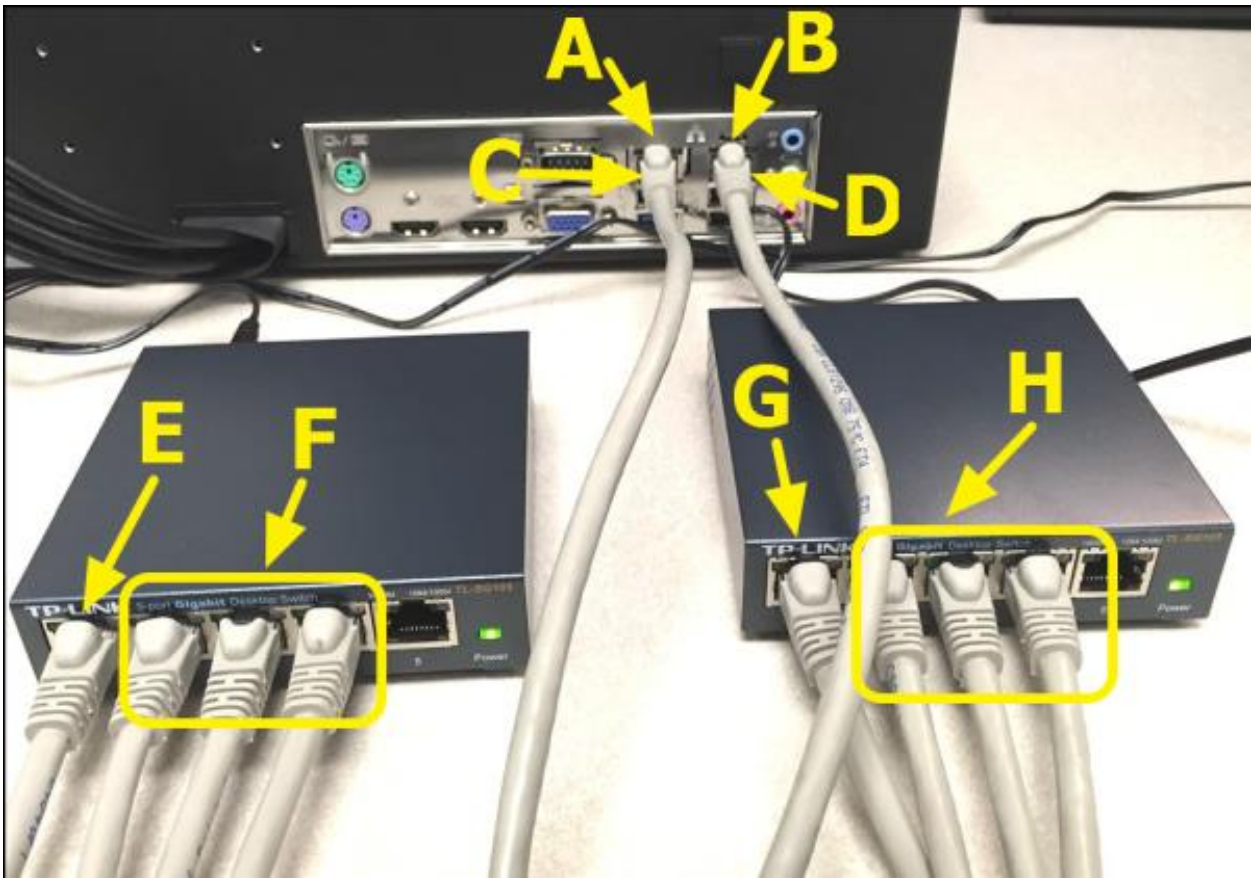
9.1 Requirements

Using the ZXi-Laptop Cloning Version requires the following:

- Desktops or laptops must be an x86 based Windows or Mac.
- Tablets must have Windows and is x86 based.
- All devices must have at least one available USB 2.0 or 3.0 Type A receptacle/port.
- All devices must support booting up from a USB flash drive.
- All devices must have support for a wired Ethernet connection (either through a built-in Ethernet port or an Ethernet adapter).

Tablets may require a docking station with a wired Ethernet port. Alternatively, it may be possible to use a USB-to-Ethernet adapter, but the laptop must support that configuration.

9.2 Setup Instructions

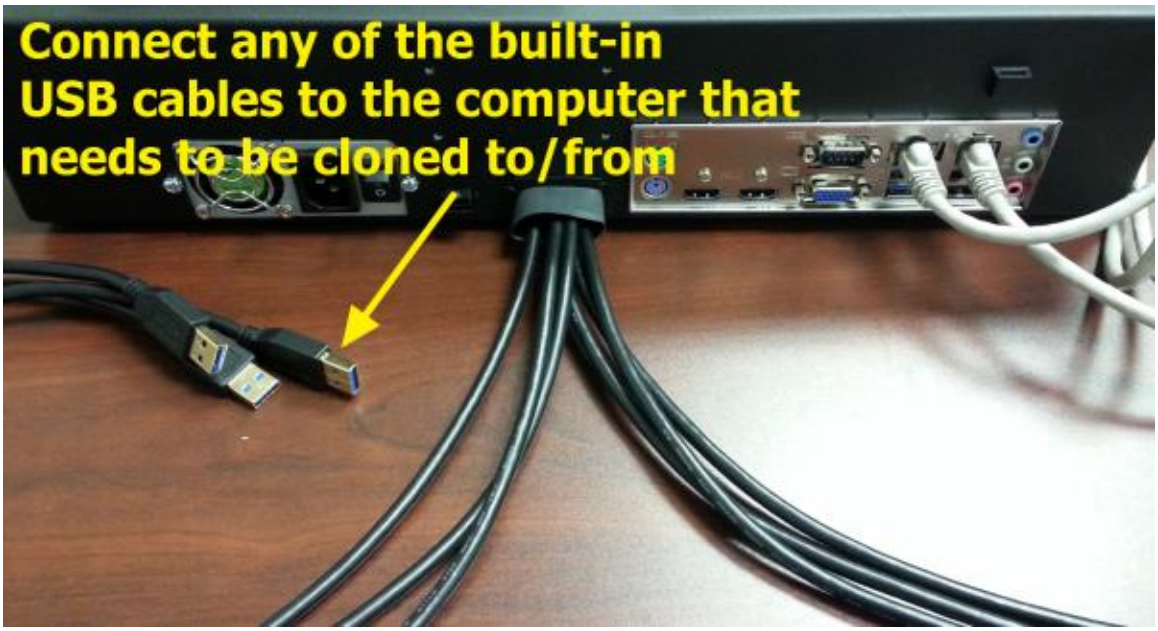


Using the picture above as a reference:

1. Each of the Gigabit Ethernet switches has an AC adapter/power supply. Connect an AC adapter/power supply to each of the switches to provide power.
2. Connect one Cat6 Ethernet cable **(C)** to one of the Ethernet ports on the ZXi **(A)**. Connect the other end of the Ethernet cable to any port on one of the Gigabit Ethernet Switches **(E)**.

   For more than one laptop or computer, it is recommended to use both switches to evenly distribute and balance the transfer rate and speed.

3. Connect a second Cat6 Ethernet cable **(D)** to the other Ethernet port on the ZXi **(B)**. Connect the other end of the Ethernet cable to any port on the other Gigabit Ethernet switch **(G)**.
4. For each computer to be cloned to/from, connect a Cat6 Ethernet cable **(F or H)** to one of the other available ports on any of the Gigabit Ethernet switches to the Ethernet port on the computer.



5. There are six (6) USB cables located in the back of the ZXi. Connect any of the built-in USB cables to the computer that needs to be cloned to/from.
6. Set the laptop/computer to boot from USB. Please contact the laptop/computer manufacturer if you do not know how to change the boot sequence to boot from USB or to find out if the computer supports this function.
7. The computer will boot from USB and the ZXi should see the computer as a Master or Target.

> For multiple computers:
>
> Each computer's display/monitor will show an IP address (for example, 169.254.11.21).
>
> The ZXi will show the last two segments of the IP address. For example, **I:11.21**
>
> The connected drive will show as ***SDA***. Additional connected drives will show as ***SDB***, ***SDC***, etc.
>
> For example, if there are two drives connected to the laptop/computer, one would show as **I:11.21/SDA** and the other drive will show as **I:11.21/SDB**.

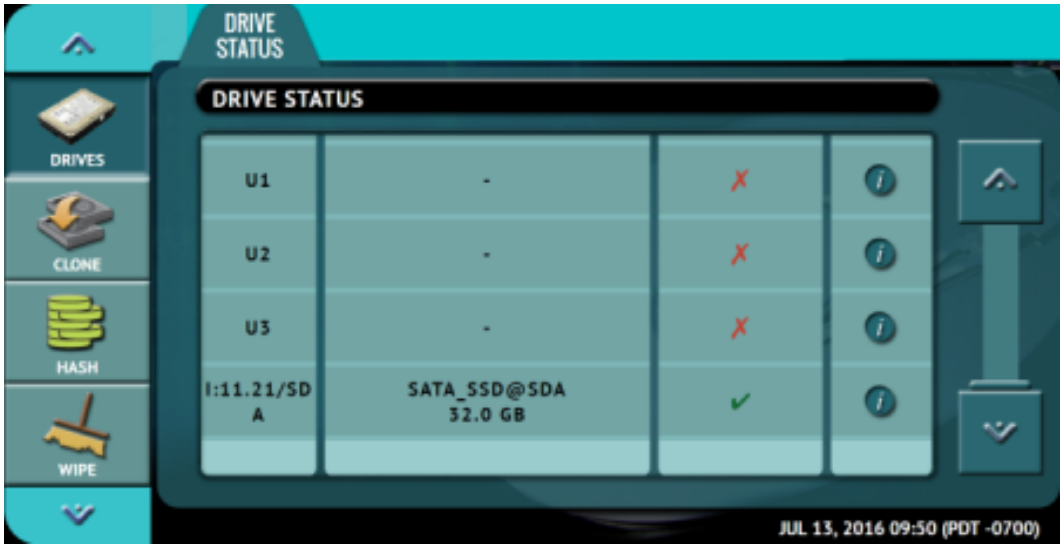
8. Once the ZXi sees all the connected computers and their drives, a Drive-to-Drive, Drive-to-Image, or Image-to-Drive clone can be performed. ***See Chapter 4 for details on Cloning***.

9.3 Additional notes

Depending on the operation or mode selected, the drives in the laptop/tablet/computer may or may not be selectable.

9.3.1 Drives

In the ***Drives*** screen, the drives will show at the bottom of the Drives screen. Scroll all the way down to see the connected drives on the tablet/laptop/computer.

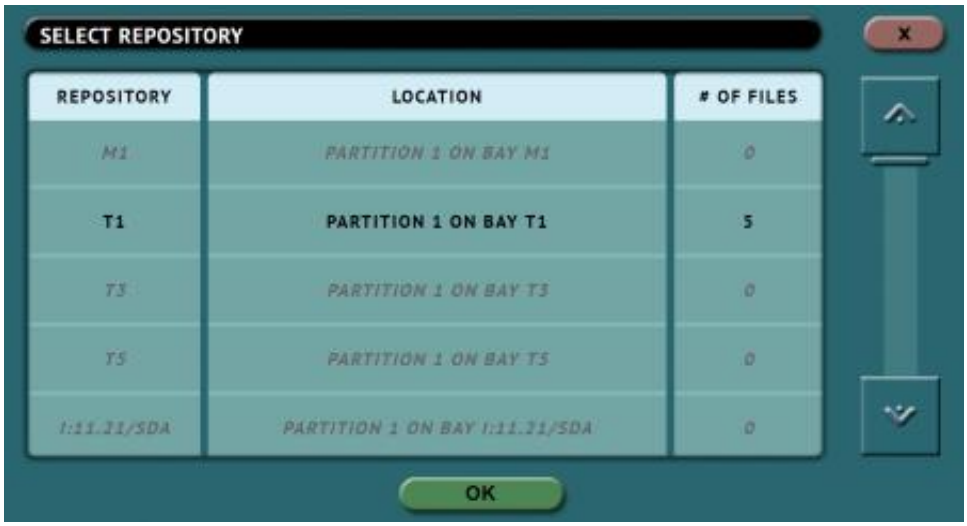


9.3.2 Clone

The drives will be selectable or grayed out depending on the ***Mode*** selected.

DRIVE TO DRIVE – Will show selectable in both the ***Master*** and ***Target*** screens.

IMAGE TO DRIVE – The drive(s) will most likely show grayed out (un-selectable) as a ***Master/Repository*** unless it contains ZXi created images. It will be selectable in the Target screen.



DRIVE TO IMAGE – The drive(s) will be selectable as a ***Master***. As a ***Repository***, it may or may not require formatting.

9.3.3 Hash

All connected drives are selectable in the Hash mode of operation.

9.3.4 Wipe

All connected drives are selectable in the Hash mode of operation.

10: Changing the default passwords

10.0 Changing the Default Passwords - Introduction

The ZXi comes with default accounts for the Command Line Interface. It is highly recommended to change the default passwords for security purposes.

- logicube
- it

If the new password(s) cannot be remembered, a system recovery must be performed to reset the passwords back to the default values.

10.1 Changing Both the *logicube* and *it* Passwords

To change both the "logicube" and "it" passwords, follow these steps:

1. Connect a USB keyboard to any available USB port of the ZXi then use the following key combinations: ***Alt+2*** then ***Alt+Shift+Enter***.
2. Once logicube prompt appears, type the following commands, one line at a time (Press the Enter key after each command/line):

   ```
   sudo mount -o remount,rw /
   passwd
   ```

3. The following prompt will appear:

   Changing password for logicube.

   (current) UNIX password:

4. Type the current password for the "logicube" account (the default password for this account is "logicube") then press the Enter key. The following prompt will appear:

   Enter new UNIX password:

5. Type a new password then press the Enter key. The following prompt will appear:

   Retype new UNIX password:

6. Type the new password again then press the Enter key. The following response should appear:

   passwd: password updated successfully

7. Next, type the following command:

   ```
   sudo smbpasswd logicube
   ```

8. The following prompt will appear:

   New SMB password:

9. Type the same password you used in step 5 above. The following prompt will appear:

   Retype new SMB password:

10. Type the same password again, then press the Enter key. The Logicube prompt should appear.
11. Next, to change the "it" password, type the following command then press the Enter key:

    ```
    sudo passwd it
    ```

12. The following prompt will appear:

    Enter new UNIX password:

13. Type a new password then press the Enter key. The following prompt will appear:

    Enter new UNIX password:

14. Type the new password again then press the Enter key. The following response should appear:

    passwd: password updated successfully

15. Next, type the following command:

    ```
    sudo smbpasswd it
    ```

16. The following prompt will appear:

    New SMB password:

17. Type the same password you used in step 5 above. The following prompt will appear:

    Retype new SMB password:

18. Type the same password again, then press the Enter key. The Logicube prompt should appear.
19. Type the following command then press the Enter key:

    ```
    sudo mount -o remount,ro /
    ```

20. Press the following key combinations to go back to the Graphical User Interface: ***Alt+1***

10.2 Changing Only the *logicube* Password

For the username: logicube

1. Connect a USB keyboard to any available USB port of the ZXi then use the following key combinations: ***Alt+2*** then ***Alt+Shift+Enter***.
2. Once logicube prompt appears, type the following commands, one line at a time (Press the Enter key after each command/line):

   ```
   sudo mount -o remount,rw /
   passwd
   ```

3. The following prompt will appear:

Changing password for logicube.

(current) UNIX password:

4. Type the current password (by default, "logicube" without the quotes) then press the Enter key. The following prompt will appear:

   Enter new UNIX password:

5. Type a new password then press the Enter key. The following prompt will appear:

   Retype new UNIX password:

6. Type the new password again then press the Enter key. The following response should appear:

   passwd: password updated successfully

7. Next, type the following command:

   ```
   sudo smbpasswd logicube
   ```

8. The following prompt will appear:

   New SMB password:

9. Type the same password you used in step 5 above. The following prompt will appear:

   Retype new SMB password:

10. Type the same password again, then press the Enter key. The Logicube prompt should appear.
11. Type the following command then press the Enter key:

    ```
    sudo mount -o remount,ro /
    ```

12. Press the following key combinations to go back to the Graphical User Interface: ***Alt+1***

10.3 Changing Only the *it* Password

For the username: it

1. Connect a USB keyboard to any available USB port of the ZXi then use the following key combinations: ***Alt+2*** then ***Alt+Shift+Enter***.
2. Once logicube prompt appears, type the following commands, one line at a time (Press the Enter key after each command/line):

   ```
   sudo mount -o remount,rw /
   sudo passwd it
   ```

3. The following prompt will appear:

   Enter new UNIX password:

4. Type a new password then press the Enter key. The following prompt will appear:

   Enter new UNIX password:

5. Type the new password again then press the Enter key. The following response should appear:

   passwd: password updated successfully

6. Next, type the following command:

   `sudo smbpasswd it`

7. The following prompt will appear:

   New SMB password:

8. Type the same password you used in step 5 above. The following prompt will appear:

   Retype new SMB password:

9. Type the same password again, then press the Enter key. The Logicube prompt should appear.
10. Type the following command then press the Enter key:

    `sudo mount -o remount,ro /`

11. Press the following key combinations to go back to the Graphical User Interface: ***Alt+1***

11: FREQUENTLY ASKED QUESTIONS

11.0 FAQs

Q. How many concurrent tasks can the ZXi run?
A. The ZXi can run up to 5 concurrent tasks.

Q. Do Target drives need to be wiped or formatted using the ZXi?
A. It is not necessary to wipe Target drives prior to cloning. However, if the user requires wiping Target drives, Logicube recommends using the ZXi to wipe Target drives. The ZXi logs all wipe operations.

Q. Can the ZXi clone Linux partitions?
A. Yes. ZXi can clone Linux partitions using both Mirror mode and Clever Clone mode.

Q. Can the ZXi clone a Hierarchical File System (HFS)?
A. Yes, ZXi can clone HFS using Mirror mode.

Q. How does the ZXi handle bad sectors found on the Master drive?
A. ZXi will retry the bad sector 7 times. After the 7th attempt, if the sector still cannot be read, it will skip that sector and list the sector in the log file.

Q. What operating system does ZXi use?
A. ZXi uses a Linux-based operating system. A Linux-based operating system provides increased stability and security over Windows-based systems.

Q. Does imaging performance slow down when multiple drives are imaged at the same time?
A. Performance is limited by the slowest drive in the configuration, however, there should not be any significant speed penalty when imaging multiple drives.

Q. How many separate tasks can you have running concurrently?
A. You can have up to five separate tasks running concurrently.

Q. Can I schedule or automate tasks?
A. ZXi features the ability to create up to 5 separate "Tasks Macros". Each macro allows you to set up to 9 operations to be performed sequentially. You can add these operations to a Macro and from the ZXi GUI select the Macro and the ZXi will perform the specified tasks/operations in the sequence you have defined. The user can save the Macro to use in future imaging sessions.

Q. Can the ZXi image to or from a network location?
A. Yes. The ZXi includes two gigabit network connections. Users can designate a network share as a repository using CIFS (Common Internet File System) or iSCSI (Internet Small Computer System Interface) protocols.

Q. Does the ZXi provide log files?
A. Yes, each operation/task produces a log file. The log file is viewable on the ZXi screen (or remotely on a PC) in an HTML format. The log files can be exported to a thumb drive (the ZXi will export in XML, HTML and PDF). XML log files can be customized using XML editors. The log files are stored on the internal hard drive within ZXi and are accessible by pressing the log file icon from the left-side navigation bar on the ZXi screen.

Q. If I am imaging to or from USB enclosures, will the ZXi's USB ports power my devices or will an additional power source be required?
A. Each of the ZXi's USB ports meets the standard specification of up to 5V of power. If your USB device has higher power requirements an external power source will be necessary. Check with the manufacturer of your USB device to determine the exact power requirements.

Q. Can the ZXi image to an external storage device such as a NAS (Network Attached Storage)?
A. Yes, ZXi can image to external storage devices. The external device can be connected to ZXi through the Gigabit Ethernet port or using the target ports (USB 3.0 or the SAS/SATA) built into ZXi. If the external storage device has a RAID configuration it will require that it be configured as a single drive. Any Master drive connected to ZXi can be imaged directly to the external storage device.

12: Index

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**

Software Attribution

Debian 8 (Jessie) (https://www.debian.org/)

Linux Kernel (4.9.6-3) (GPL v2) (http://www.kernel.org) (modified)

libcli (1.9.5) (LGPL v2.1) (https://github.com/dparrish/libcli) (modified)

ntfs-3g (1:2013.1.13AR.1-2ubuntu4) (GPL v2) (https://packages.debian.org/source/stretch/ntfs-3g) (modified)

PDFJS (1.0.907) (Apache License v2.0) (https://github.com/mozilla/pdfjs-dist) (modified)

blistr (MIT) (http://github.com/idleberg/Bootstrap-Listr) (modified)

jstree (3.3.7) (MIT) (http://jstree.com/) (modified)

Electrostatic Discharge (ESD) WARNING

All electronic products may be susceptible to Electrostatic Discharge (ESD). Electrostatic discharge (ESD) is the sudden flow of electricity between two electrically charged objects caused by contact, an electrical short, or dielectric breakdown. The ZClone ZXi (ZXi) has been designed to minimize the effects of ESD and if an ESD event occurs the unit may experience a temporary loss of functionality. If this occurs, please power down the ZXi and power it back up, this should clear any temporary loss of functionality.