ZXi™-10G User's Manual

Logicube, Inc.

Chatsworth, CA 91311

USA

Phone: 818 700 8488

Fax: 818 700 8466

Version: 2.0a

Date: 01/27/2022

MAN-ZXi-10G

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 HAZ7ARDOUS 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 ZXi-10G

The ZXi™-10G provides the ability, with an optional PCIe Expansion Module to clone up to 16 M.2 NVMe SSDs. The ZXi-10G is the first hard drive duplicator on the market to include two 10 GbE network connections, allowing you to streamline your workflow and clone directly to or from a network repository or a NAS device. The ZXi-10G efficiently performs hard drive duplication and wiping tasks including PC deployments, OS upgrades, content/application distribution, and data backup tasks.

1.1 Features

- High-speed cloning – The ZXi™-10G will clone at blazing speeds up to 29GB/min* using SATA SSDs
- M.2 NVMe Cloning – The optional PCIe Expansion Module supports cloning up to 16 M.2 NVMe SSDs. Clone up to 129GB/min* using high-performance NVMe SSDs.
- The ZXi-10G 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.

- Two high-speed 10GbE connections are available to clone or create images to/from a network repository or NAS and achieve transfer speeds of up to 30GB/min. Utilize a 2.5GbE connection to help minimize bottlenecks.
- Supports cloning to and from USB enclosures and thumb drives. 9 ports are available:
    - 6 USB 3.2 Gen 1 (Type A)
    - 2 USB 3.2 Gen 2 (Type A)
    - 1 USB 3.2 Gen 2x2 (Type C)
- Two Thunderbolt™ 4/USB 3.2 Gen 2x2 ports allow users to connect Thunderbolt external storage enclosures to the available port on the ZXi-10G and clone to/from these solutions
- Optional 4-Port 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 10 SATA (8 SAS) targets from a network repository or an external USB enclosure connected to the ZXi-10G
- M.2 SATA, 1.8”/2.5”/3.5” IDE and IDE ZIF drives, eSATA, microSATA, mSATA and flash media are supported with optional adapters
- 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-10G created image repository stored on an external USB enclosure or a network repository to a total of 6 SATA/SAS target hard drives
- Supports multiple master drives – Users can assign any port as a master or target
- Wipe feature – Choose from Secure Erase, DoD wipe, and custom pass settings. Complies with NIST 800-88 guidelines. User selectable option to verify wipe pass value during the wipe process.
- Hash verification (SHA1, SHA256 or MD5) allows users to clone and verify the exact replication of the source drive. Available with the purchase of an optional software activation package
- Multi-session capability allows users to perform multiple tasks, including cloning, wiping or hashing concurrently
- Write-protected master drives – Any drives designated as master by the user are automatically write-blocked to prevent any alteration to sensitive data on the master drive
- Task Macro feature allows users to set specific tasks to be performed sequentially. For example, wipe, then clone, then hash.

- 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-10G created images in a repository on a USB enclosure connected to ZXi-10G or on a shared network location and then clone to selected targets
- Bad sector handling – When bad sectors are encountered on the source drive the cloning process can abort or skip the bad sector. Bad sectors are logged for review.
- Advanced administrative functions allow users to create/manage image repositories, manage network settings, create user profiles, save configurations, manage drive station assignments, etc.

- Audit trail/log report provides detailed information on each completed task. Logs can be printed using a web browser and a PC. Includes a digital signature for authentication purposes.
- HPA/DCO support – Clone or wipe HPA/DCO areas of a drive
- Color touch screen display provides an intuitive and easy-to-use interface
- Removable drive stations are user and field-replaceable
- Remote operation allows users to control all operations from a remote computer using a web browser or CLI interface

*Speed referenced was achieved using high-performance SSDs and mirror mode. The specification and condition of drives and settings used may affect the achieved speed.

1.2 In the Box

The complete ZXi-10G system includes the following:

- The Logicube ZXi-10G unit
- Power cable
- 6 SAS/SATA 5” data/power cables
- 3 Cat 7 network cables
- CD-ROM with user’s manual

1.3 Options

The following options are available with the ZXi-10G:

- 4-Port Drive Expansion Kit: Provides an additional 2 SATA/SAS and 2 SATA-only drive stations. Includes 4 drive stations, 4 cables, and a drive tray.
- PCIe Expansion Module: Provides support for up to 16 M.2 NVMe SSDs.
- Hash Verification Option: Clone and verify the exact replication of the master drive in one single process. Features SHA-1, SHA-256, or MD5 algorithms. Hash verification is embedded in the audit trail/log file.
- SAS Option: Enables support for SAS drives.
- mSATA to SATA adapter
- Micro SATA to SATA adapter
- eSATA cable
- 2.5"/3.5" IDE to SATA adapter
- 1.8" IDE to SATA adapter
- 1.8" ZIF to SATA adapter

- USB Flash Reader
- SATA/SAS data & power replacement cable
- Extended warranties

1.4 Specifications

Power Requirements	Operating Temperature	Storage Temperature	Relative Humidity	Net Weight	Dimensions
110V-240V 7.5A-3.5A 50-60Hz	32° to 122° F 0° to 50° C	-4° to 176° F -20° to 80° C	Operating: 85% RH, non-condensing Storage: 95% RH, non-condensing	14 lbs 6.4 kg	3.7" H x 19" D x 17.2" W 94 mm x 483 mm x 437 mm

WARNINGS:

- Avoid dropping the Logicube ZXi-10G or subjecting it to sharp jolts. When in use, place it on a flat surface.
- Keep the unit dry. If the ZXi-10G 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-10G. Doing so may void the warranty. If the unit requires service, please contact Logicube Technical Support for assistance.

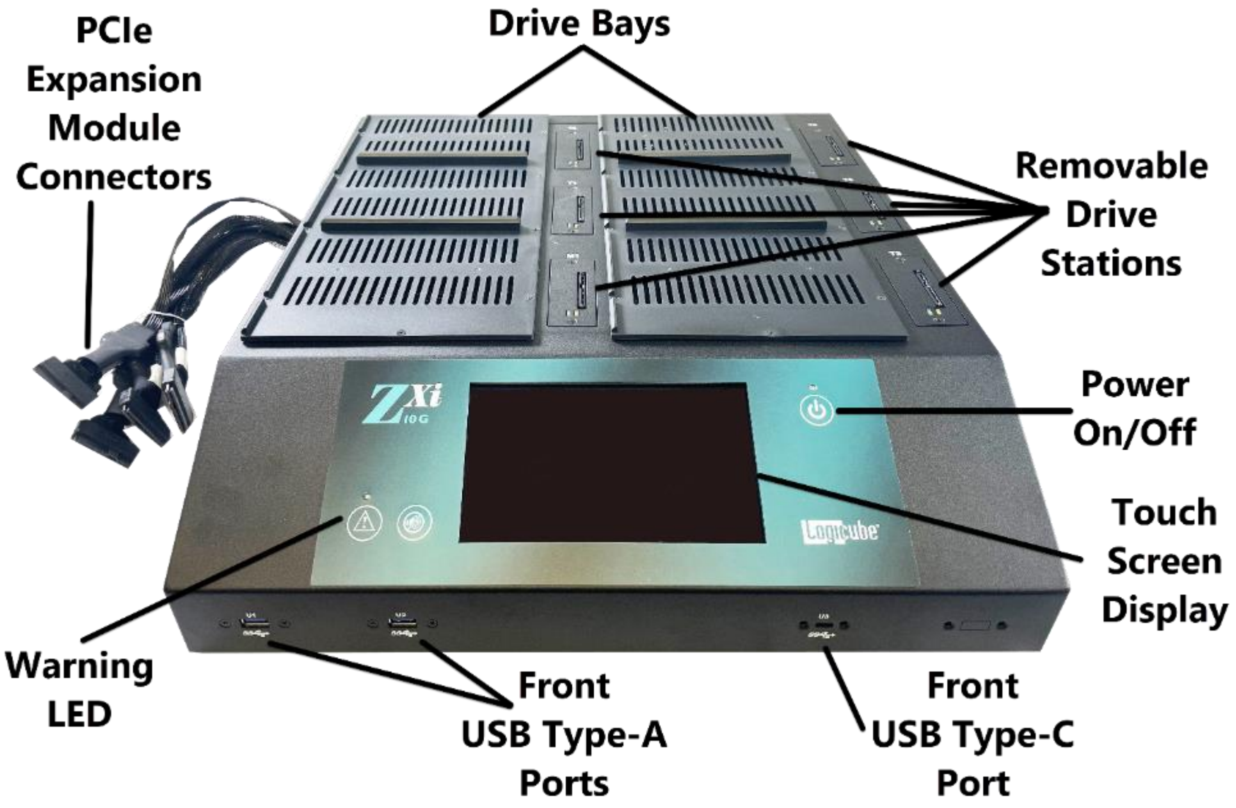
2: Getting Started

2.0 Overview of the ZXi-10G

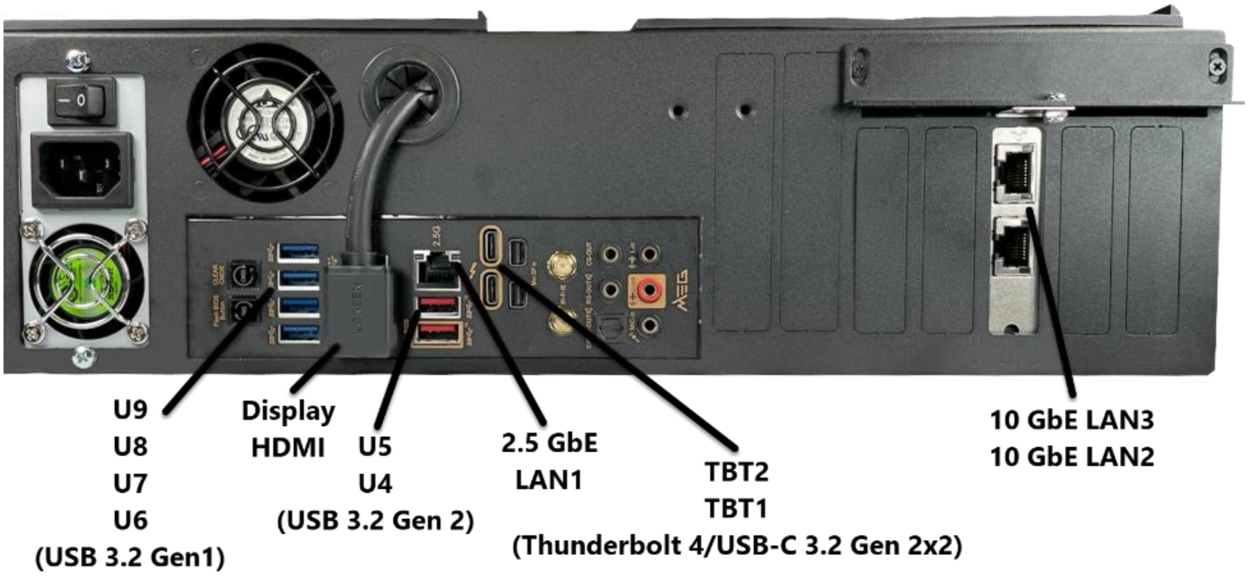
ℹ ⚠

Special Icons – Throughout this manual, two icons 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.

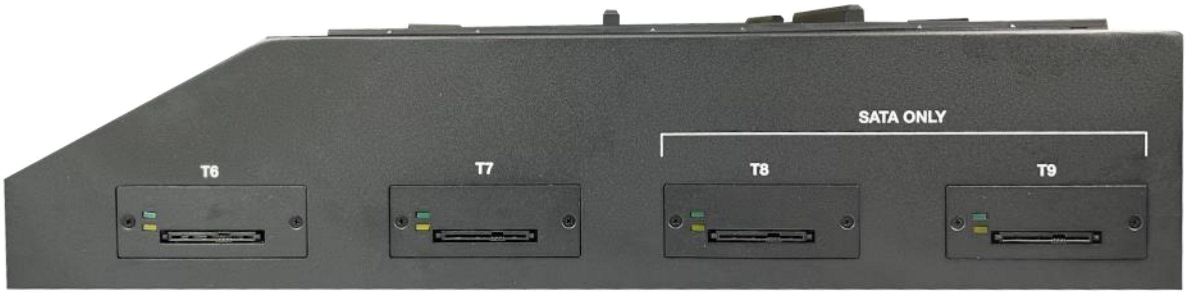
ZXi-10G Overview



ZXi-10G Rear View



ZXi-10G Expansion Bays



2.1 Turning the ZXi-10G On and Off

The ZXi-10G comes with a NEMA 5-15P to IEC C-13 power cable. Attach the included power cable to the power connector in the back of the ZXi-10G.

To turn the ZXi-10G on, turn the power supply switch (located near to the power connector in the back of the ZXi-10G) to the ON position. Press and release the power button on the front of the ZXi-10G. The ZXi-10G 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-10G off, press and release the power button located on the front of the ZXi-10G. Another way to turn the ZXi-10G off is to 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.

> ⚠ It is not recommended to use the power switch located on the back to turn the ZXi-10G off.

2.2 Connecting various drive types

The ZXi-10G comes standard with SAS/SATA cables. One end of the cable has a male connector that connects to the ZXi-10G. On the other end is a female connector that connects to a drive or Logicube qualified drive adapter.

> ℹ Support for SAS drives is optional. 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, contact our sales team at sales@logicube.com.

Cables and adapters are available for the following drive types:

- SAS
- SATA
- USB
- Thunderbolt (through the USB-C port)
- M.2 (NVMe, AHCI, and SATA) (optional)
- 1.8” micro SATA (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)

> ⚠ The Thunderbolt/USB-C ports are not hot-pluggable when using Thunderbolt drives. For a Thunderbolt drive to be recognized, the ZXi-10G must be turned off when connecting a Thunderbolt drive.

> ℹ When connecting/disconnecting drives using drive adapters, 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-10G ports are hot-swappable (except for the Thunderbolt 4 ports). Drives that are not being used in any task (clone, hash, wipe, etc.) can be disconnected at any time.

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

Each connected drive can be configured as a Master, Target, or both Master/Target. For details and important information on how to change the *Bay Roles*, see *Section 5.9.4*.

When disconnecting drives, it is very important to make sure the drives are not being used on any task. Disconnecting drives while the ZXi-10G is using the drive for a task may cause data loss.

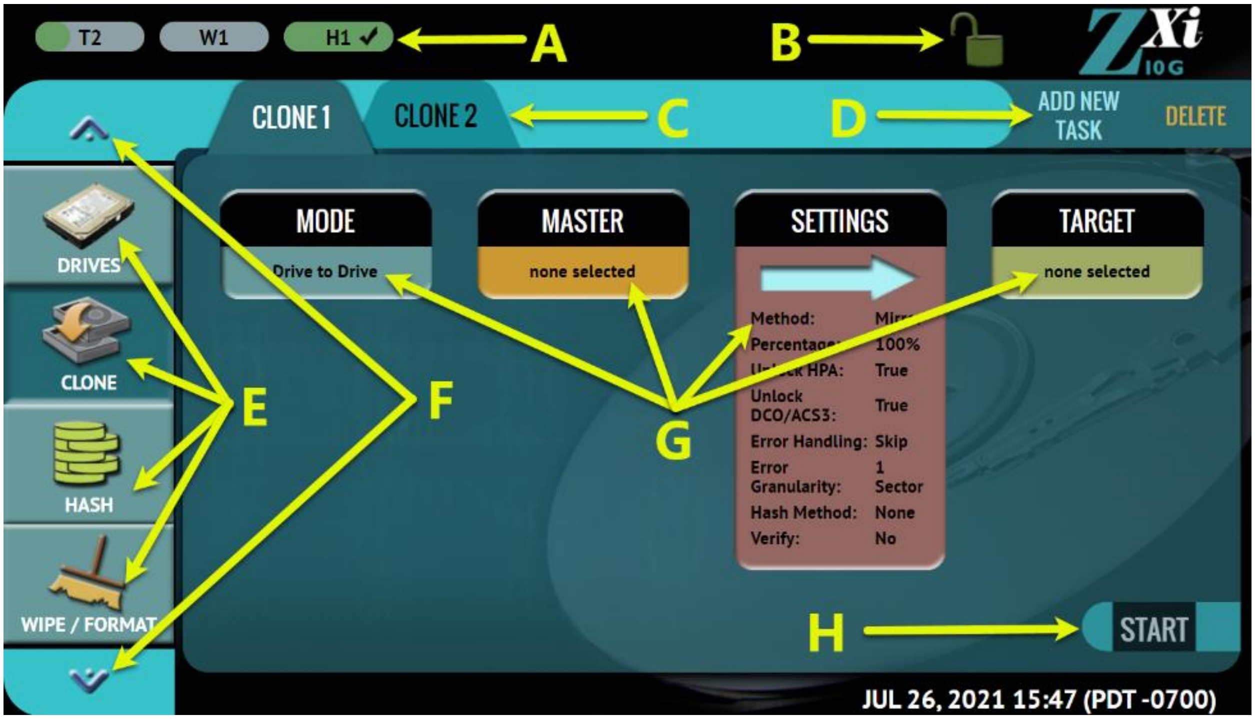
2.3 Drive Bay LEDs

Each bay has a drive station that has the following LEDs:

- Green LED
  - OFF – The ZXi-10G is not detecting a connection and is not supplying power to that bay.
  - ON (Solid) – The ZXi-10G 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-10G is gathering drive information details) or during any clone, wipe, or hash task as the ZXi-10G 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.



Drive to Drive

none selected

Method: Mirr
Percentage: 100%
Unlock HPA: True
Unlock DCO/ACS3: True
Error Handling: Skip
Error Granularity: 1 Sector
Hash Method: None
Verify: No

none selected

JUL 26, 2021 15:47 (PDT -0700)

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-10G 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 Operating System and ZXi-10G Application Software

The ZXi-10G has an SSD storage drive that contains the operating system and ZXi-10G 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-10G (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-10G can perform up to five (5) tasks for each mode of operation (specifically Image, Hash, and/or Wipe).

It is highly recommended to change the passwords for built-in accounts. Instructions on how to change the passwords to the two built-in user accounts can be found in *Section 5.9.2.2*.

There are software options available such as:

- Support for SAS (Serial Attached SCSI) drives
- Verify functionality

To find out if these options are enabled on ZXi-10G, tap the *Statistics* icon from the navigation menu then select the *Options* tab.

For more information on these and other options, see *Chapter 8: Hardware and Software Options*.

To purchase this option, contact the Logicube Sales Department at sales@logicube.com.

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 ⓘ

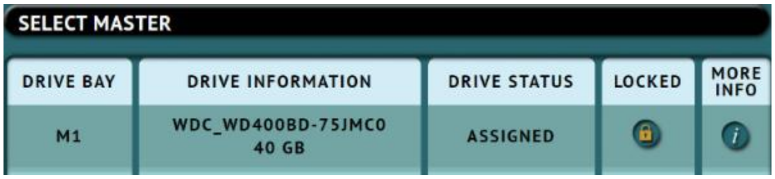
Drives types are listed in the following order:

- SAS/SATA ports
- USB ports
- PCIe (NVMe) ports
- Thunderbolt Ports

3.1.1 ATA Security Locked Drives

With ZXi-10G software version 2.0 (and newer), drives that are locked with the ATA security standard can be temporarily unlocked. The password used to lock the drive is required to unlock the drive.

Drives that are locked with the ATA security standard will show a locked icon in the *LOCKED* column when selecting drives (Master or Target).

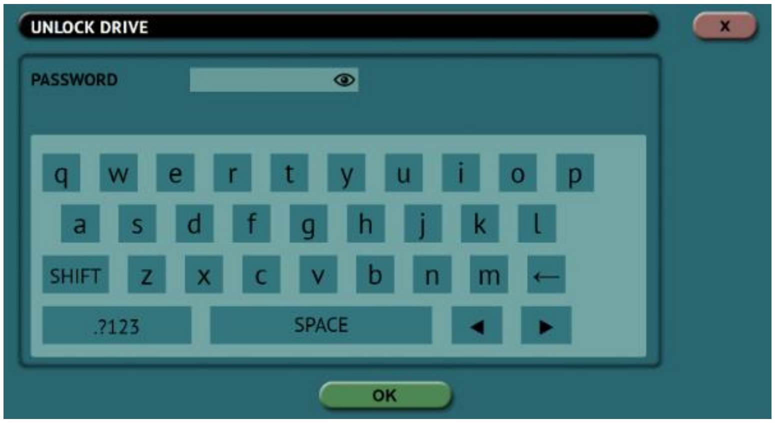


SELECT MASTER

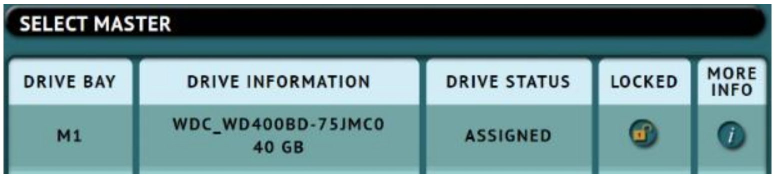
DRIVE BAY	DRIVE INFORMATION	DRIVE STATUS	LOCKED	MORE INFO
M1	WDC_WD400BD-75JMC0 40 GB	ASSIGNED	🔒	ⓘ

When the drive is locked, the contents of the drive are not accessible. Locked drives cannot be cloned (as Master or Target), hashed, or wiped without first being unlocked.

To temporarily unlock the drive, go to the Clone, Hash, or Wipe screen, and in the drive selection screen, tap the locked icon, The UNLOCK DRIVE screen will appear:



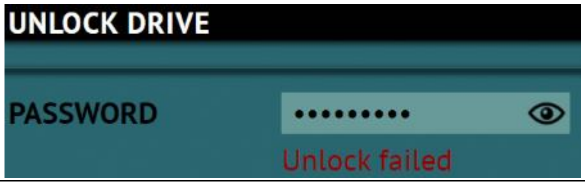
Enter the password to unlock the drive. If the entered password is correct, the screen will change to show an UNLOCKED icon:



SELECT MASTER

DRIVE BAY	DRIVE INFORMATION	DRIVE STATUS	LOCKED	MORE INFO
M1	WDC_WD400BD-75JMC0 40 GB	ASSIGNED	🔓	ⓘ

If the wrong password was entered, an ‘Unlock failed’ message will appear:



UNLOCK DRIVE

PASSWORD ••••••••••

Unlock failed

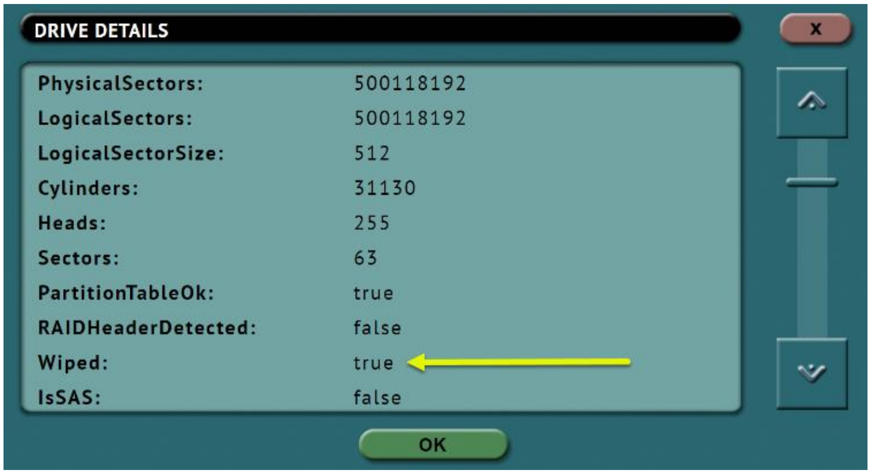
Once the drive is unlocked, it can be used for a clone task (as Master or Target), a hash task, or a wipe task.

The drive will remain unlocked temporarily until the drive is disconnected or powered down. If the drive is disconnected then reconnected, it will be locked again. While the drive is unlocked, a Secure Erase wipe will permanently remove the password lock.

3.1.2 Blank Disk Check

A blank disk check can be performed to see if a drive has been wiped by the ZXi-10G. This check may not be accurate if Secure Erase was used to wipe the drive. To perform a blank disk check:

1. Connect a drive to the ZXi-10G.
2. Go to Drives to see the list of connected drives.
3. Tap the *More Info* icon to the right of the drive to display information about the drive.
4. Tap or click the down arrow located to the right of the screen to scroll down to the second page of information.
5. Locate the line that shows "Wiped". This will either show *True* (drive is blank) or *False*.



PhysicalSectors:	500118192
LogicalSectors:	500118192
LogicalSectorSize:	512
Cylinders:	31130
Heads:	255
Sectors:	63
PartitionTableOk:	true
RAIDHeaderDetected:	false
Wiped:	true
IsSAS:	false

A drive that has just been wiped by the ZXi-10G must be disconnected then reconnected to refresh the drive details.

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).

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-10G to one or more Target drives.
- Drive to Image – Creates a Logicube ZXi-10G image file to a Target drive or Repository. This image file can be restored to drives using the Image to Drive mode.

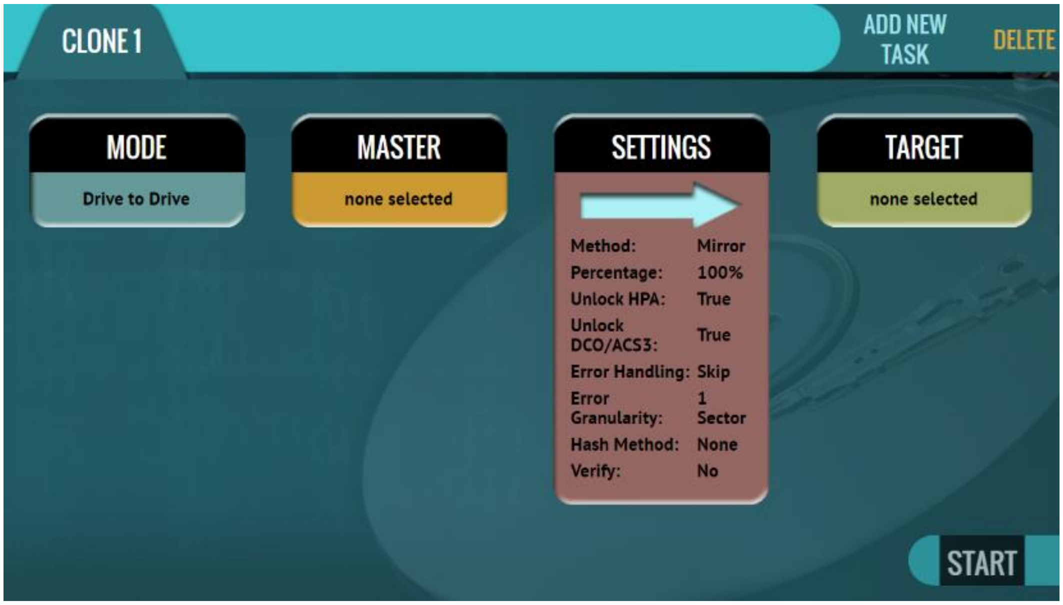
One or more Master drives can be cloned to one or more Target drives by using additional cloning tasks. Any drive bay can be configured as a Master, Target, or both Master and Target. Details on how to change the bay roles can be found in *Section 5.9.4*.

The ZXi-10G 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



MODE: Drive to Drive

MASTER: none selected

SETTINGS:

Method:	Mirror
Percentage:	100%
Unlock HPA:	True
Unlock DCO/ACS3:	True
Error Handling:	Skip
Error Granularity:	1 Sector
Hash Method:	None
Verify:	No

TARGET: none selected

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 or image file to be restored 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.

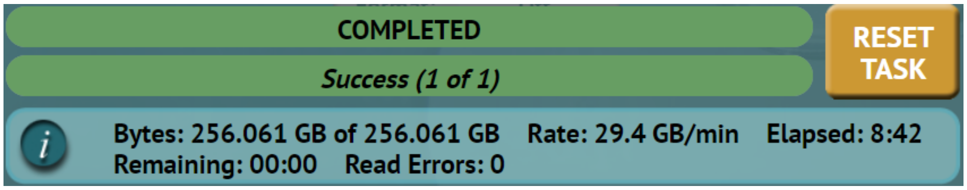
5. Tap the *Target* (or *Image File*) icon and select the Target or Image File then tap the *OK* icon.

> For *Drive to Image*, the ZXi-10G must be used to format drives. If the Target drive is not formatted by the ZXi-10G, the *Format* icon will appear in the Format column. Tap the f *(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 do not show as being used or assigned for other tasks.



COMPLETED

Success (1 of 1)

Bytes: 256.061 GB of 256.061 GB Rate: 29.4 GB/min Elapsed: 8:42
Remaining: 00:00 Read Errors: 0

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

3.3 Hash

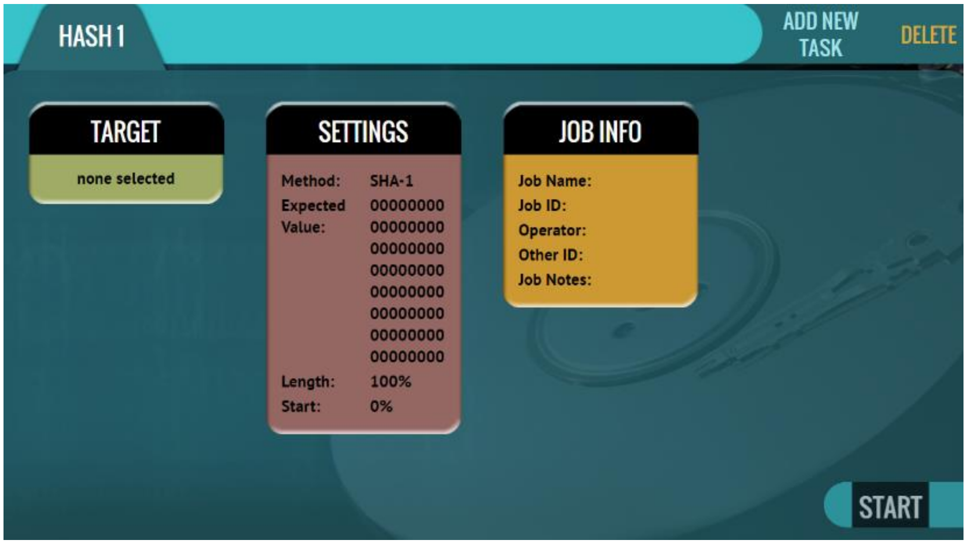
HASH

A hash or operation can be performed on any connected drive. Performing a hash task will instruct the ZXi-10G 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 ZXi-10G 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

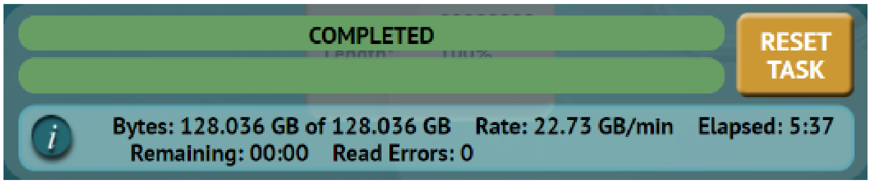


none selected

Method: SHA-1
Expected Value: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
Length: 100%
Start: 0%

Job Name:
Job ID:
Operator:
Other ID:
Job Notes:

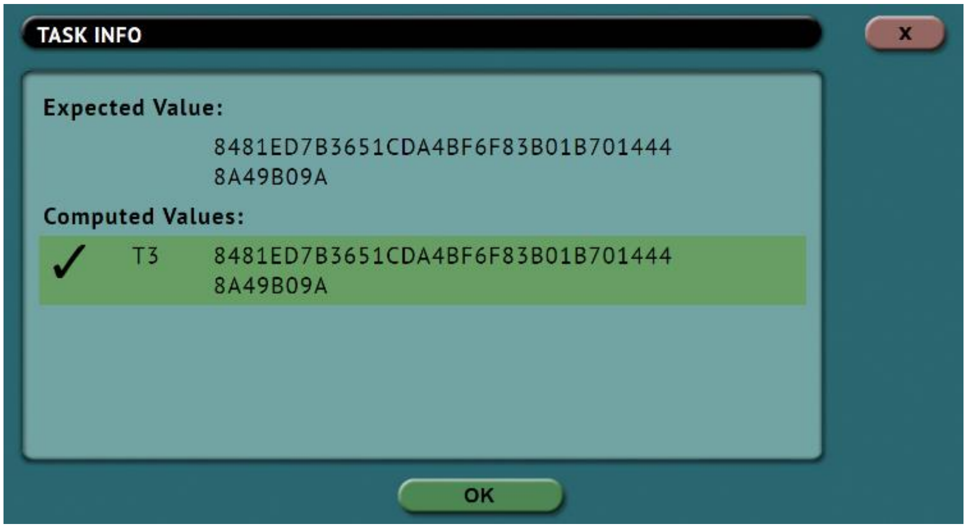
1. Select *Hash* from the types of operation on the left side.
2. Tap the *Target* icon and select the drive(s) to be hashed then tap the *OK* icon.
3. Tap the *Settings* icon to choose the different settings. Details for every setting can be found in *Section 5.3.2*.
4. Change any of the optional settings (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 do not show as being used or assigned for other tasks. Click the *Info* icon on the bottom left of the status to view the hash value. The hash value can also be seen in the log file (See *Section 3.6* for more information on logs).



COMPLETED

Bytes: 128.036 GB of 128.036 GB Rate: 22.73 GB/min Elapsed: 5:37
Remaining: 00:00 Read Errors: 0

Here is a screenshot of the hash value seen in the Information screen:


TASK INFO

Expected Value:

8481ED7B3651CDA4BF6F83B01B701444
8A49B09A

Computed Values:

✓ T3 8481ED7B3651CDA4BF6F83B01B701444
8A49B09A

3.4 Wipe / Format

Drives connected to bays that are configured as Target (or both Master and Target) can be wiped or formatted. Drives to be used as Targets for the “Drive to Image” method must be formatted by the ZXi-10G. The following methods are available in the Wipe/Format menu:

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

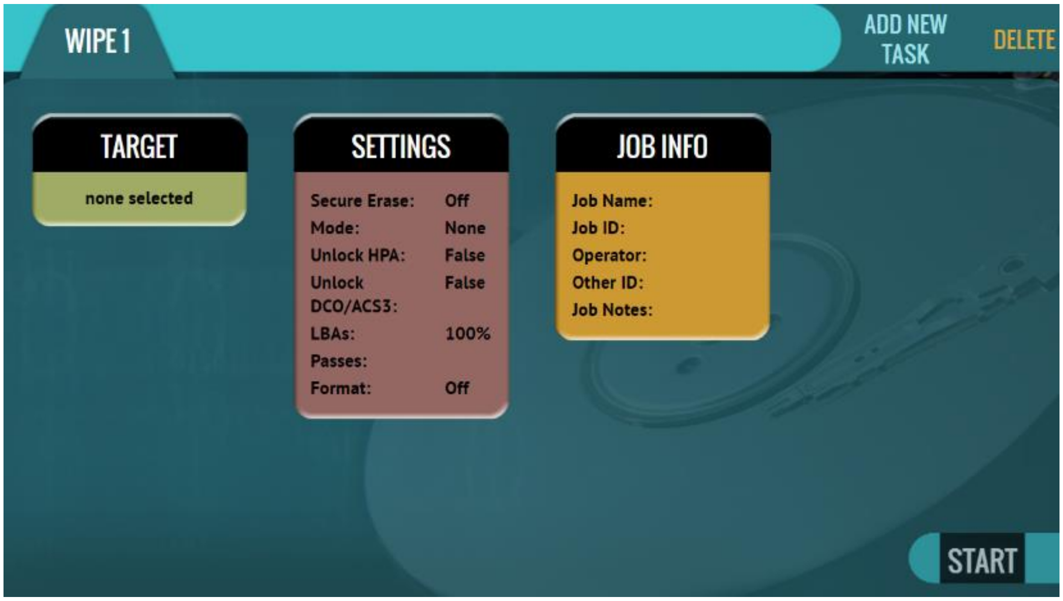
- *Secure Erase* – Sends a command to the drive instructing it to wipe the drive based on the hard drive manufacturer’s specifications for the Secure Erase command.

  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 PCIe 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. Also, a 7-pass DoD wipe can be set with pre-selected pass values.
- *Format* – Formats a drive. Supported file systems are *NTFS, EXT4, exFAT,* and *FAT32*. The ZXi-10G 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 ZXi-10G will perform a Secure Erase first then a Wipe Patterns wipe.

3.4.1 Step-By-Step Instructions – Wipe / Format



none selected

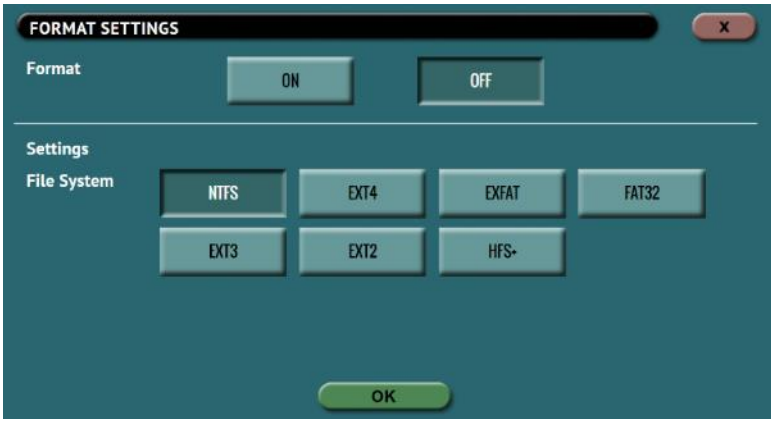
Secure Erase: Off
Mode: None
Unlock HPA: False
Unlock DCO/ACS3: False
LBAs: 100%
Passes:
Format: Off

Job Name:
Job ID:
Operator:
Other ID:
Job Notes:

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.

Optional: Tap Job Info to set the Job Name, Job ID, Operator, Other ID, or Job Notes.

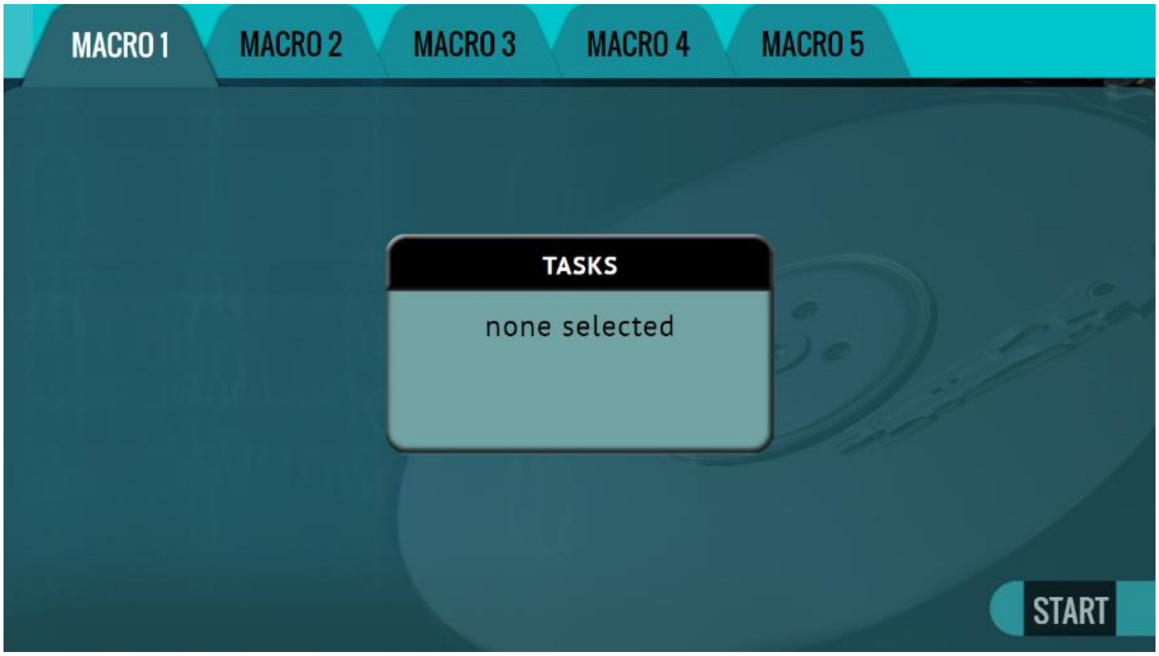
7. Tap the *Start* icon to start the Wipe task. A Secure Erase will be performed first (if selected), then a Wipe Pattern (if selected), then finally a Format (if selected).
8. When finished, the status will show "COMPLETED". At this point, it is recommended to tap *Reset Task* to reset the task, so the drive bays properly reset and do 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:



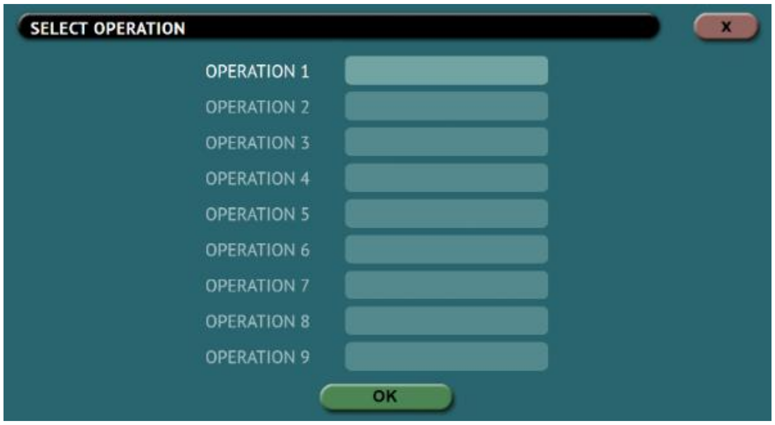
TASKS

none selected

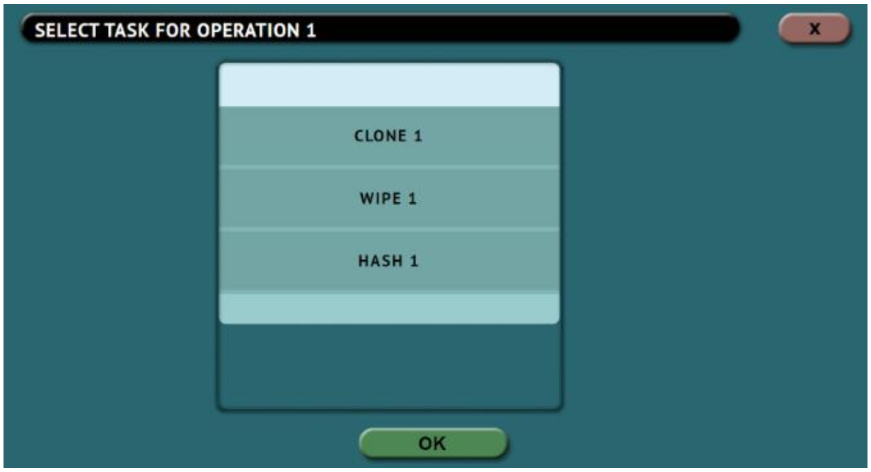
Each task or operation must be set up before setting up the macro. For example, to set up a Task Macro that will perform a wipe, then clone, users must first set up both the wipe and clone tasks. Once the wipe (for example, Wipe 1) and clone (for example, Image 1) have been set up, the Task Macro can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

3.5.1 Step-By-Step Instructions – Task Macro

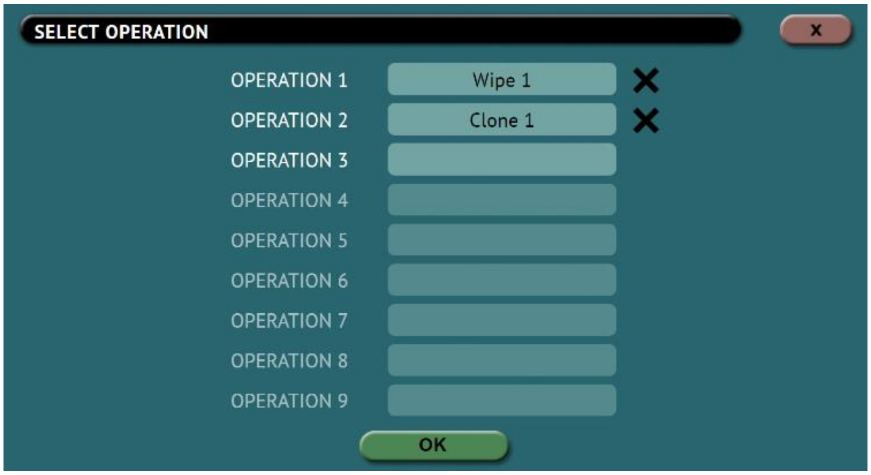
Tapping this icon allows the user to set specific tasks for each macro. The following window will appear:



Tap *Operation 1* to set the first operation in the macro. The following screen will appear allowing the user to choose the task. Choose a task then 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.



OPERATION 1 Wipe 1

OPERATION 2 Clone 1

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

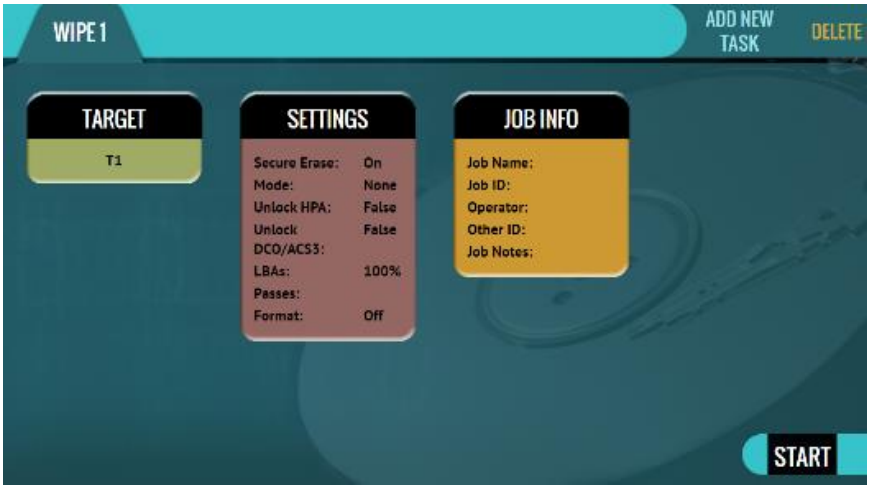
To start the macro and have the ZXi-10G perform all the operations on the task list, tap the *Start* icon in the Task Macro screen.

> If the Tasks Macro's Start button is not clickable (grayed out), check each of the tasks set for the Macro (for example, check Clone 1 and Hash 1). This typically means one or more tasks are not set up properly/completely.

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.

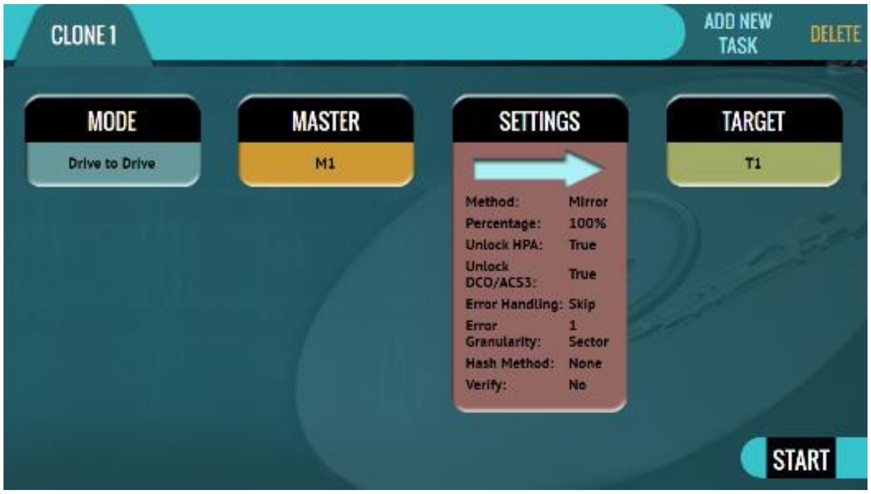


TARGET
T1

SETTINGS
Secure Erase: On
Mode: None
Unlock HPA: False
Unlock DCO/ACS3: False
LBAs: 100%
Passes:
Format: Off

JOB INFO
Job Name:
Job ID:
Operator:
Other ID:
Job Notes:

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.



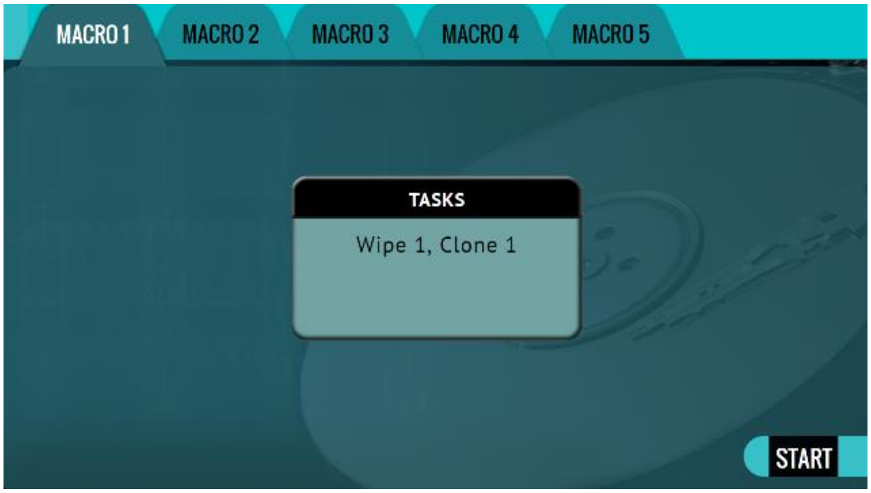
MODE
Drive to Drive

MASTER
M1

SETTINGS
Method: Mirror
Percentage: 100%
Unlock HPA: True
Unlock DCO/ACS3: True
Error Handling: Skip
Error Granularity: 1 Sector
Hash Method: None
Verify: No

TARGET
T1

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.



Wipe 1, Clone 1

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

3.6 Logs

Audit logs of all clone, hash, and wipe operations are stored and saved on the ZXi-10G. Logs can be viewed directly on the ZXi-10G or from a computer's browser (if the ZXi-10G is connected to a network). Logs can be exported to a USB flash drive in PDF, HTML, and XML format.

Software v2.0 adds S.M.A.R.T. data logs for drives used in any *Clone*, *Hash*, or *Wipe* operation.

Two files will be exported, "pre" and "post", capturing S.M.A.R.T. data at the beginning of the task and the end of the task. S.M.A.R.T. logs are located in the smartlogs subfolder and can be retrieved by following the instructions in *Section 3.6.4*.

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

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

To view the audit log files:

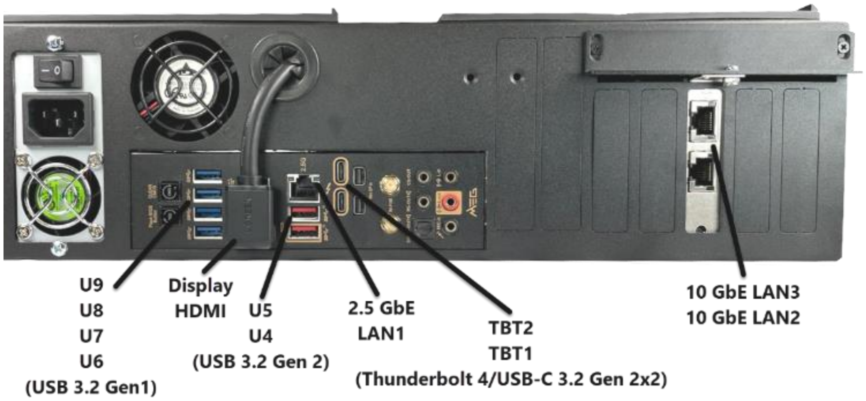
1. Select *Logs* from the types of operation on the left side. A list of log files will appear sorted by date (newest on top).
2. Select the log file to view by tapping the name of the log file. This will highlight the log file chosen.
3. Tap the *View* icon to view the log file on-screen.

The audit log files can also be exported to a USB drive. To export the audit log files:

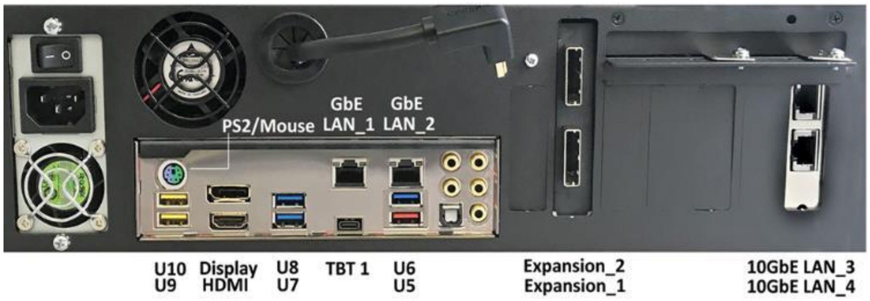
1. Select *Logs* from the types of operation on the left side. A list of log files will appear sorted by date (newest on top).
2. Select the log file to view by tapping the name of the log file. This will highlight the log file chosen.
3. The log files will be exported to a USB flash drive. The USB flash drive will need to be connected to one of the USB ports located in the rear panel of the ZXi-10G. The specific USB port is dependent on the I/O ports located in the rear panel of the ZXi-10G:

> The USB flash drive connected to U9 must be formatted in Windows using the NTFS, FAT32, or FAT file system.

a. If the rear I/O ports look like the image below, connect a formatted USB flash drive to the U9 USB port.



b. If the rear I/O ports look like the image below, connect a formatted USB flash drive to the U9 or U10 USB port. Disconnect any other drive connected to U9 and U10.



4. 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.

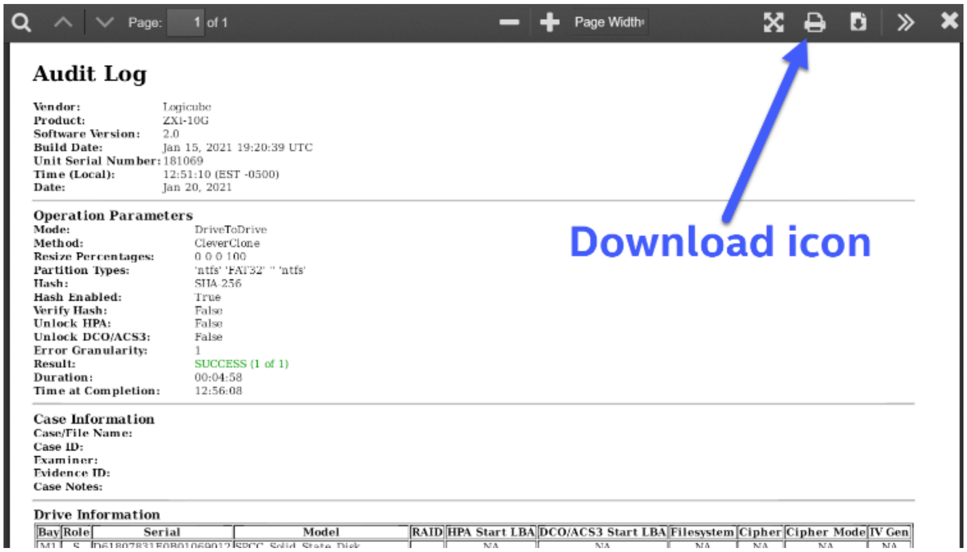
Repeat steps 2 and 3 if other log files need to be exported or viewed. Alternatively, all the log files can be exported by tapping the *Select All* button to select all the log files. Once all log files are selected, they can be exported in a single operation.

Log files can also be accessed over the network. See Section 3.6.4 for details.

To print the audit 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 file can be printed to an available printer configured on the computer.

3.6.2 Viewing and Downloading Log Files from the Web Interface

When using the web interface (see Section 7.1 for details on the web interface), the log file will be viewed on a web browser. There is a download icon on the browser that can be used to download the log file being viewed.



Audit Log

Vendor: Logicube
Product: ZXi-10G
Software Version: 2.0
Build Date: Jan 15, 2021 19:20:39 UTC
Unit Serial Number: 181069
Time (Local): 12:51:10 (EST -0500)
Date: Jan 20, 2021

Operation Parameters
Mode: DriveToDrive
Method: CleverClone
Resize Percentages: 0 0 0 100
Partition Types: 'ntfs' 'FAT32' '' 'ntfs'
Hash: SHA-256
Hash Enabled: True
Verify Hash: False
Unlock HPA: False
Unlock DCO/ACS3: False
Error Granularity: 1
Result: SUCCESS (1 of 1)
Duration: 00:04:58
Time at Completion: 12:56:08

Case Information
Case/File Name:
Case ID:
Examiner:
Evidence ID:
Case Notes:

Drive Information

Bay	Role	Serial	Model	RAID	HPA Start LBA	DCO/ACS3 Start LBA	Filesystem	Cipher	Cipher Mode	IV Gen
M1	S	D61807831E0B01069012	SPCC Solid State Disk		NA	NA	NA	NA	NA	NA

3.6.3 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.

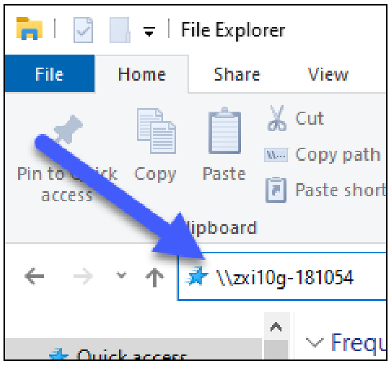
- If a log file deletion password was not created, a confirmation screen will appear confirming to delete the single log file or all log files.
- If a log file deletion password was created, a screen will appear prompting to enter the log file deletion password. Enter the log file deletion password. 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.

3.6.4 Accessing the Logs Over a Network

The log files can also be accessed through a network on a computer if the ZXi-10G is connected to the same network.

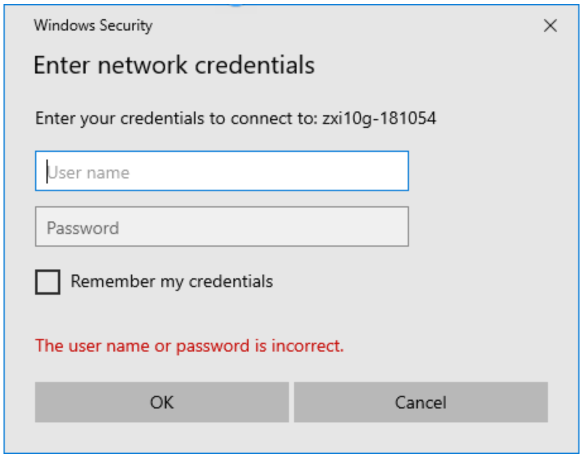
1. Open Windows Explorer or a similar window and browse to the hostname or the IP address found in the Statistics screen. Use two backslashes before the hostname or IP address as seen below. See Section 5.7 for more information on the Statistics screen.



\\zxi10g-181054

2. A Windows security screen will appear prompting to enter a User name and Password to connect to the ZXi-10G. Login with the following credentials:

- User name: *it*
- Password *it*



Windows Security

Enter network credentials

Enter your credentials to connect to: zxi10g-181054

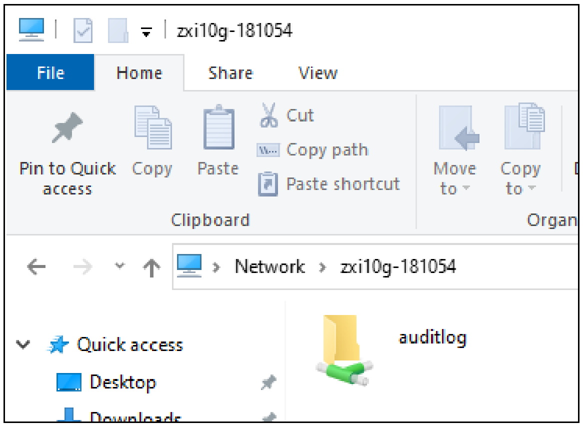
User name

Password

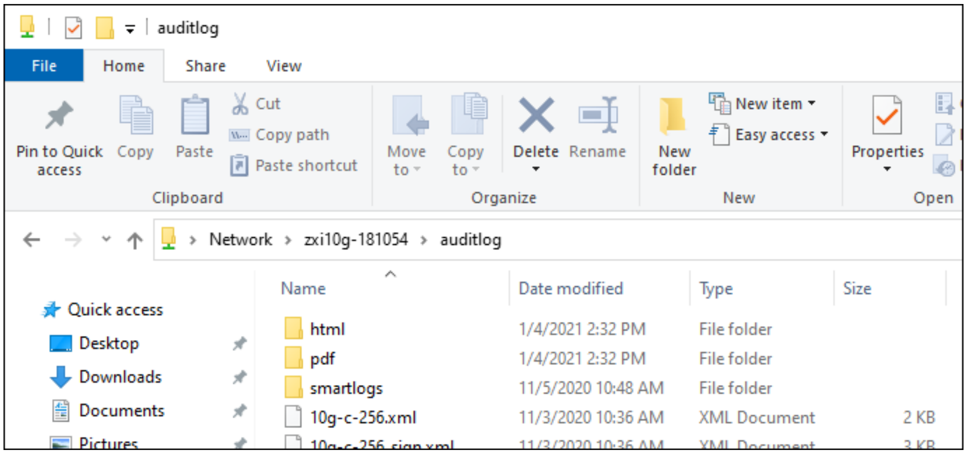
□ Remember my credentials

The user name or password is incorrect.

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



4. The auditlog folder contains the HTML, PDF, S.M.A.R.T., and XML files for each of the log files. The html and pdf folders contain the HTML and PDF 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.



Name	Date modified	Type	Size
html	1/4/2021 2:32 PM	File folder	
pdf	1/4/2021 2:32 PM	File folder	
smartlogs	11/5/2020 10:48 AM	File folder	
10g-c-256.xml	11/3/2020 10:36 AM	XML Document	2 KB
10g-c-256_sign.xml	11/3/2020 10:36 AM	XML Document	3 KB

3.7 Statistics

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

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

- About – This screen will show information about the ZXi-10G including the current software installed. Additionally, a QR code can be found on this page. When the QR code is scanned on a device connected to the same network the ZXi-10G is connected to, it will open a web browser to the ZXi-10G's IP address to access the web interface.

- *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 ZXi-10G.
- 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).
- Debug Logs – Allows the export of debug logs for Logicube technical support purposes.
- Help – Contains a QR code linking to the user's manual.

3.8 Manage Repositories

Repositories can be added to the ZXi-10G in this operation. Repositories can be drives connected to the Target ports of the ZXi-10G (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 ZXi-10G:

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.*

- Interfaces – This allows the configuration of the network interface which includes setting a static IP address and allows certain network services to be enabled or disabled.
- HTTP Proxy – For the ZXi-10G 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 a password.
- Network Configurations – Allows changes to the ZXi-10G's hostname and NTP server list.
- HTTPS – View, select, upload, or generate HTTPS certificates for secure remote access.

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 ZXi-10G: From the web using a network connection (with internet access) 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 5.12: Power Off*.

POWER OFF – The ZXi-10G can be remotely turned off or restarted by going to this tab. Additionally, the ZXi-10G's screen can be refreshed.

DRIVE POWER – Inactive drives connected to the ZXi-10G can be set to go to standby mode in this tab. The default is set to 0 minutes (OFF).

4: Cloning

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.

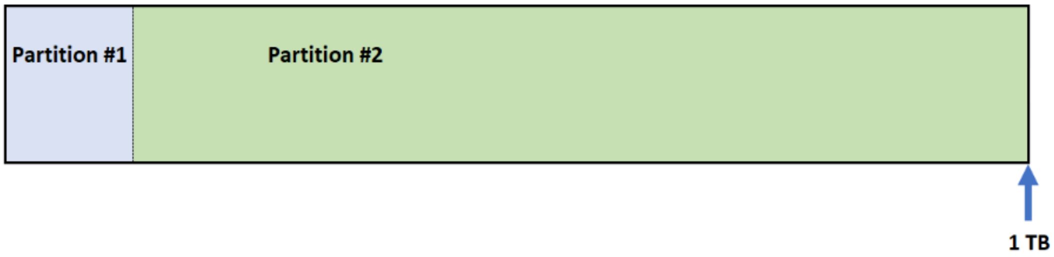
If the Master drive is larger in capacity than any Target drive, it is still possible to clone the drive, but some adjustments will need to be made to the Master drive. The following applies to any Operating System:

- 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.

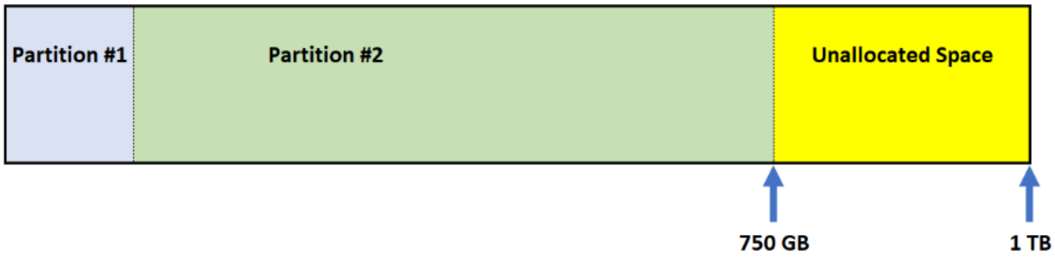
⚠ Before making any changes to the Master drive, it is highly recommended to make a backup copy of the Master drive by performing a Mirror copy of the drive to make sure there is an exact duplicate backup of the Master drive.

ℹ 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.

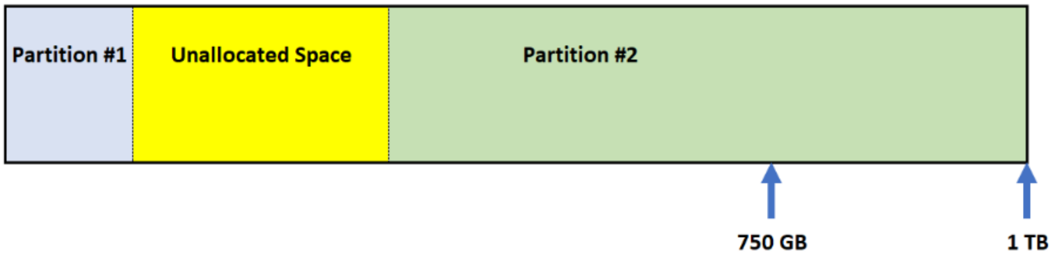
Sample original drive (1 TB drive):



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, they 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-10G 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-by-bit clone of a drive, the Target drive (including the BitLocker encrypted partition) will be an exact duplicate of the Master drive.

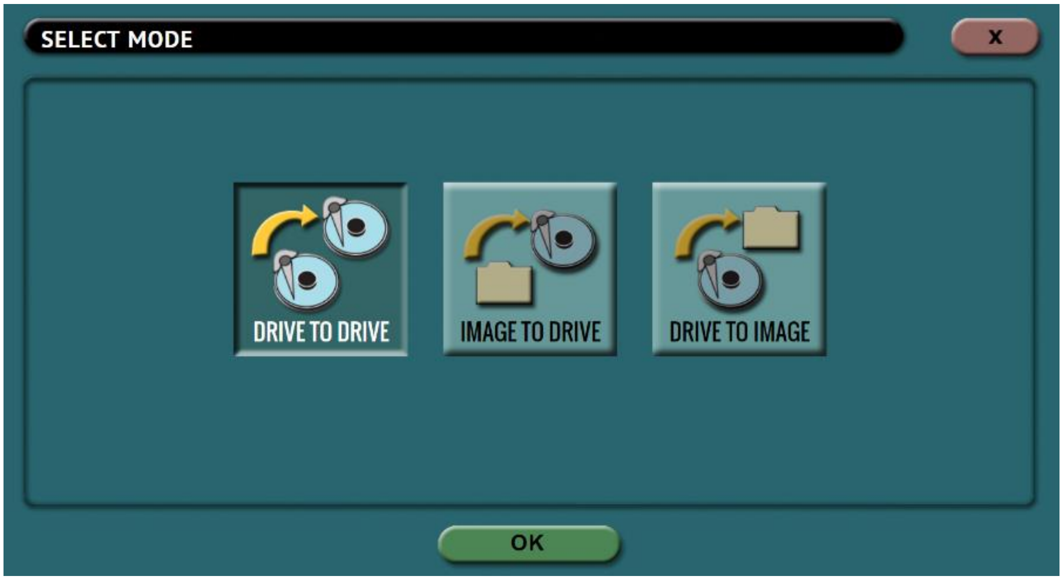
Clever – Using Clever, partitions can be resized. However, when cloning BitLocker encrypted drives, it is highly recommended to keep the BitLocker encrypted partition size the same as the Master (do not resize the BitLocker encrypted partition).

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 and BitLocker has been decrypted, the partitions can be resized to a larger size.

4.1 Mode

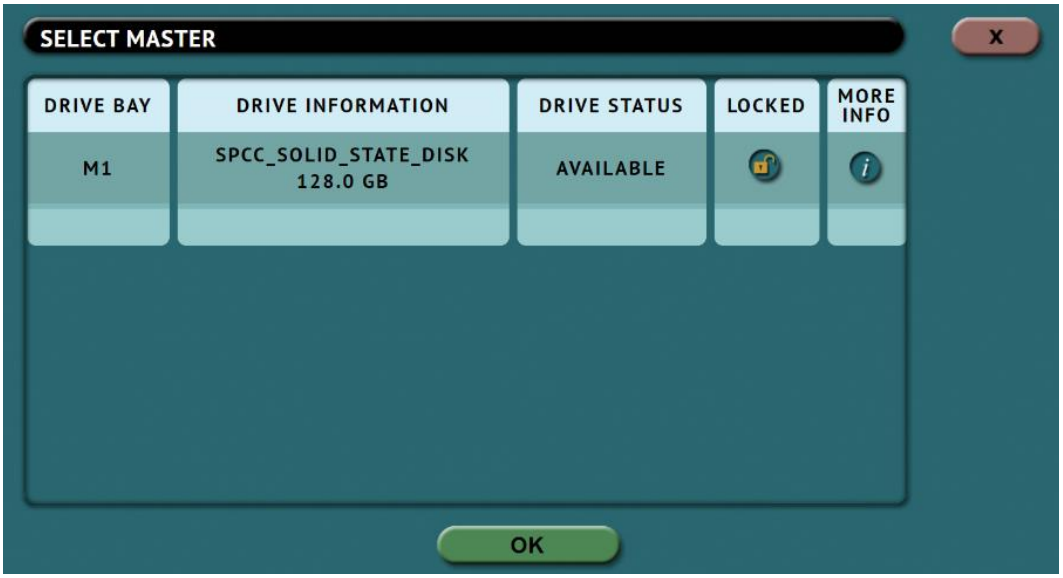
Tap this icon to choose between the following imaging modes:



- Drive to Drive – Clones one Master drive to one or more Target drives.
- Image to Drive – Restores a ZXi-10G 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).



DRIVE BAY	DRIVE INFORMATION	DRIVE STATUS	LOCKED	MORE INFO
M1	SPCC_SOLID_STATE_DISK 128.0 GB	AVAILABLE	🔓	ⓘ

When *Image to Drive* mode is selected, the Image File window will list all available drives that may contain ZXi-10G 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 (*Section 4.3.1*).
- HPA/DCO – Available in the following modes (*Section 4.3.2*):
  - Drive to Drive
  - Drive to Image
- Error Handling – Available in all modes (*Section 4.3.3*).
- Hash/Verification Method – Available in all modes (*Section 4.3.4*). Hash Method is not available in Image to Drive.
- File Image Method Settings – Available in Drive to Image mode (*Section 4.3.5*).
- Clone Method Settings – Available in the following modes (*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 *Job Name* field to underscores "_" when creating the log or file names.
>
> POSIX portable characters are:
> Uppercase A to Z
> Lowercase a to z
> Numbers 0 to 9
> Period (.)
> Underscore (_)
> 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 – If supported by the drive, HPA is set with the SET MAX ADDRESS command. The Host Protected Area is an area of a drive that is normally not visible to an Operating System, BIOS, or the user.

DCO – If supported by the drive, DCO is typically set by using the DCO MODIFY or DEVICE CONFIGURATION SET command. The Device Configuration Overlay limits the size of a drive only. For example, a 160GB drive can be made to look like a 100GB drive to a computer. Like HPA, this hidden area is normally not visible to an Operating System, BIOS, or the user.

ACS3 – If supported by the drive, this is set using the ACCESSIBLE MAX ADDRESS command as specified by the ATA/ATAPI Command Set. This is the maximum LBA that is accessible by read commands and write commands that return command completion without error.

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 are 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 during the cloning process.

> 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, 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 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.

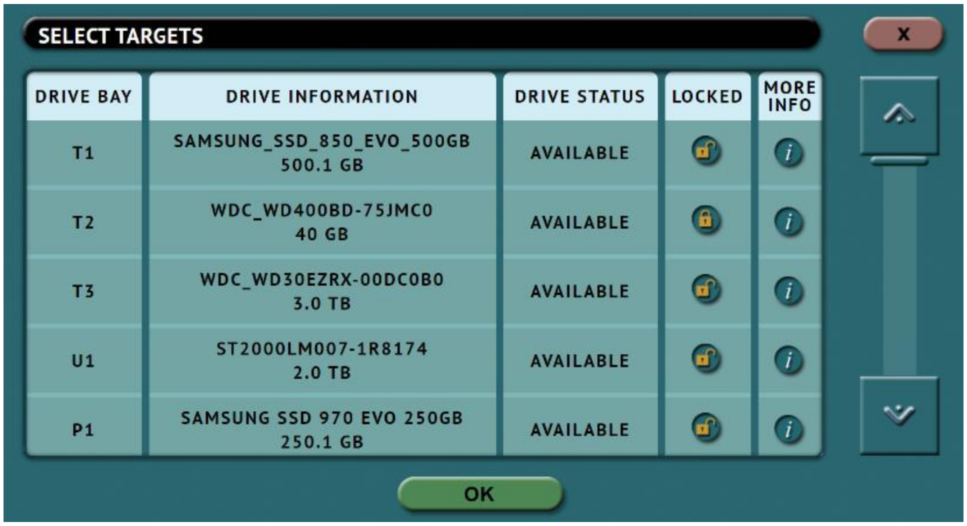
> It is recommended that all System Restore, Recovery, and OEM partitions should not be expanded. Setting the slider/percentage to 0% will instruct the unit to keep the same partition size.

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-10G. 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-10G'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).



SELECT TARGETS

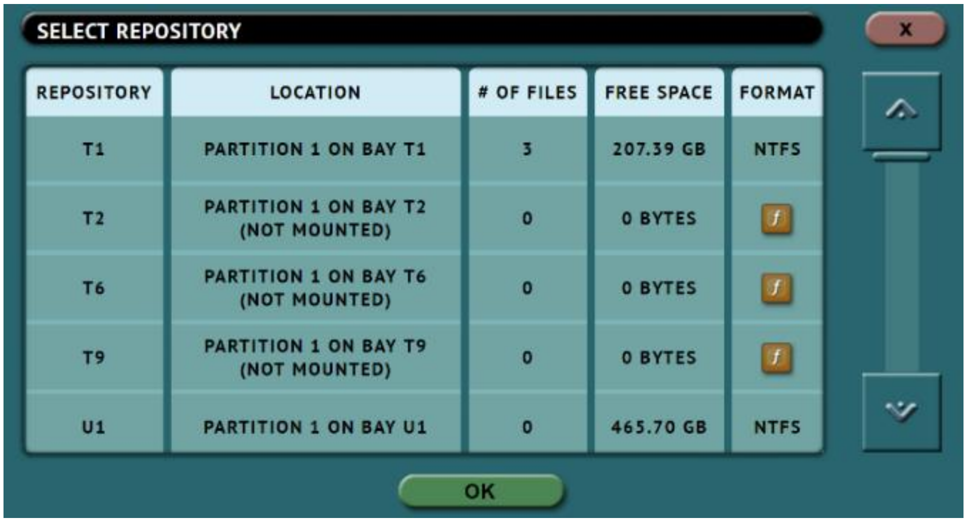
DRIVE BAY	DRIVE INFORMATION	DRIVE STATUS	LOCKED	MORE INFO
T1	SAMSUNG_SSD_850_EVO_500GB 500.1 GB	AVAILABLE	🔓	ⓘ
T2	WDC_WD400BD-75JMC0 40 GB	AVAILABLE	🔒	ⓘ
T3	WDC_WD30EZRX-00DC0B0 3.0 TB	AVAILABLE	🔓	ⓘ
U1	ST2000LM007-1R8174 2.0 TB	AVAILABLE	🔓	ⓘ
P1	SAMSUNG SSD 970 EVO 250GB 250.1 GB	AVAILABLE	🔓	ⓘ

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:

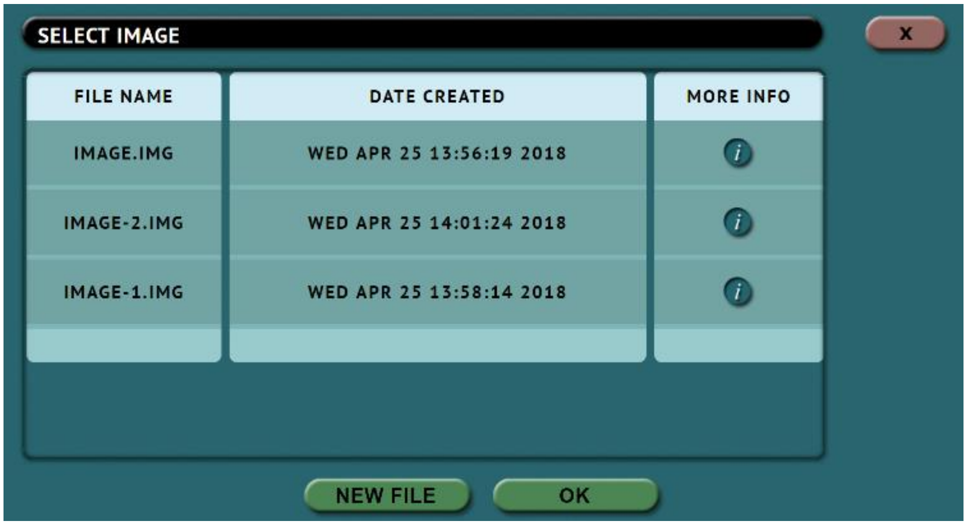
- An unformatted drive on T2, T6, and T9 that can be formatted to be used as a repository to store images (the ZXi-10G can format a drive using EXT4, NTFS, exFAT, or FAT32 for repository purposes)
- A formatted drive on T1 and U1 that can be used as a repository



SELECT REPOSITORY

REPOSITORY	LOCATION	# OF FILES	FREE SPACE	FORMAT
T1	PARTITION 1 ON BAY T1	3	207.39 GB	NTFS
T2	PARTITION 1 ON BAY T2 (NOT MOUNTED)	0	0 BYTES	f
T6	PARTITION 1 ON BAY T6 (NOT MOUNTED)	0	0 BYTES	f
T9	PARTITION 1 ON BAY T9 (NOT MOUNTED)	0	0 BYTES	f
U1	PARTITION 1 ON BAY U1	0	465.70 GB	NTFS

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.



SELECT IMAGE

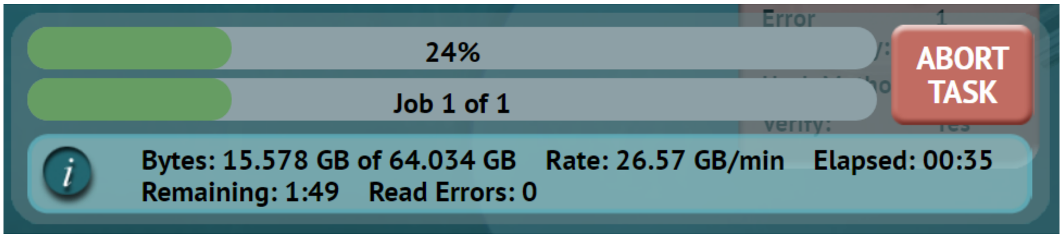
FILE NAME	DATE CREATED	MORE INFO
IMAGE.IMG	WED APR 25 13:56:19 2018	i
IMAGE-2.IMG	WED APR 25 14:01:24 2018	i
IMAGE-1.IMG	WED APR 25 13:58:14 2018	i

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).

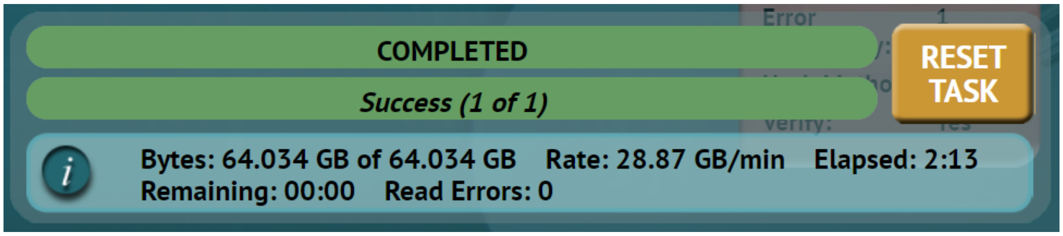


24%

Job 1 of 1

Bytes: 15.578 GB of 64.034 GB Rate: 26.57 GB/min Elapsed: 00:35
Remaining: 1:49 Read Errors: 0

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 do not show as being used or assigned for other tasks.



COMPLETED

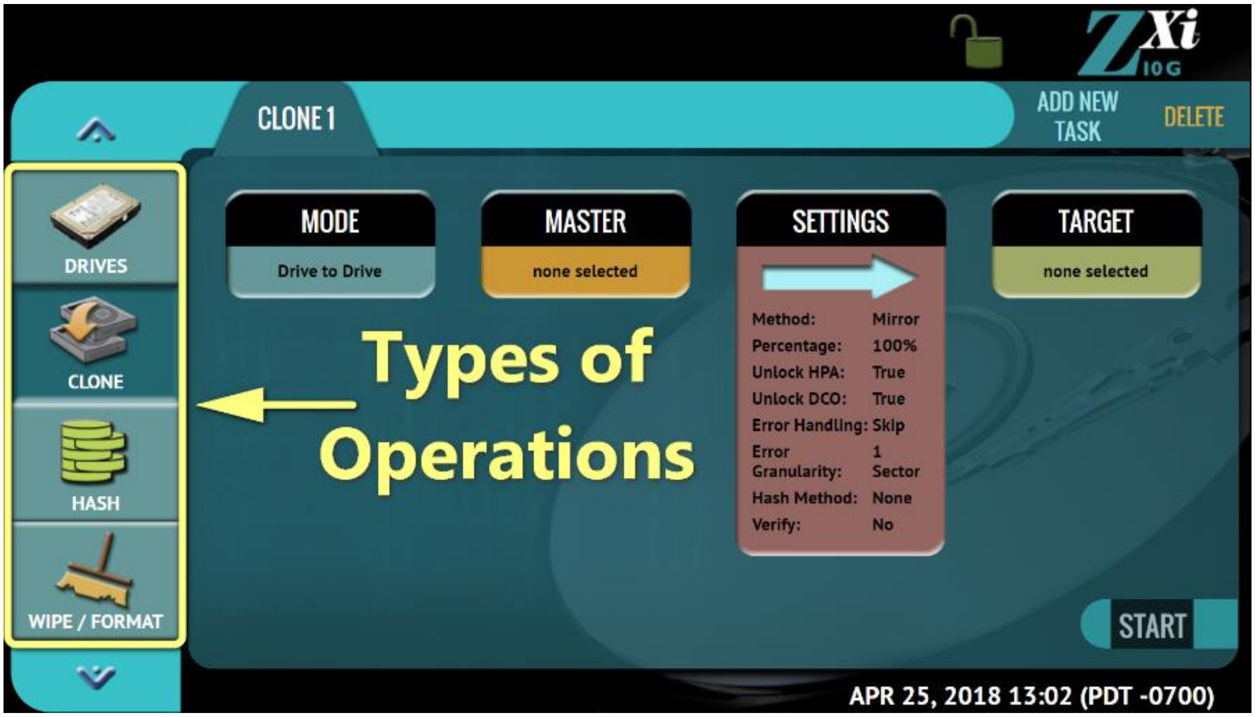
Success (1 of 1)

Bytes: 64.034 GB of 64.034 GB Rate: 28.87 GB/min Elapsed: 2:13
Remaining: 00:00 Read Errors: 0

5: Types of Operations

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.



Method: Mirror
Percentage: 100%
Unlock HPA: True
Unlock DCO: True
Error Handling: Skip
Error Granularity: 1 Sector
Hash Method: None
Verify: No

APR 25, 2018 13:02 (PDT -0700)

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).
    - Drive to Drive – Performs a bit-for-bit copy of the Master producing an exact duplicate of the Master drive.
    - Image to Drive – Restores an image created by the ZXi-10G to one or more Target drives.
    - Drive to Image – Creates a Logicube ZXi-10G 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 value 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:
     - NTFS
     - EXT4
     - EXFAT
     - FAT32
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 – View. Export, or delete logs of each cloning, hash, or wipe/format task that has been performed on the ZXi-10G.
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).
   - Debug Logs – Allows the export of debug logs for support purposes.
   - Help – Contains a QR code to scan, tap, or click that links to the user's manual.
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 – This allows the user to set ISCSI protocol settings.
9. SYSTEM SETTINGS – This mode allows changes to the system settings which include the following:
   - Profiles – This 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 on-screen menu and allows the change of the system's Time Zone.
- Bay Roles – This 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:
    - Interfaces – Edit TCP/IP and enable or disable certain network services.
    - HTTP Proxy – Set proxy settings (if required by the user's network).
    - Network Configurations - Change the ZXi-10G's hostname or NTP servers.
    - HTTPS – View, select, upload, or generate HTTPS certificates for secure remote access.
11. SOFTWARE UPDATES – Perform software and firmware updates on the unit. The 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.
    - PXEboot Update – This is reserved for future use.
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 on 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.

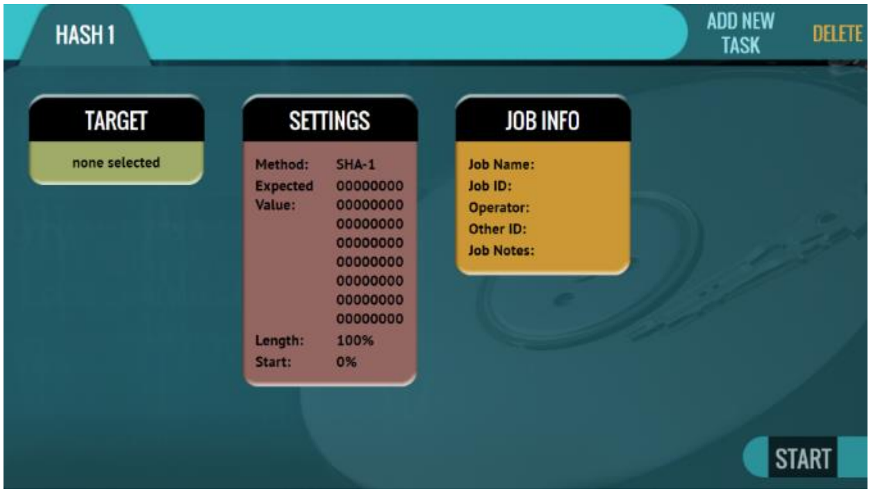
5.2 Clone

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*



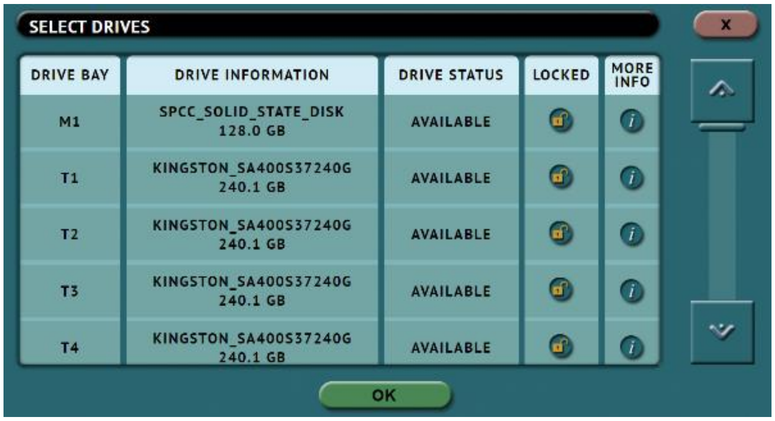
none selected

Method: SHA-1
Expected Value: 00000000
00000000
00000000
00000000
00000000
00000000
00000000
00000000
Length: 100%
Start: 0%

Job Name:
Job ID:
Operator:
Other ID:
Job Notes:

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*.

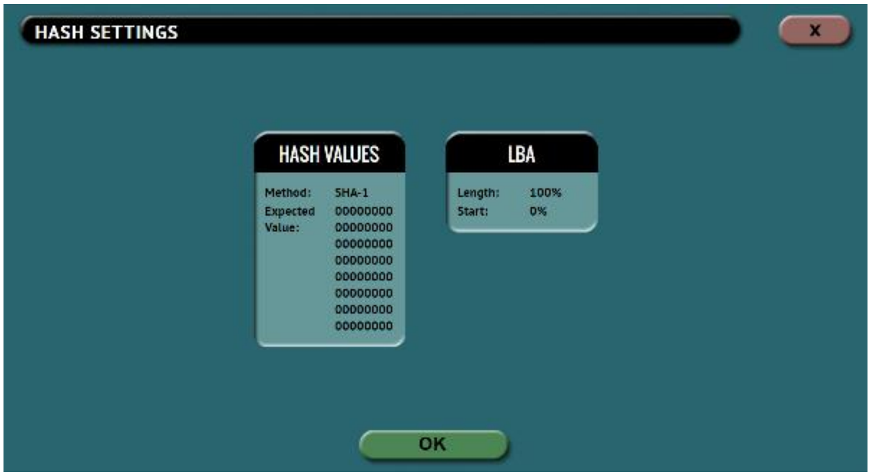


DRIVE BAY	DRIVE INFORMATION	DRIVE STATUS	LOCKED	MORE INFO
M1	SPCC_SOLID_STATE_DISK 128.0 GB	AVAILABLE	🔓	ⓘ
T1	KINGSTON_SA400S37240G 240.1 GB	AVAILABLE	🔓	ⓘ
T2	KINGSTON_SA400S37240G 240.1 GB	AVAILABLE	🔓	ⓘ
T3	KINGSTON_SA400S37240G 240.1 GB	AVAILABLE	🔓	ⓘ
T4	KINGSTON_SA400S37240G 240.1 GB	AVAILABLE	🔓	ⓘ

5.3.2 Settings

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

5.3.2.1 Hash Settings

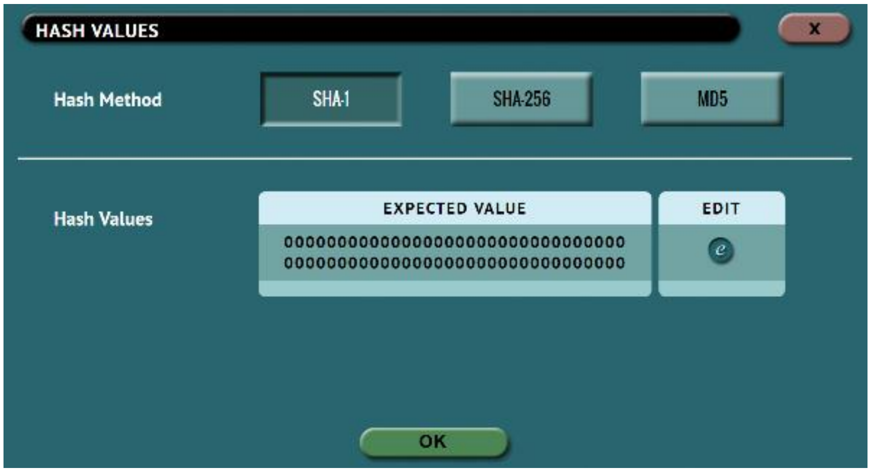


Method: SHA-1
Expected Value: 00000000
00000000
00000000
00000000
00000000
00000000
00000000
00000000
00000000

Length: 100%
Start: 0%

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.



00000000000000000000000000000000
00000000000000000000000000000000

5.3.2.1.1 Hash Method

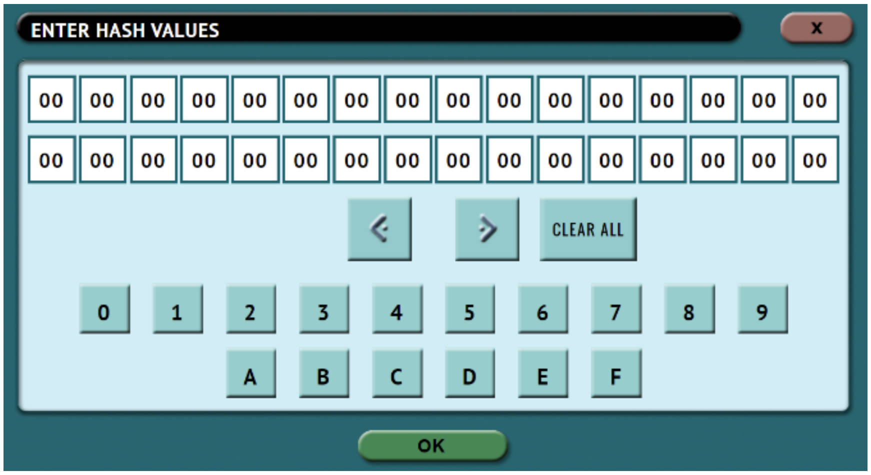
Select one of the following hash methods:

- 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 the calculated 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.



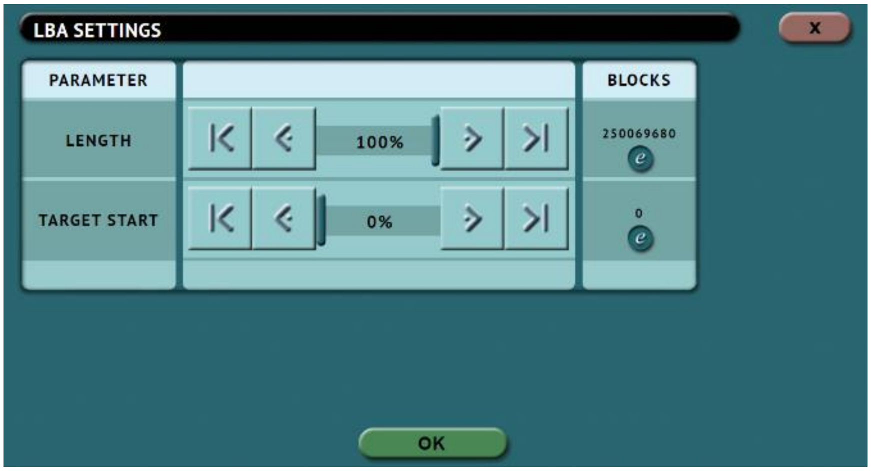
ENTER HASH VALUES

00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

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).



LBA SETTINGS

PARAMETER		BLOCKS
LENGTH	100%	250069680
TARGET START	0%	0

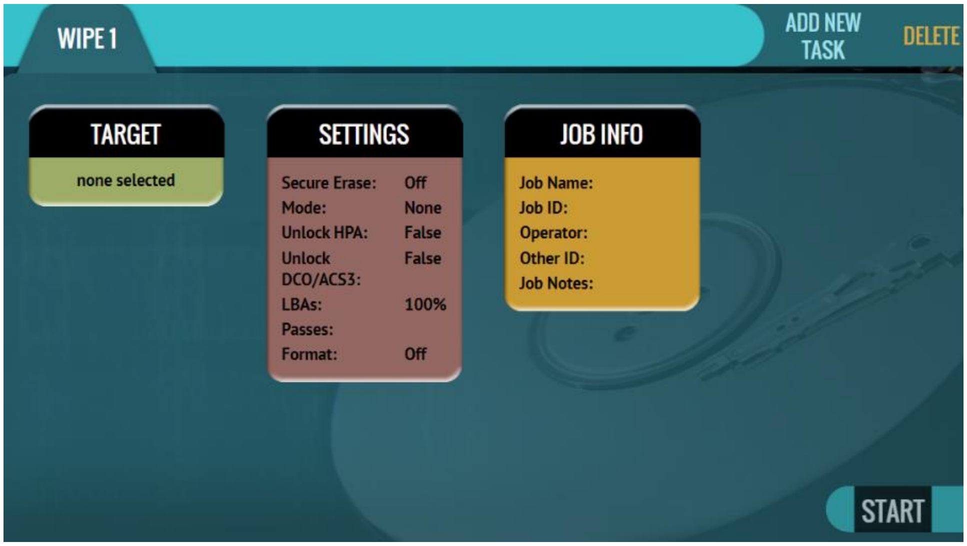
5.3.3 Job Info

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.



TARGET: none selected

SETTINGS

Secure Erase:	Off
Mode:	None
Unlock HPA:	False
Unlock DCO/ACS3:	False
LBAs:	100%
Passes:	
Format:	Off

JOB INFO

Job Name:
Job ID:
Operator:
Other ID:
Job Notes:

- 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.

  Secure erase will not work on drives connected through the USB or Thunderbolt ports, including NVMe SSDs.

- 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. The ZXi-10G can verify each pass value through a setting. Any HPA, DCO, or ACS3 can be unlocked and wiped in these settings.

- Format – Formats the Target drive with one of the following user-selectable file systems: NTFS, EXT4, exFAT, and FAT32.

  Drives used as a repository for the Drive to Image mode need to be formatted using the ZXi-10G.

The following selections are available when performing a wipe:

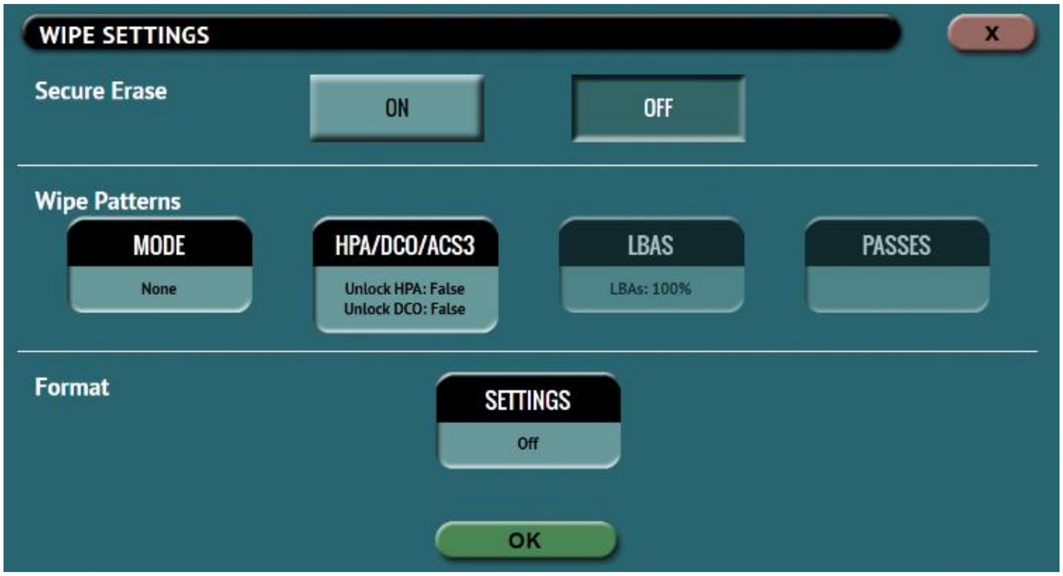
- Target
- Settings
- Job Info

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.



WIPE SETTINGS

Secure Erase: ON / OFF

Wipe Patterns

MODE: None

HPA/DCO/ACS3: Unlock HPA: False
Unlock DCO: False

LBAS: LBAs: 100%

PASSES

Format

SETTINGS: Off

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

> Each of the settings 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.

Additional Information on Secure Erase:

- For SAS (Serial Attached SCSI) drives, Secure Erase sends a ‘Format’ command.

- For SATA drives, Secure Erase sends a ‘Security Erase Unit’ command. If the SATA drives supports the ‘Enhanced Security Erase Unit’ command, the enhanced command will be sent.
- Since Secure Erase is controlled by the drive, for questions on how each drive supports these features, or what the drive will do with these commands, please contact the drive manufacturer.
- Secure Erase will not work on drives connected through the USB or Thunderbolt ports.

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.

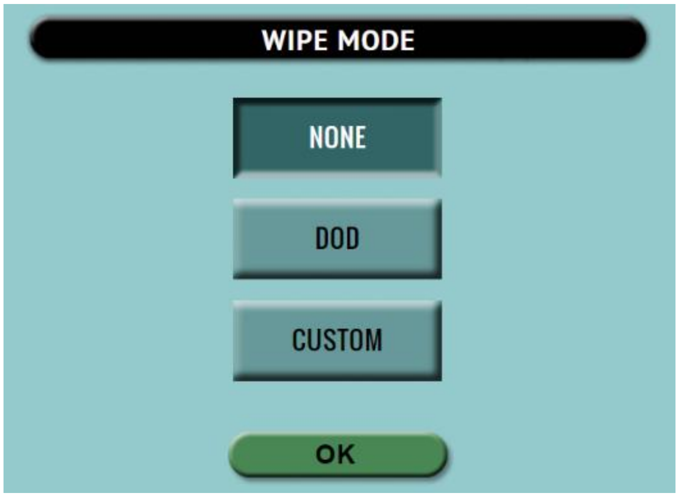
There are 4 selections when setting a wipe pattern:

- 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

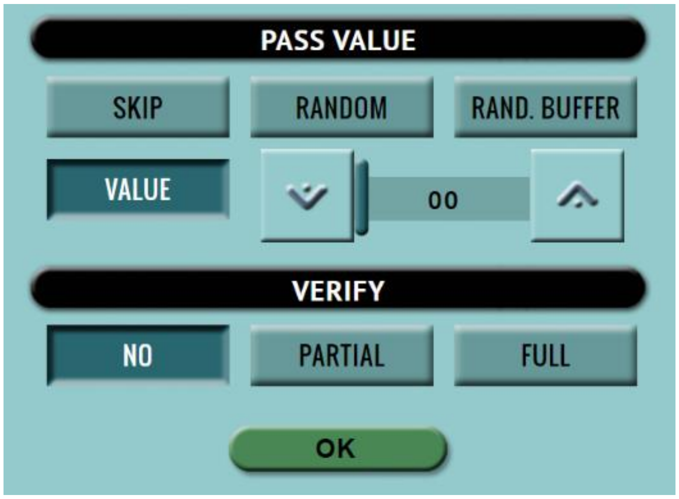
By default, this is set to 100% which will wipe all Logical Block Addresses (LBAs) and will wipe the entire drive (100%). The LBA count can be adjusted by tapping the *edit* icon.

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.
- RAND. 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.
- VERIFY – Select *YES* to verify each wipe pass value the unit performs.

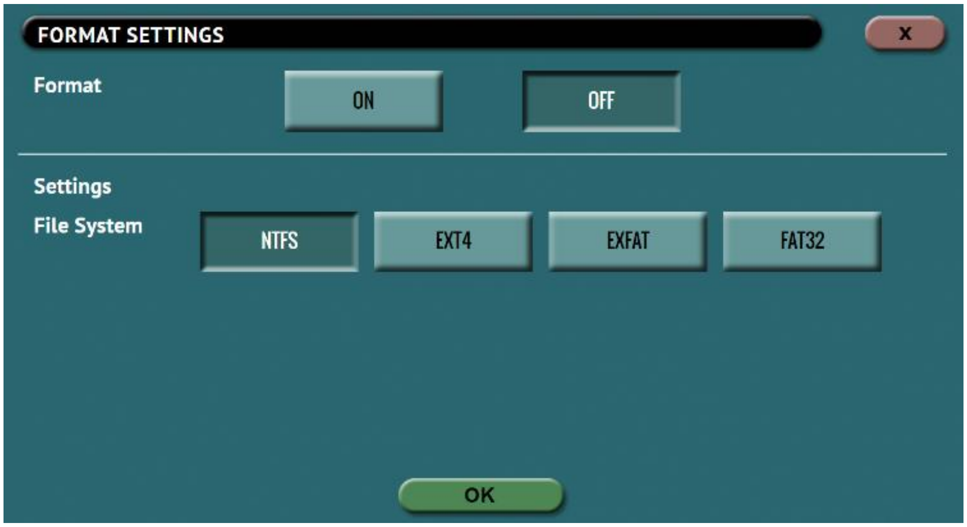
  When *Verify* is set to *YES*, the total time to wipe the drive could double if FULL is selected.

  - PARTIAL – Will take pseudorandom locations on the drive and verify the value that was written to those locations. When set, Partial verification will be used for drives over 16GB in capacity. If a drive used is 16GB or less in capacity, and Partial verification is used, full verification will be used.
  - FULL – A full verification of the wipe process will be performed. All values set to be written to the Target drive will be verified.

5.4.2.3 Format

Formats the Target using the NTFS, EXT4, exFAT, or FAT32 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. 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 from NTFS, EXT4, exFAT, or FAT32.

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.

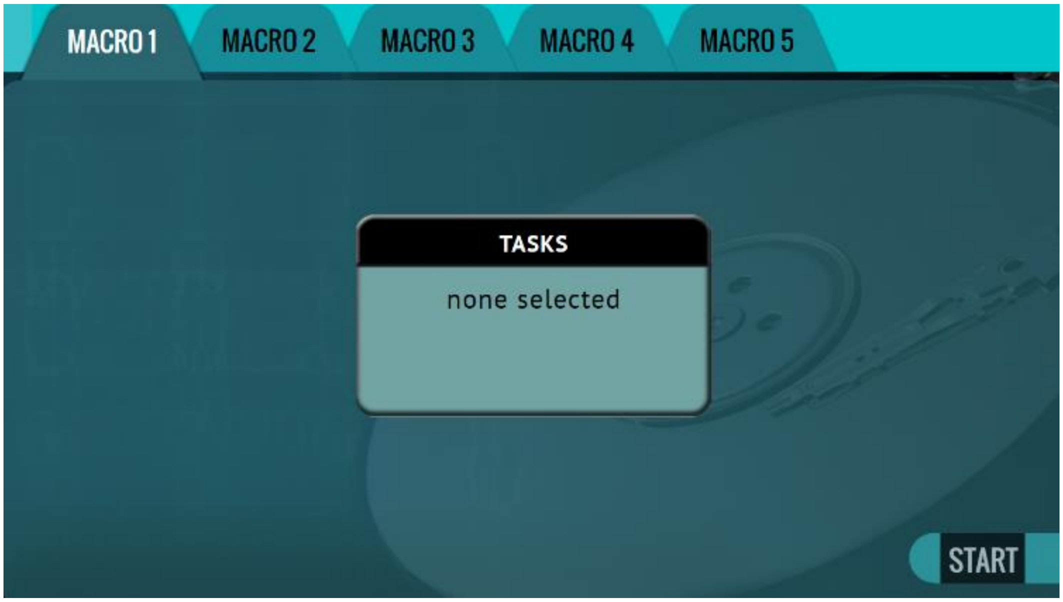
Information entered here will appear in the logs. More information on the Job Info screen can be found in *Section 4.3.1*.

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) have 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

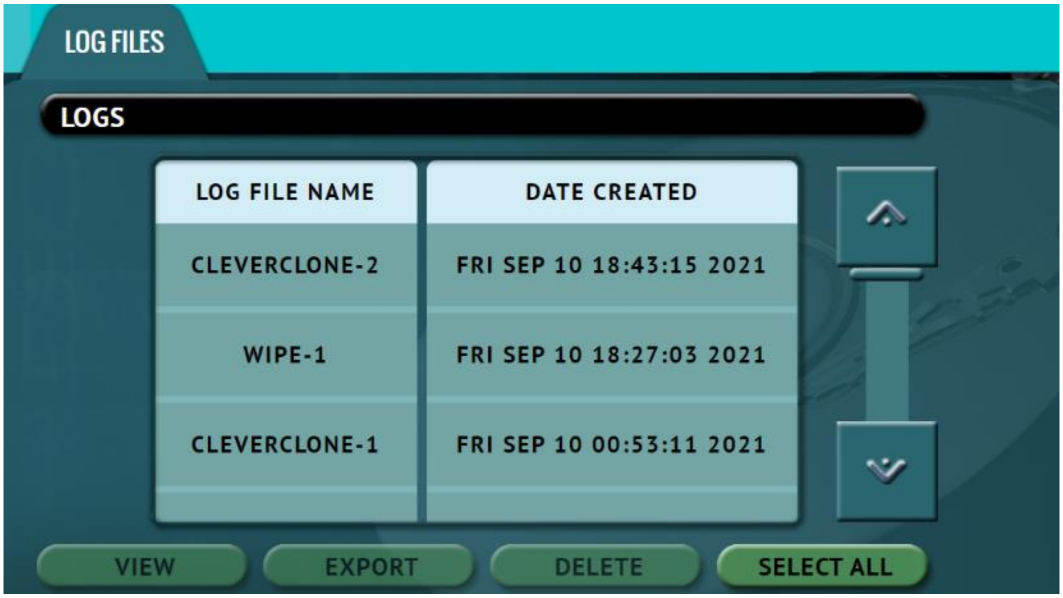
To set a macro to perform a Wipe using Secure Erase on T1, immediately followed by performing a Drive to Drive Clone from M1 to the newly wiped (secure erased) T1, the Wipe and Imaging Tasks first need to be set up.

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

Audit 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.



LOG FILE NAME	DATE CREATED
CLEVERCLONE-2	FRI SEP 10 18:43:15 2021
WIPE-1	FRI SEP 10 18:27:03 2021
CLEVERCLONE-1	FRI SEP 10 00:53:11 2021

Software v2.0 adds S.M.A.R.T. data logs for drives used in any *Clone*, *Hash*, or *Wipe* operation.

Two files will be exported, "pre" and "post", capturing S.M.A.R.T. data at the beginning of the task and the end of the task. S.M.A.R.T. logs are located in the smartlogs subfolder and can be retrieved by following the instructions in *Section 3.6.4*.

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

Audit 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

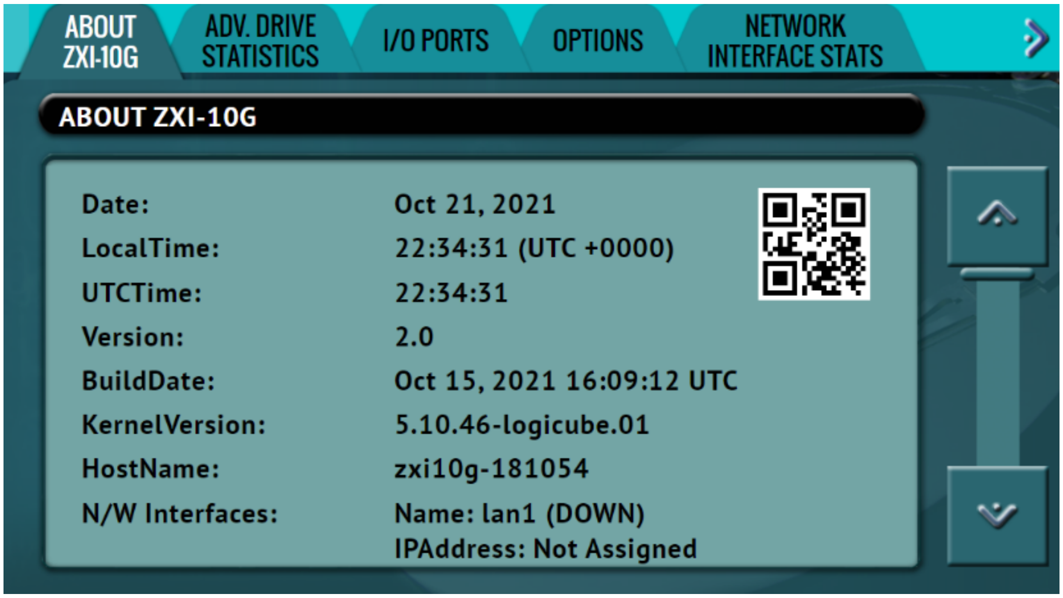
See *Section 3.6.1* for instructions on how to export the log files.
See *Section 3.6.2* for instructions on how to delete the log files.
See *Section 3.6.3* for instructions on how to access the logs over a network.

5.7 Statistics

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

5.7.1 About Screen

The *About* screen will show information about the ZXi-10G including the current software installed, hostname, and IP address. There is a QR code that can be scanned on a phone or tablet. If the phone or tablet is connected to the same network the ZXi-10G is connected to, it will open a web browser and connect to the IP address or hostname of the ZXi-10G.

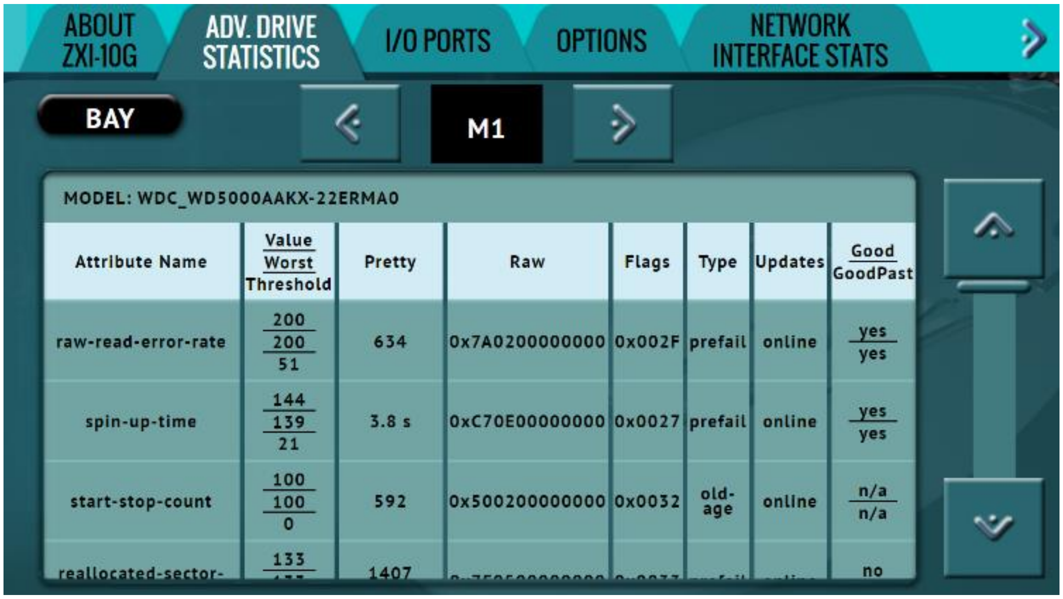


ABOUT ZXI-10G

Date: Oct 21, 2021
LocalTime: 22:34:31 (UTC +0000)
UTCTime: 22:34:31
Version: 2.0
BuildDate: Oct 15, 2021 16:09:12 UTC
KernelVersion: 5.10.46-logicube.01
HostName: zxi10g-181054
N/W Interfaces: Name: lan1 (DOWN)
IPAddress: Not Assigned

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.

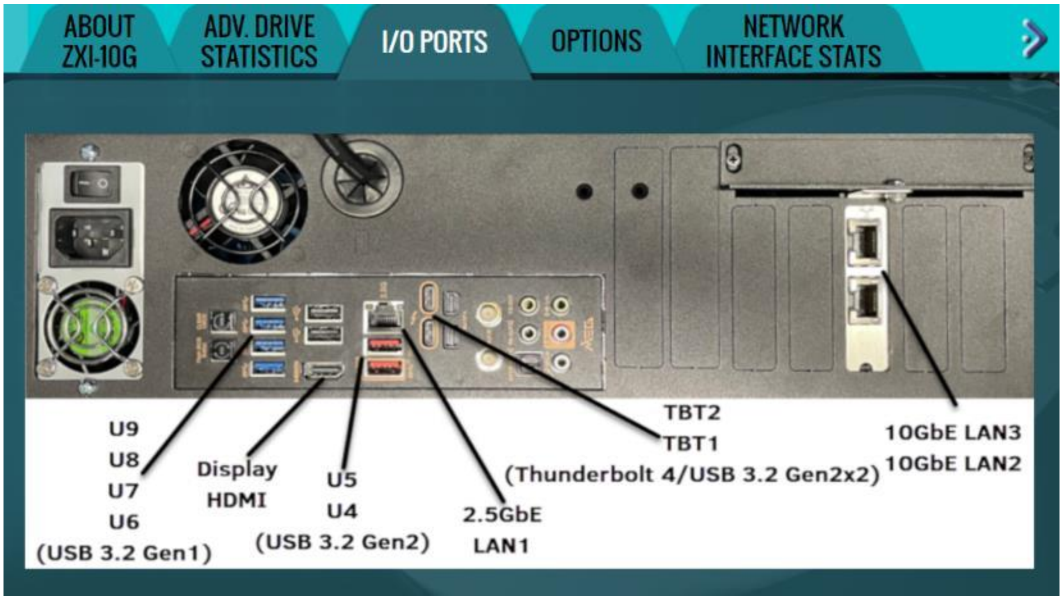


MODEL: WDC_WD5000AAKX-22ERMA0

Attribute Name	Value Worst Threshold	Pretty	Raw	Flags	Type	Updates	Good GoodPast
raw-read-error-rate	200 200 51	634	0x7A0200000000	0x002F	prefail	online	yes yes
spin-up-time	144 139 21	3.8 s	0xC70E00000000	0x0027	prefail	online	yes yes
start-stop-count	100 100 0	592	0x500200000000	0x0032	old-age	online	n/a n/a
reallocated-sector-	133	1407					no

5.7.3 I/O Ports

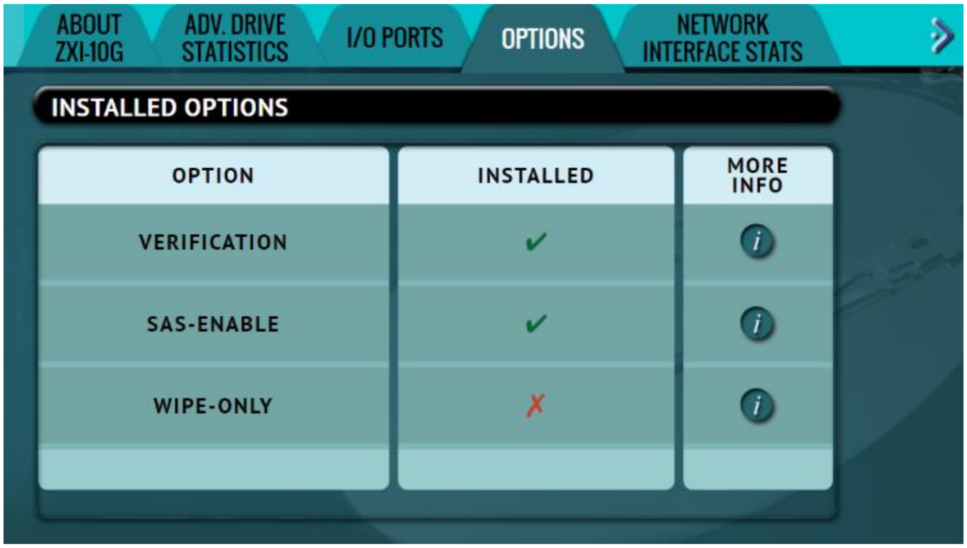
The *I/O Ports* tab displays a diagram of the input and output ports located in the back of the ZXi-10G.



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.

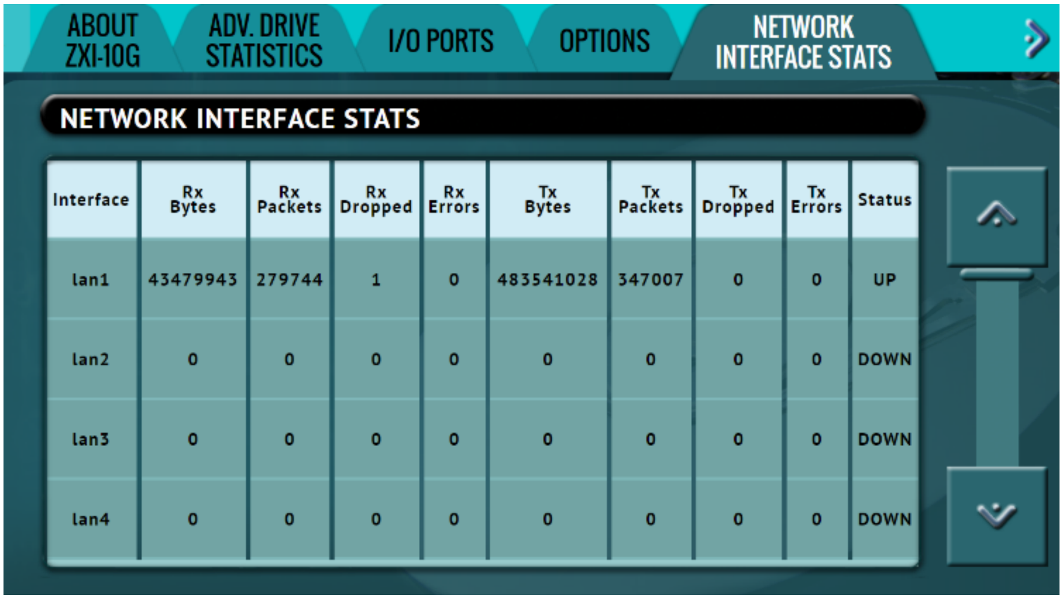


INSTALLED OPTIONS

OPTION	INSTALLED	MORE INFO
VERIFICATION	✓	ⓘ
SAS-ENABLE	✓	ⓘ
WIPE-ONLY	✗	ⓘ

5.7.5 Network Interface Stats

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



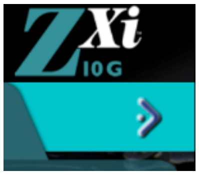
NETWORK INTERFACE STATS

Interface	Rx Bytes	Rx Packets	Rx Dropped	Rx Errors	Tx Bytes	Tx Packets	Tx Dropped	Tx Errors	Status
lan1	43479943	279744	1	0	483541028	347007	0	0	UP
lan2	0	0	0	0	0	0	0	0	DOWN
lan3	0	0	0	0	0	0	0	0	DOWN
lan4	0	0	0	0	0	0	0	0	DOWN

5.7.6 Debug Logs

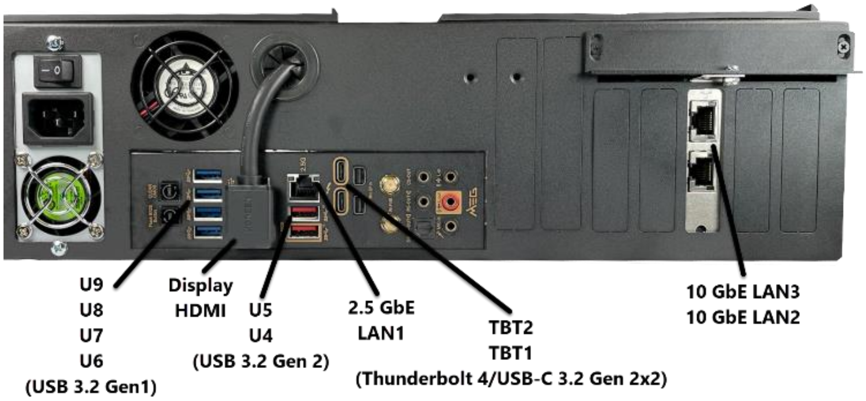
There may be times when Logicube Technical Support will ask for debug logs. This tab allows the user to export the debug logs to a USB flash drive (connected to the U9 or U10 port).

To access the Debug Logs tab in the System Settings screen, tap the right navigation arrow below the ZXi-10G logo (located on the top-right of the screen):

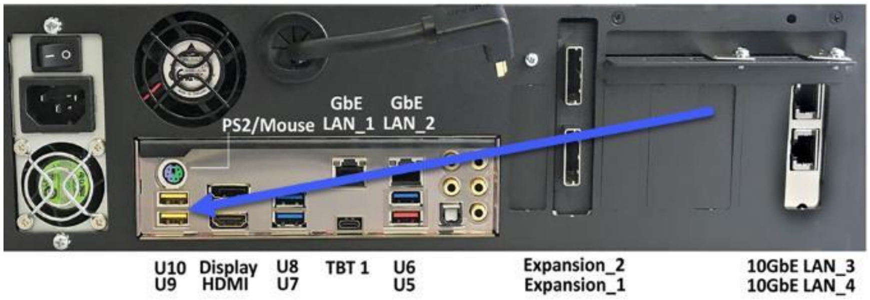


To export the debug logs:

1. The debug log files will be exported to a USB flash drive. The USB flash drive will need to be connected to one of the USB ports located in the rear panel of the ZXi-10G. The specific USB port is dependent on the I/O ports located in the rear panel of the ZXi-10G:
   a. If the rear I/O ports look like the image below, connect a formatted USB flash drive to the U9 USB port.



   b. If the rear I/O ports look like the image below, connect a formatted USB flash drive to the U9 or U10 USB port. Disconnect any other drive connected to U9 and U10.



1. Connect a formatted USB flash drive to the U9 (or U10 USB port, depending on the rear I/O ports above) located in the back panel of the unit.

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

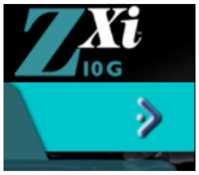
2. From the Debug Logs screen, tap *Export*.
3. The Debug Logs will be exported to the USB flash drive and can be zipped/compressed and sent to Technical Support.

5.7.7 Help

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

- From the touch screen (if the unit is connected to a network with Internet access), simply tap the QR code.
- Through a web browser, when using the web interface (see *Section 9.1* for more information on the web interface), click the QR code.
- Scan the QR code from a mobile phone or tablet that has internet access.

To access the Help tab in the System Settings screen, tap the right navigation arrow below the ZXi-10G logo (located on the top-right of the screen):



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

The following information is required to set up an SMB/CIFS repository:

- Path – Also called the Network Path (The IP address/Hostname and sharename).
- Domain – If the shared resource is in a domain. If not, use the workgroup name.
- Username – The username with full permissions to the shared resource (read and write access).
- Password – The password for the username.

The following information is required to set up an iSCSI repository:

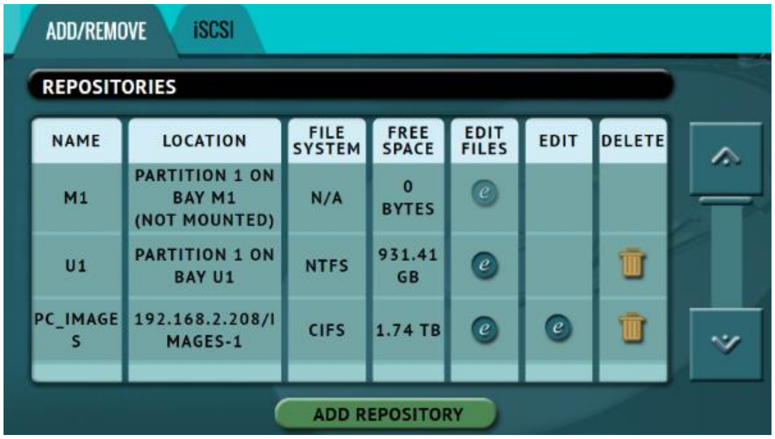
- Portal – The IP address or hostname of the iSCSI Target.
- Username – The username with full permissions to the shared resource (read and write access).
- Password – The password for the username.

> 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.

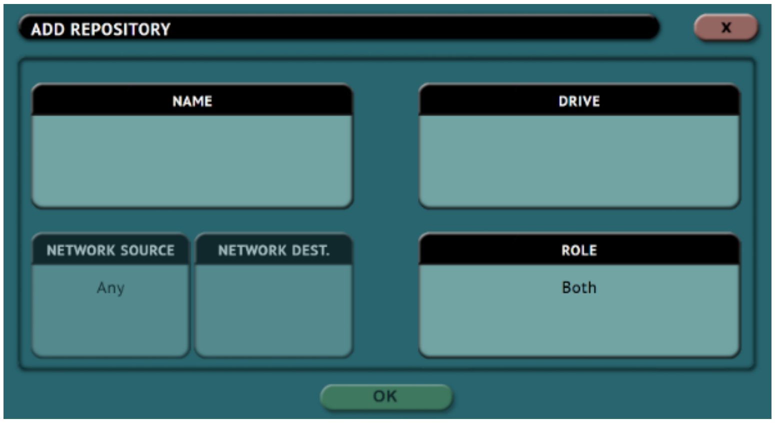
> If a repository location shows *(NOT MOUNTED)*, it is because the drive attached is not formatted by the unit or the unit cannot connect to the shared network resource.



REPOSITORIES

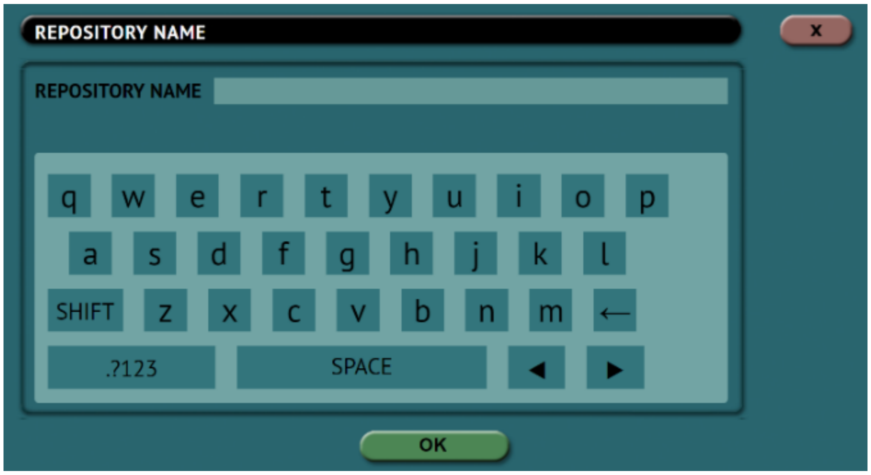
NAME	LOCATION	FILE SYSTEM	FREE SPACE	EDIT FILES	EDIT	DELETE
M1	PARTITION 1 ON BAY M1 (NOT MOUNTED)	N/A	0 BYTES	e		
U1	PARTITION 1 ON BAY U1	NTFS	931.41 GB	e		🗑
PC_IMAGES	192.168.2.208/IMAGES-1	CIFS	1.74 TB	e	e	🗑

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

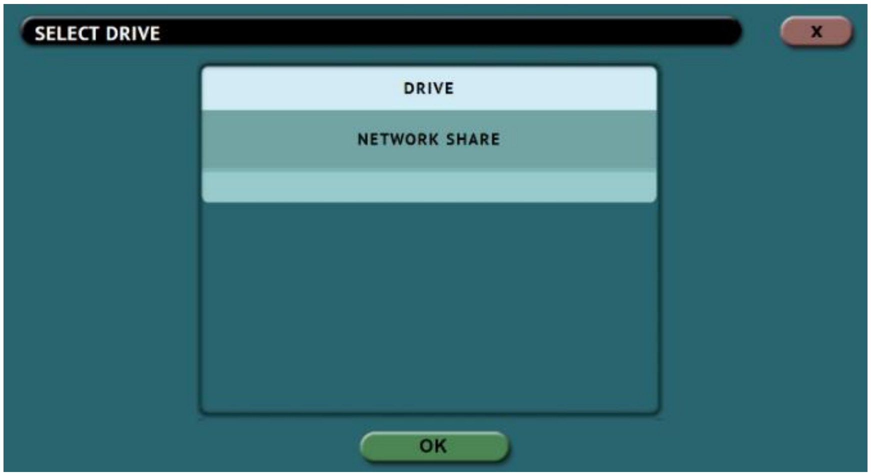


NETWORK SOURCE: Any
NETWORK DEST.:
ROLE: Both

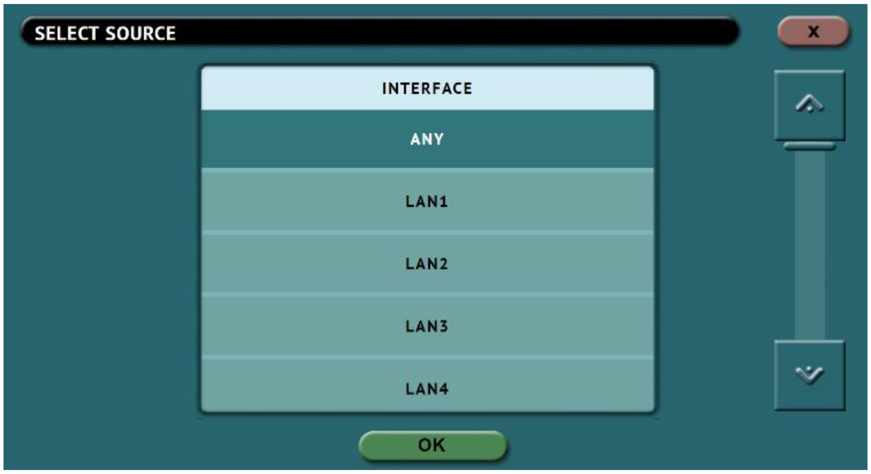
Tap *Name* to set the name of the repository. Tap the *OK* icon when finished.



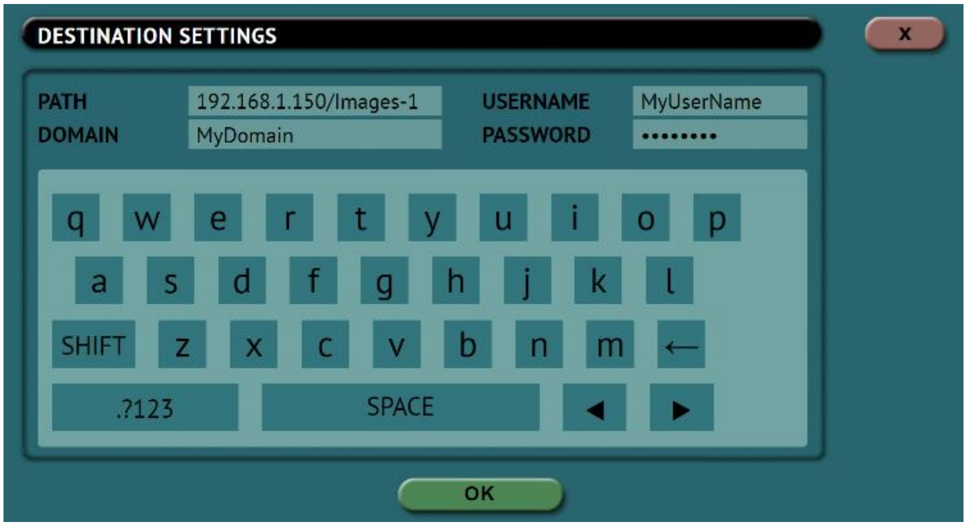
Tap *Drive* to select *network share* to set as a repository. Tap the *OK* icon when finished.



OPTIONAL: Tap *Network Source* to specify which network interface to use. By default, it is set to “Any”.



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



DESTINATION SETTINGS

PATH 192.168.1.150/Images-1

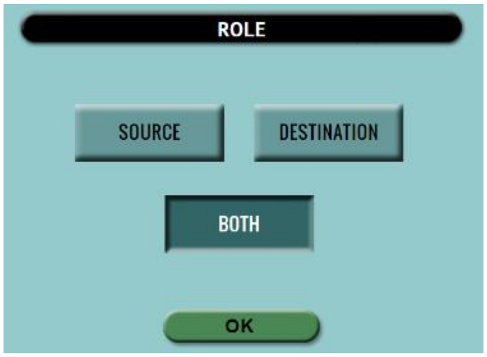
DOMAIN MyDomain

USERNAME MyUserName

PASSWORD ••••••••

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.



ROLE

5.8.1.2 Editing or Deleting/Removing a Repository

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

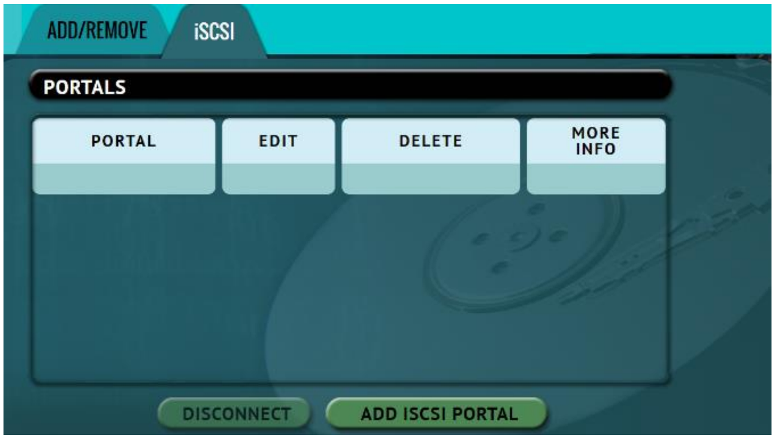
5.8.2 iSCSI

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

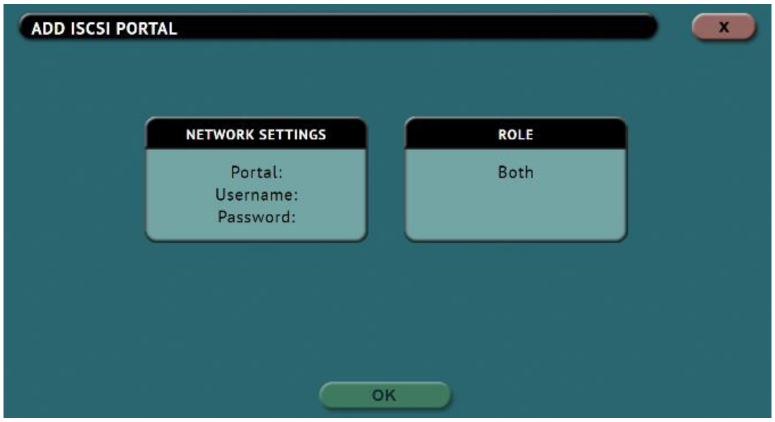
To add a repository using the iSCSI protocol, an iSCSI Target must be set up on the remote system. Since networks are configured differently, a Systems Administrator or Network Administrator may be needed to set up the iSCSI protocol.

Once the iSCSI Target has been setup:

1. Tap *Add iSCSI Portal*.

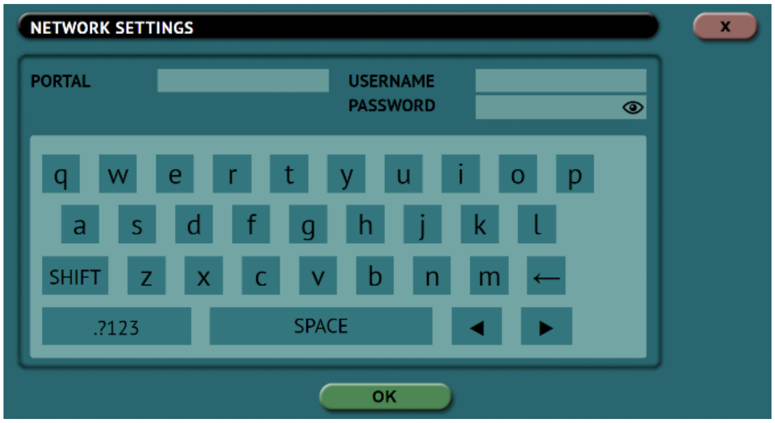


2. The *Add iSCSI Portal* window should appear:



ROLE: Both

3. Tap *Network Settings* and input the *Portal* (IP address or hostname), *Username*, and *Password*. Tap the *OK* icon when finished.



4. Optional: Tap *Role* and input the role for this repository.

5. Tap *OK* when finished. The screen will go back to the *Portals* screen.

6. In the *Portals* screen, tap the iSCSI portal to highlight it, then tap *Connect*.

7. The ZXi-10G will attempt to connect to the iSCSI target. If successful, a “connected” screen will appear. Tap *OK* to continue.

> Multiple iSCSI connections can be added. To disconnect an iSCSI connection, highlight the portal to disconnect, then tap *Disconnect*. To edit or delete an iSCSI connection, tap *Edit* or *Delete*.

5.9 System Settings

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

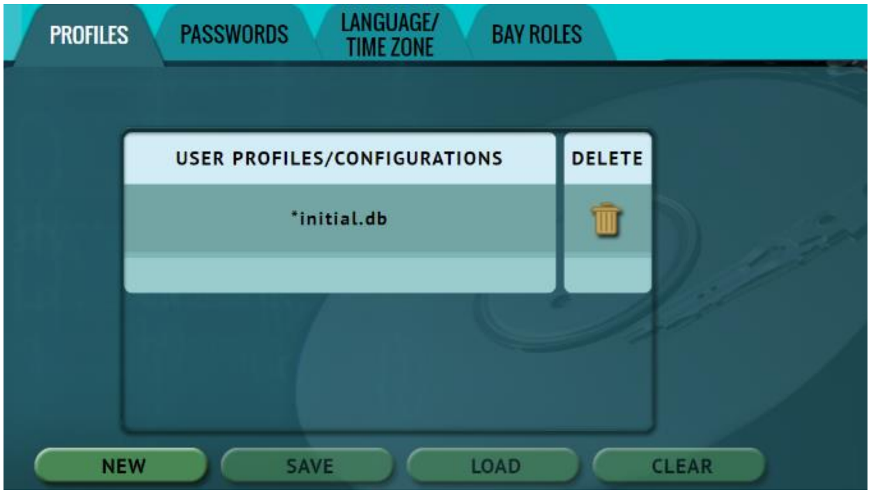
5.9.1 Profiles

> 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 on this screen:

- New – Allows the user to create a new profile name.
- Save – Saves the selected profile.
- Load – Loads the selected profile.
- Clear – Clears the selected profile of all saved settings and resets the profile to contain default settings. After clearing the selected profile, the profile will need to be saved to save any changes.

> With software version 2.0 and newer, settings and selections are now persistent through a reboot/power-off sequence. When the ZXi-10G is turned on, it will load all the previous settings and selections.



USER PROFILES/CONFIGURATIONS	DELETE
*initial.db	🗑

The asterisk (*) next to the profile name is the currently loaded profile.

After loading a profile, it is recommended to refresh the User Interface. This can be done one of several ways:

- From the touch screen, go to the POWER OFF menu and tap the *Refresh* button.

- If a web browser is used for remote operation, press the F5 key on the computer's keyboard or locate the *Refresh* icon on the browser.

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

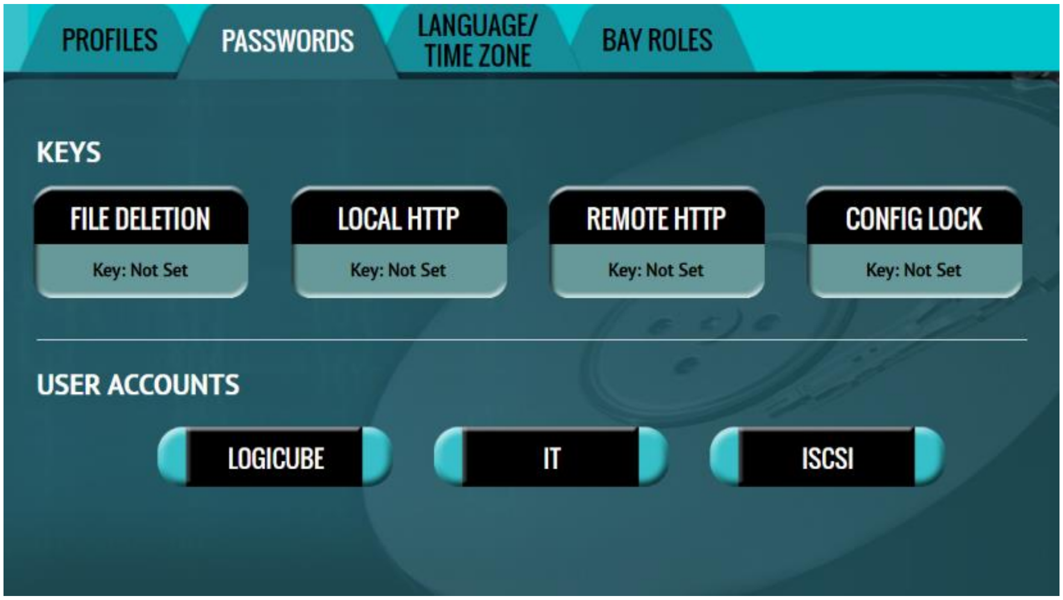
5.9.2 Passwords

There are seven keys or passwords that can be set or changed.

- Key: Log File Deletion – A key can be set as an extra layer of protection when deleting log files. If this key is set, a key prompt will appear, and the correct key must be entered before any log files can be deleted.
- Key: Local HTTP – A key can be set to lock the local touch screen on the unit. If this key is set, a key prompt will appear, and the correct key must be entered before allowing access to the local touch screen.

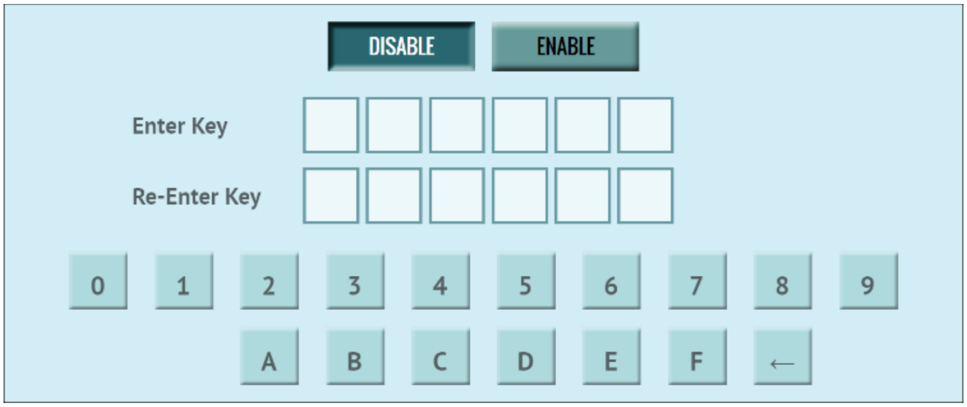
- Key: Remote HTTP – A key can be set to lock remote HTTP access (through a web browser). If this key is set, a key prompt will appear, and the correct key must be entered before allowing access through a web browser.
- Key: Config Lock – A key can be set to lock out any configuration changes. If this key is set, 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.
- User Account: LOGICUBE – Allows the user to change the *logicube* local account.
- User Account: IT – Allows the user to change the *it* local account.
- User Account: ISCSI – Allows the user to change the *iscsi* local account.



5.9.2.1 Setting Key Passwords

To set a key for *Log File Deletion, Local HTTP, Remote HTTP, or Config Lock*, tap one of the buttons. 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.

The *Auto Lock* button is available for the following keys:

- Local HTTP
- Remote HTTP
- Config Lock

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.

⚠

Remember the Config Lock Key! If the unit is configured to load a user profile with the Config Lock set to enabled and the password is forgotten, the only way to reset the Config Lock is to 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.

5.9.2.1.1 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.

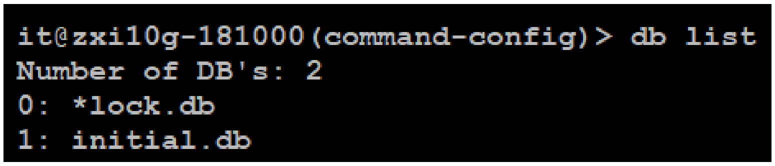
5.9.2.1.2 Forgotten Password for any Keys

If any of the keys are forgotten, the INITIAL.DB profile will need to be loaded using the Command Line Interface (CLI). See *Section 7.2* for more information on how to connect 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. Log in 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 configuration loaded each time the unit is turned on.



```
it@zxi10g-181000(command-config)> db list
Number of DB's: 2
0: *lock.db
1: initial.db
```

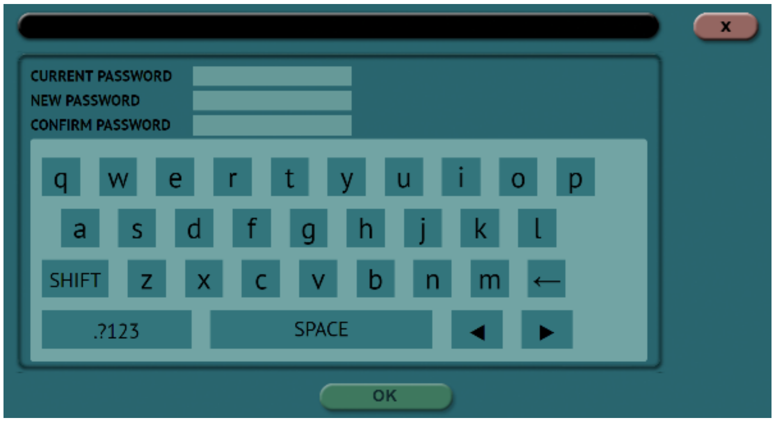
5. Type *db load initial.db* then press the Enter key to load the default database. There should be a response showing “Command (DbManagement) Successful”.
6. Type *db list* again and there should be an asterisk (*) on initial.db.
7. Turn the unit off using the power button, then close the Telnet/SSH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

5.9.2.2 User Account Passwords

This unit comes with the following built-in user accounts:

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

All user account passwords can be changed on this screen. To change the password for either account, tap either the *LOGICUBE*, *IT*, or *iSCSI* button. A screen will appear:



1. Enter the current password.

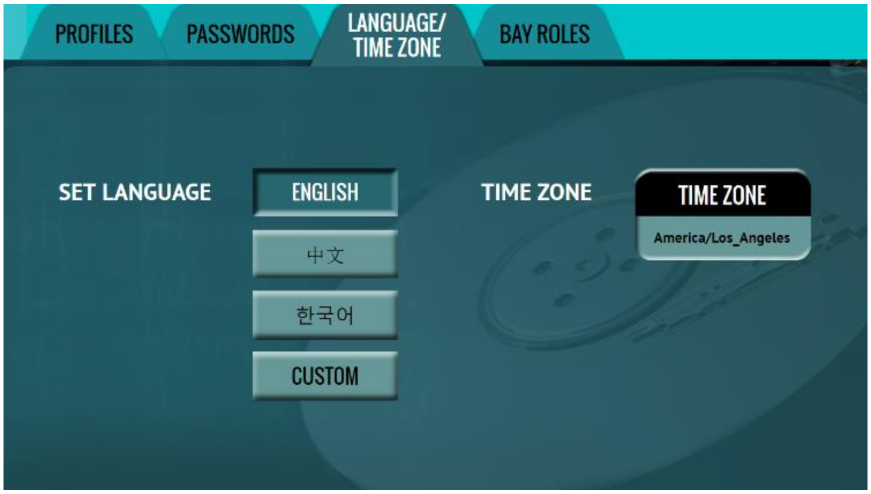
The default password for each account is:

LOGICUBE: logicube
IT: it
ISCSI: logicube@19755

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

The *User Account Passwords* do not need to be saved into a user profile. Changing any of these two passwords will take effect immediately. If the User Account password is forgotten, contact Tech Support assistance.

5.9.3 Language/Time Zone



TIME ZONE: America/Los_Angeles

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.

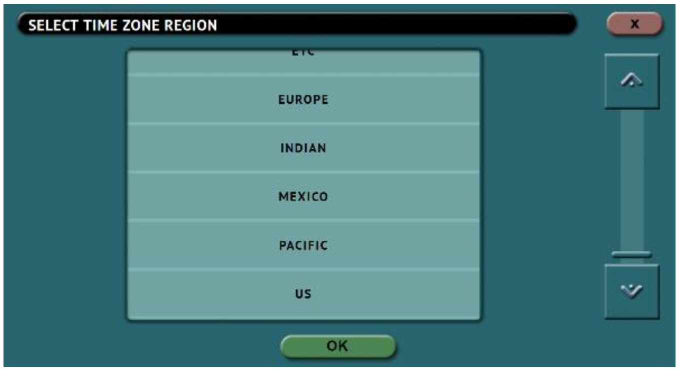
5.9.3.1 Language

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.

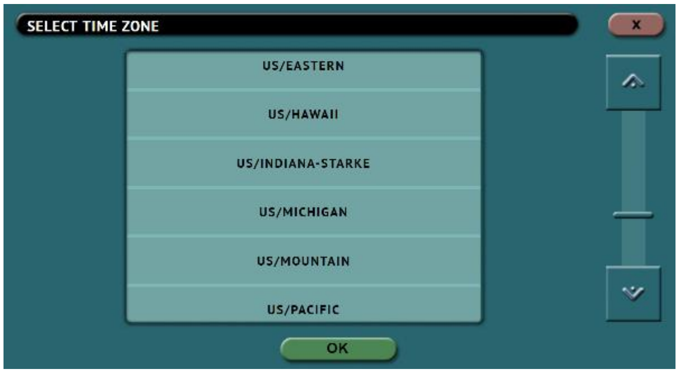
The *Custom* button is reserved for future language releases.

5.9.3.2 Time Zone

The ZXi-10G 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. To set the time zone, tap *Time Zone* to select the time zone region. Tap the *OK* icon to continue.

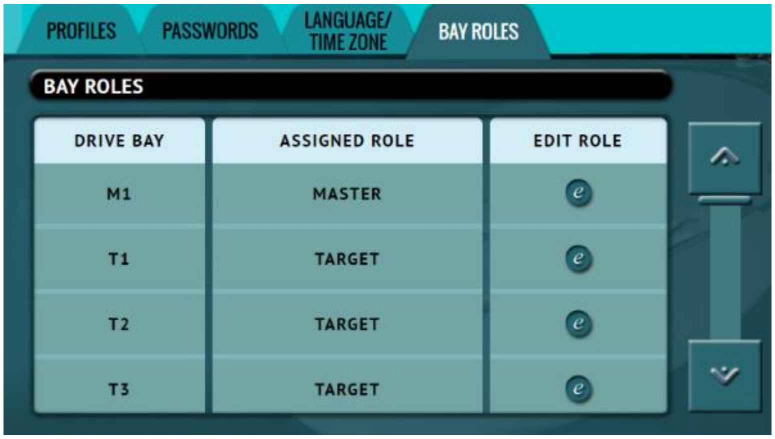


After selecting the region, select the desired time zone. Tap the *OK* icon to set the time zone.



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.



BAY ROLES

DRIVE BAY	ASSIGNED ROLE	EDIT ROLE
M1	MASTER	e
T1	TARGET	e
T2	TARGET	e
T3	TARGET	e

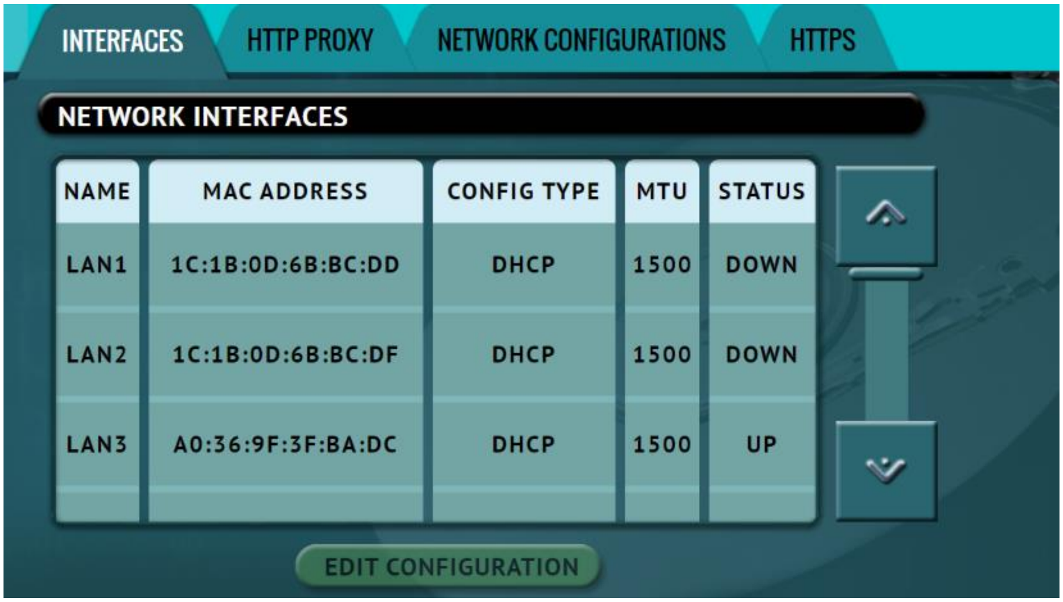
5.10 Network Settings

The Network Settings screen has the following tabs: *Interfaces*, *HTTP Proxy*, *Network Configurations*, and *HTTPS*.

5.10.1 Interfaces

The Interfaces tab displays the network interface information (MAC Address, Configuration type (DHCP or Static), MTU, and the link status. A static IP or DHCP can be set on this screen. This tab also allows and enabling or disabling certain network services. To edit the network interface configuration, tap the Ethernet adapter name then tap the *Edit Configuration* button.

There is a PXE button for future use.



NETWORK INTERFACES

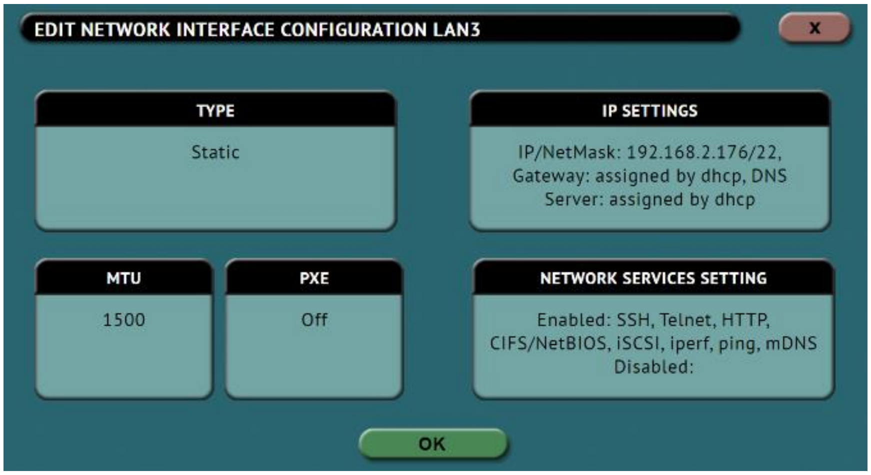
NAME	MAC ADDRESS	CONFIG TYPE	MTU	STATUS
LAN1	1C:1B:0D:6B:BC:DD	DHCP	1500	DOWN
LAN2	1C:1B:0D:6B:BC:DF	DHCP	1500	DOWN
LAN3	A0:36:9F:3F:BA:DC	DHCP	1500	UP

5.10.1.1 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 *Interfaces* tab, select the network interface to edit (LAN1, LAN2, or LAN3) then tap *Edit Configuration*. The *Edit Network Interface Configuration* screen should appear.

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



EDIT NETWORK INTERFACE CONFIGURATION LAN3

TYPE: Static

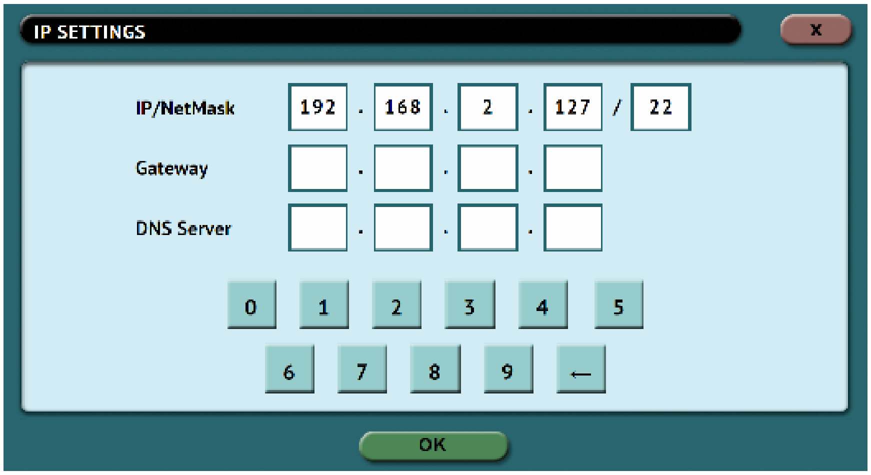
IP SETTINGS: IP/NetMask: 192.168.2.176/22, Gateway: assigned by dhcp, DNS Server: assigned by dhcp

MTU: 1500

PXE: Off

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

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


IP SETTINGS

IP/NetMask 192 . 168 . 2 . 127 / 22

Gateway . . .

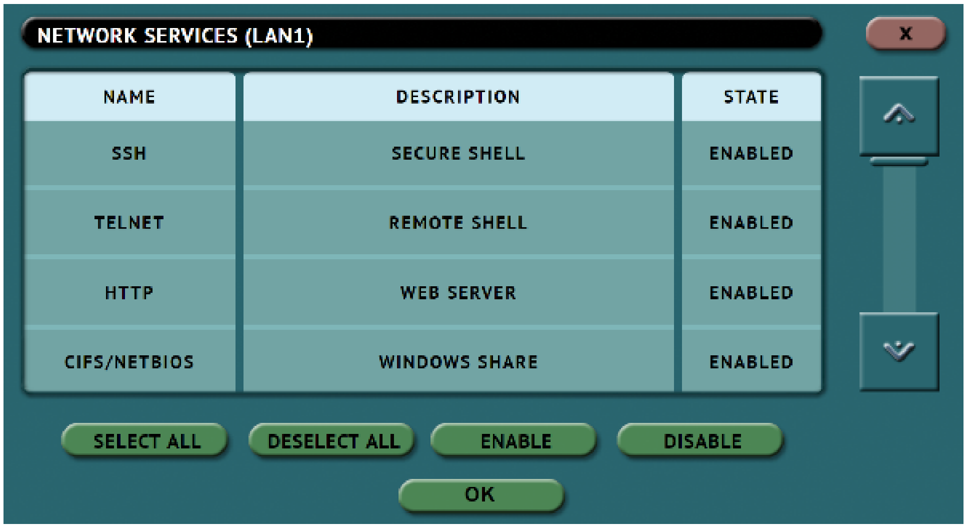
DNS Server . . .

5.10.1.2 MTU

Users can set the MTU (Maximum Transmission Unit) value on this screen. The default is 1500. Check with your network or IT administrator to find out what value to set this to.

5.10.1.3 Enabling/Disabling Network Services

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


NETWORK SERVICES (LAN1)

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

Tap each network service to be enabled or disabled then tap the *Enable* or *Disable* icon.

The following services 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.
- MDNS – Disabling this will block outgoing Multicast DNS packets from the ZXi-10G.

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 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 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 a password.

5.10.2.1 Server

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

5.10.2.2 Username/Password

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

5.10.3 Network Configurations

The ZXi-10G's hostname and NTP Server list can be configured in this tab. Changes on this screen take effect immediately.

> Multiple NTP server entries are separated by a space. For example:
>
> ntp-b.nist.gov time.google.com us.pool.ntp.org

5.10.4 HTTPS

HTTPS certificates are required for secure remote access. On this tab, users can view, select, upload, or generate HTTPS certificates.

5.11 Software Updates

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 *ZXi-10G Software readme* file located on the ZXi-10G Support page on the Logicube website at https://www.logicube.com/knowledgebase/zxi-10g.

In-depth information on updating the ZXi-10G software can be found in *Chapter 6: Updating/Loading/Re-loading Software*.

The *PXEBOOT Update* tab is reserved for future use.

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

The latest ZXi-10G software, manual, and readme file (which contains the software release notes) can always be found on the ZXi-10G support page at https://www.logicube.com/knowledgebase/zxi-10g.

The ZXi-10G software release may contain both a software and firmware update. This chapter details how to update/reinstall the software and firmware.

6.1 Requirements

⚠

A System Restore is required for all ZXi-10G units that currently have a software version below v2.0 (v1.0 through v1.0u2).

To check the currently installed software version, go to the STATISTICS screen and in the ABOUT ZXi-10G tab, look for "Version".

Proceed to *Section 6.2* for the System Restore (if the current software is below v2.0).

Proceed to *Section 6.3* for updating/reinstalling the software (if the current software is v2.0 and above).

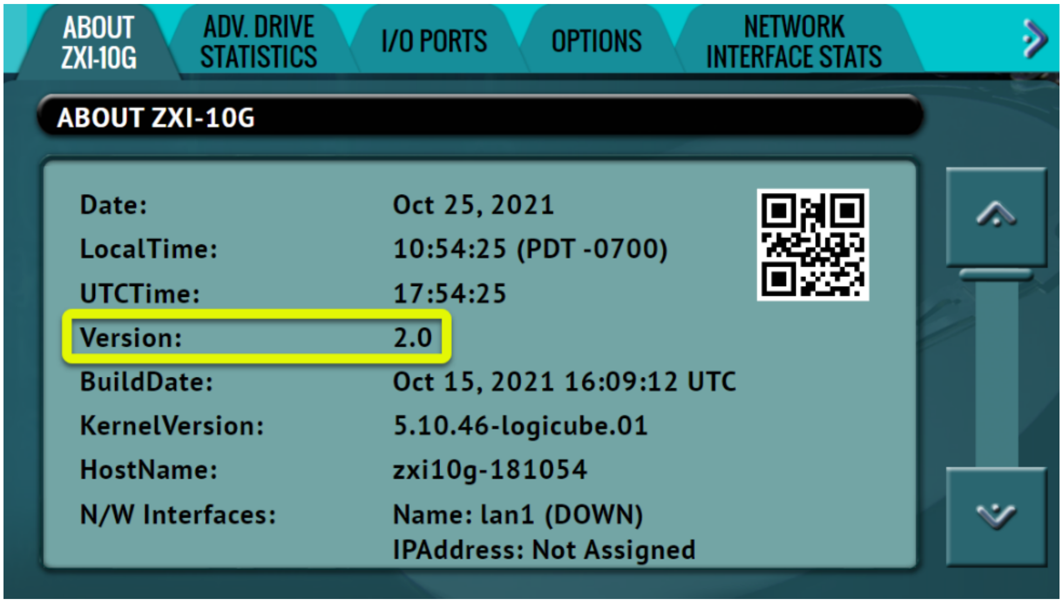
To perform the software update/reinstall, one of the following is required:

- The ZXi-10G connected to a network with Internet access (for updating "FROM NETWORK"), or
- The ZXi-10G with your own USB flash drive. The USB flash drive must be formatted FAT32 or NTFS (for updating "FROM USB DRIVE")

6.2 System Restore

If the current software on the ZXi-10G is below v2.0, a system restore is required.

To check the currently installed software version, go to the *Statistics* screen and in the *About ZXi-10G* tab, look for *Version*.



ABOUT ZXI-10G

Date:	Oct 25, 2021
LocalTime:	10:54:25 (PDT -0700)
UTCTime:	17:54:25
Version:	2.0
BuildDate:	Oct 15, 2021 16:09:12 UTC
KernelVersion:	5.10.46-logicube.01
HostName:	zxi10g-181054
N/W Interfaces:	Name: lan1 (DOWN) IPAddress: Not Assigned

6.2.1 WARNING: Log files will be deleted

Performing the system restore will delete all the log files. Log files can be backed up before the recovery process.

If the ZXi-10G boots up properly, the audit log files can be backed up easily. See *Section 3.6.1 (Viewing or exporting logs)* or *Section 3.6.4 (Accessing logs over a network)* for more information on how to back up the log files if the ZXi-10G boots up properly.

If the ZXi-10G does not boot up properly, there is a possibility the log files may be backed up by following the steps in this section.

6.2.1.1 Requirements for backing up the log files

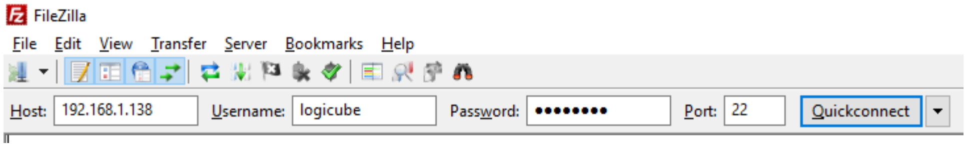
- The ZXi-10G connected to a network
- A computer with a Secure FTP (SFTP) client (E.g. FileZilla or WinSCP) connected to the same network

6.2.1.2 Backing up the log files

The outlined steps in this section use an open-source SFTP client called FileZilla. Other SFTP clients can be used.

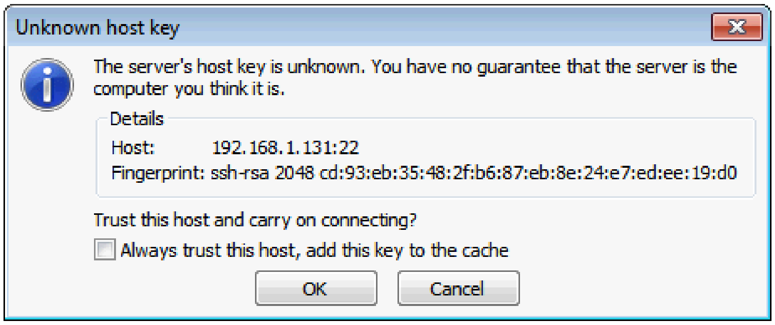
1. Make sure the Logicube device is connected to a network accessible by the computer with the SFTP client and if there is an error message, leave the error message on the screen.
2. Open FileZilla. Similar to the screenshot below, enter the following information then click the Quickconnect button:
    - Host: The IP address or hostname of the Logicube device
    - Username: logicube

- Password: logicube
- Port: 22



Host: 192.168.1.138 Username: logicube Password: •••••••• Port: 22

3. A window may appear labeled *Unknown host key*. If this window appears, click *OK*.



The server's host key is unknown. You have no guarantee that the server is the computer you think it is.

Details

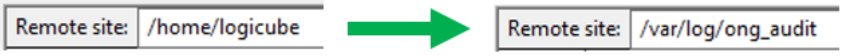
Host: 192.168.1.131:22

Fingerprint: ssh-rsa 2048 cd:93:eb:35:48:2f:b6:87:eb:8e:24:e7:ed:ee:19:d0

Trust this host and carry on connecting?

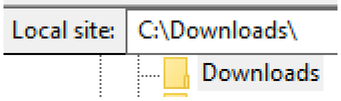
□ Always trust this host, add this key to the cache

4. On the right window pane, change the 'Remote site' to */var/log/ong_audit* then press the *Enter* key.



Remote site: /home/logicube → Remote site: /var/log/ong_audit

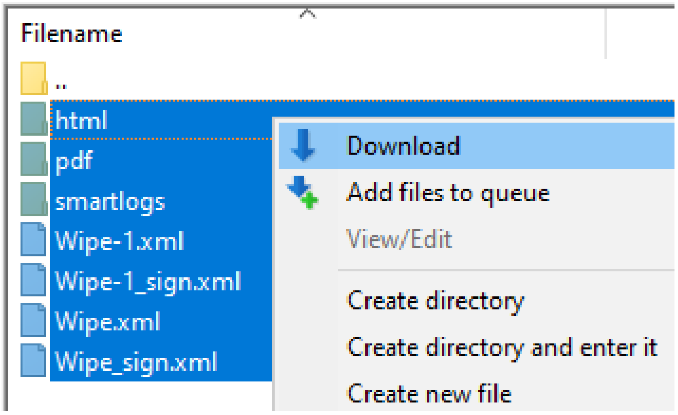
5. On the left window pane, change the 'Local site' to where you want to download the files. In the example below, it will be downloaded to C:\Downloads.



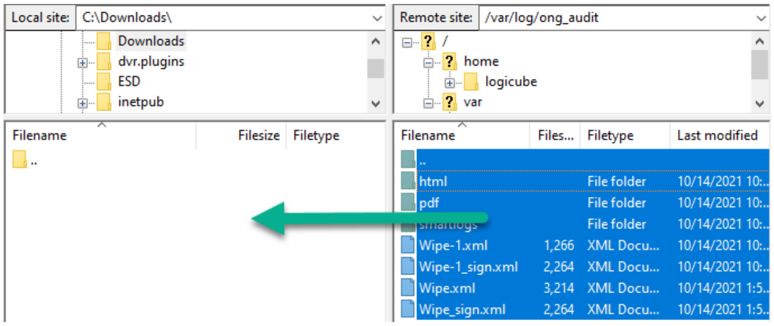
Local site: C:\Downloads\

6. On the right side (Remote site), the /var/log/ong_audit directory has all of the log files. Highlight all the files and folders. There are two ways to download the files:

   a. Right-click the mouse button and select *Download*, or



b. While holding down the left mouse button, drag and drop the log files to the left window pane.



Local site: C:\Downloads\

Remote site: /var/log/ong_audit

Filename	Filesize	Filetype
..		

Filename	Files...	Filetype	Last modified
..			
html		File folder	10/14/2021 10:...
pdf		File folder	10/14/2021 10:...
smartlogs		File folder	10/14/2021 10:...
Wipe-1.xml	1,266	XML Docu...	10/14/2021 10:...
Wipe-1_sign.xml	2,264	XML Docu...	10/14/2021 10:...
Wipe.xml	3,214	XML Docu...	10/14/2021 1:5...
Wipe_sign.xml	2,264	XML Docu...	10/14/2021 1:5...

7. The log files should now be backed up to your computer.

6.2.2 System Restore Requirements

- Your own 4 GB or larger capacity USB flash drive
- A computer with a Windows Operating System
- A wired USB keyboard

6.2.3 Creating the System Restore USB flash drive

Here are the steps to prepare the flash drive with the software necessary to be bootable:

> It is recommended to use Chrome, Firefox, or the new Chromium-based Edge web browser to download the files. Internet Explorer does not download *.img files properly.

1. Go to http://updates.logicube.com/ZXi-10G-recovery/. Look for the following two files:

    - The ZXi-10G image file (a file with a *.img extension)
    - win32diskimager-v1.0.0-binary.zip – An open-source tool used for writing images to USB flash drives or SD/CF cards

    > Balena Etcher may be used instead of Win32DiskImager. The instructions in this section are for Win32DiskImager.

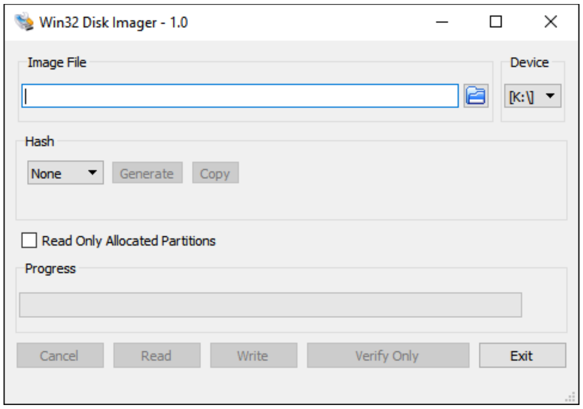
2. Download both files. If the image file will not download, right-click on the link and use the ‘Save Target As…’ or ‘Save Link As’ option and make sure it is saved with the *.img file extension.

3. Extract all the files in the win32diskimager-v1.0.0-binary.zip file to a folder or directory of your choosing.

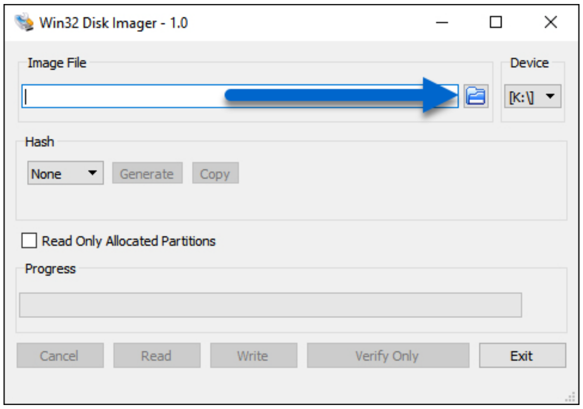
4. Connect a USB flash drive that is at least 4 GB in capacity to the computer where the software was downloaded. It is recommended that all other USB drives are unplugged.

The contents of the USB flash drive will be overwritten. If there is data on the USB flash drive that should not be deleted, back up the contents of the USB flash drive or use another USB flash drive for this procedure.

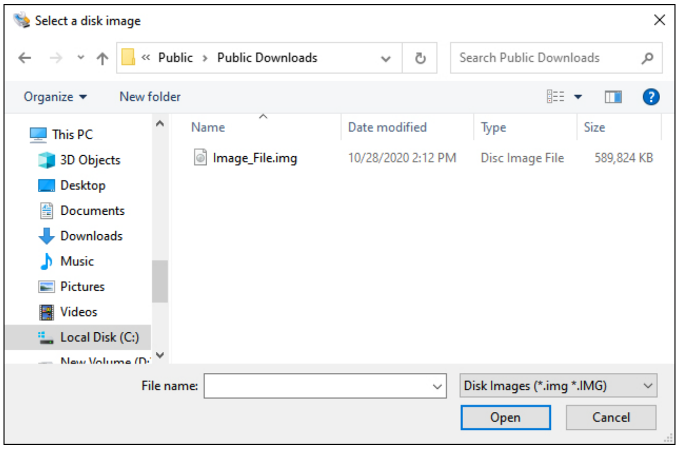
5. In the win32diskimager-v1.0.0-binary folder where the software was extracted, run the file *Win32DiskImager.exe*. The Win32 Disk Imager window will appear.



6. Click the folder icon to select a disk image.



7. In the folder where the files were downloaded (in step 2), select the restore file and click the *Open* icon. Note the screenshot below shows a different file name.



Name	Date modified	Type	Size
Image_File.img	10/28/2020 2:12 PM	Disc Image File	589,824 KB

8. The Image file should now be seen in the Win32 Disk Imager screen under ‘Image File’.

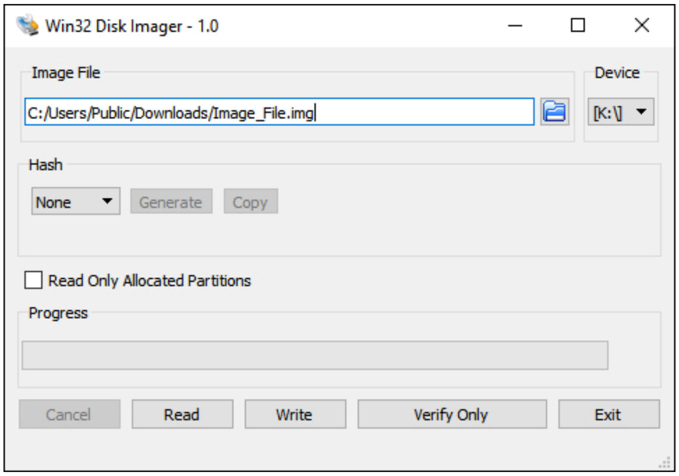


Image File: C:/Users/Public/Downloads/Image_File.img

Device: [K:\]

Hash: None

□ Read Only Allocated Partitions

9. Under ‘Device’, select the drive letter for the USB flash drive that was connected during step 3 then click the *Write* icon.

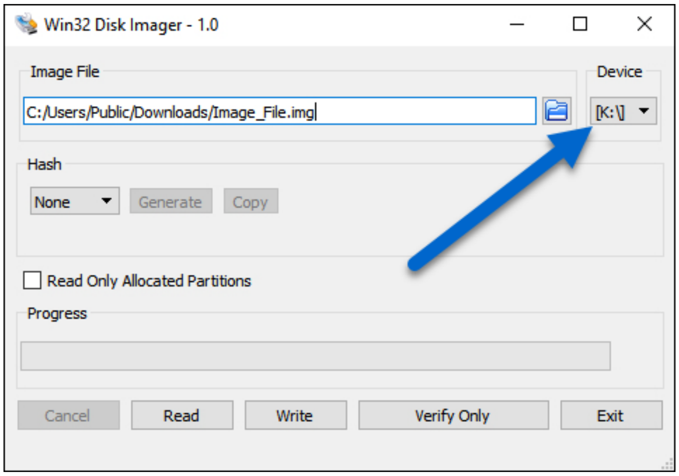


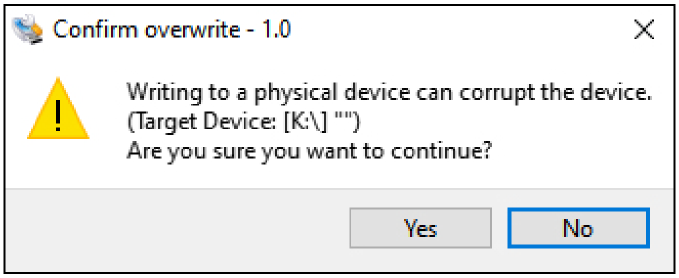
Image File: C:/Users/Public/Downloads/Image_File.img

Device: [K:\]

Hash: None

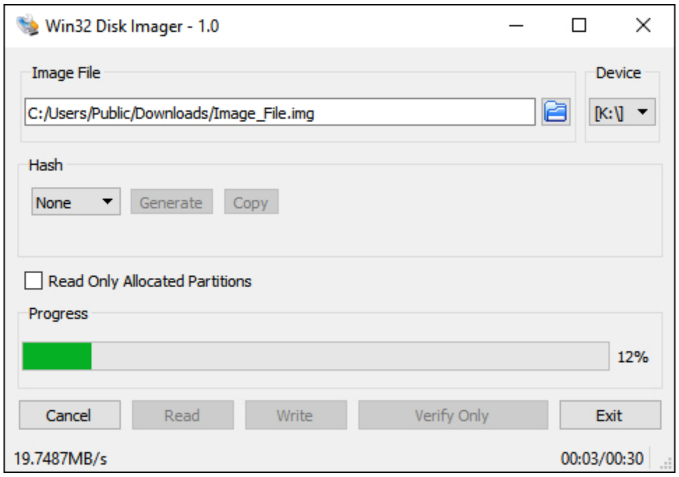
□ Read Only Allocated Partitions

10. A confirmation screen will appear. Make sure that the “Target Device” is set to the correct drive letter. If it is the correct drive letter, click *Yes* to continue. If it is showing the wrong drive letter, click *No*. This will take you back to the previous screen where you can select the correct drive letter (back to step 9).



Writing to a physical device can corrupt the device.
(Target Device: [K:\] "")
Are you sure you want to continue?

11. The USB flash drive is now being prepared and the progress bar should be advancing.



Win32 Disk Imager - 1.0

Image File: C:/Users/Public/Downloads/Image_File.img

Device: [K:\]

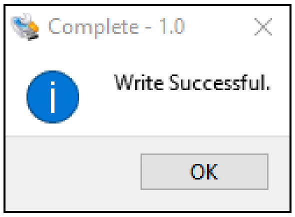
Hash: None

□ Read Only Allocated Partitions

Progress: 12%

19.7487MB/s 00:03/00:30

12. When it is finished, a prompt should appear stating the write was successful. Click the *OK* icon to continue. Close the Win32 Disk Imager window. The USB flash drive is now ready to be used.



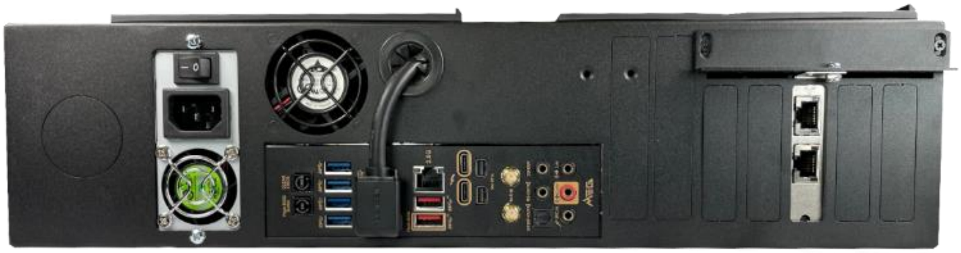
Complete - 1.0

Write Successful.

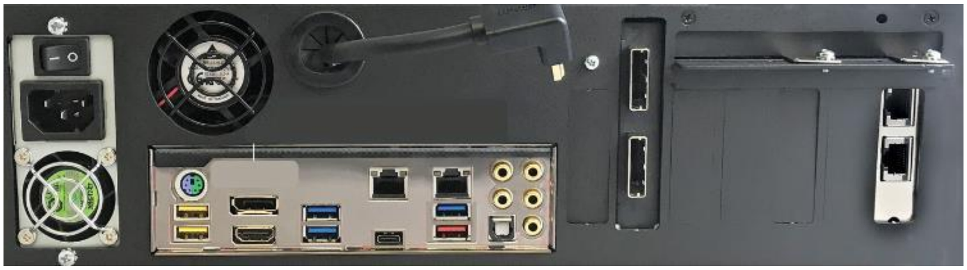
13. Disconnect the USB flash drive from the computer.

6.2.4 Using the System Restore USB Flash Drive

1. Turn the ZXi-10G OFF and disconnect all drives (and any drive adapters) connected to all ports.
2. Connect a wired USB keyboard to of the USB ports.
3. Connect the USB system restore flash drive (created in *Section 6.2.3*) to any other USB port.
4. Determine which ZXi-10G version you have.
   a. If the back of the ZXi looks like the following picture, turn the ZXi-10G on and immediately press and hold the F11 key on the keyboard. Keep holding the F11 key down until a boot menu appears.

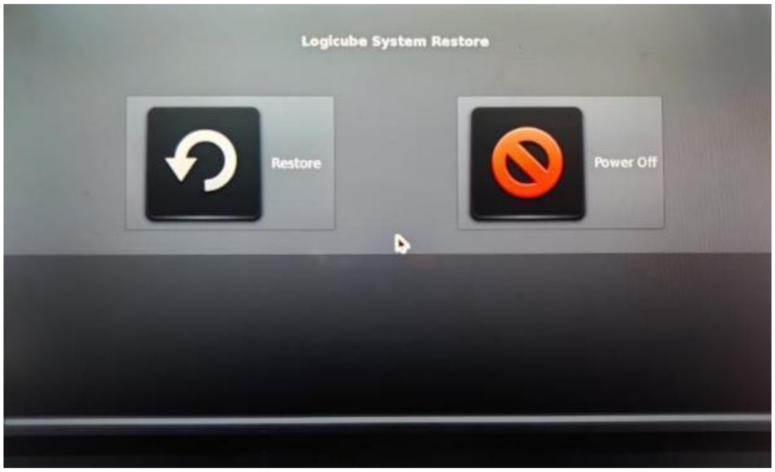


b. If the back of the ZXi looks like the following picture, turn the ZXi-10G on and immediately press and hold the F12 key on the keyboard. Keep holding the F12 key down until a boot menu appears.

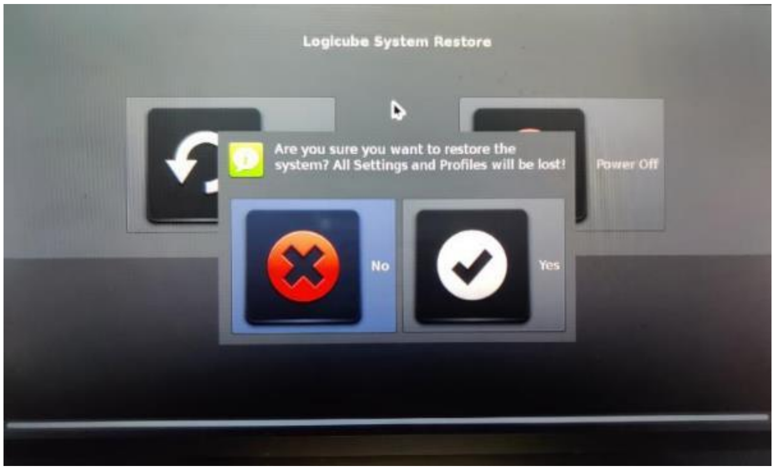


5. When the boot menu appears, it should show the USB flash drive with the Restore software. Select to boot from the USB Restore software.

6. The System Restore will load. When the System Recovery fully loads, the following screen will appear. Tap *Restore*.

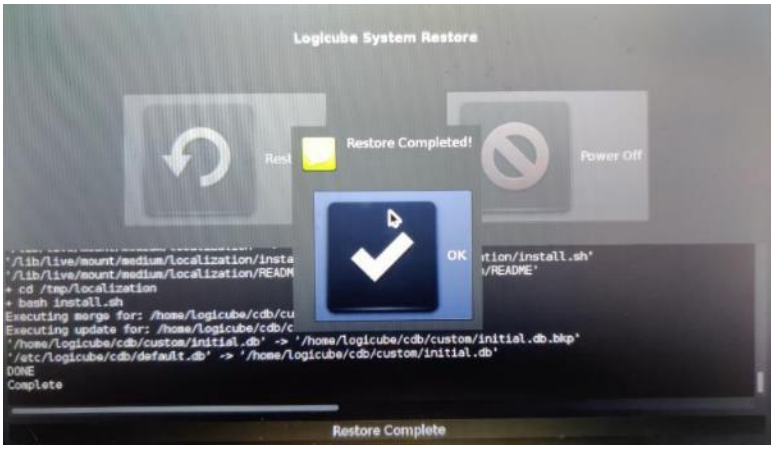


7. A confirmation screen will appear. Tap *Yes* to continue with the System Restore.


Are you sure you want to restore the system? All Settings and Profiles will be lost!

8. The system restore will begin. The entire process may take up to 10 (ten) minutes to complete.

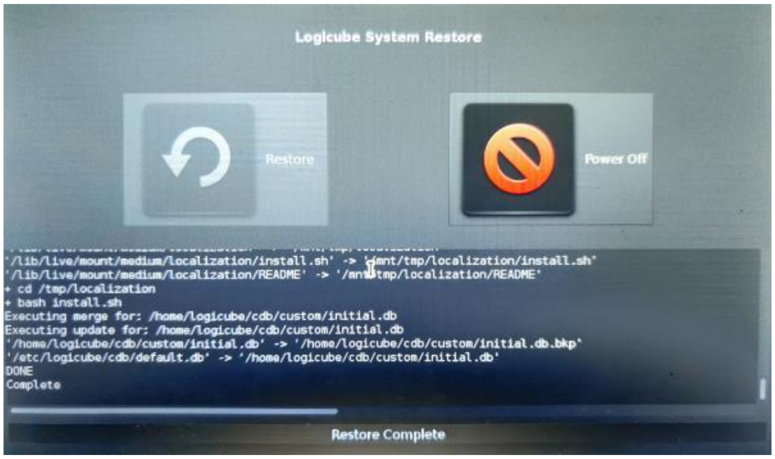
9. When finished, the following screen will appear. Tap *OK*.



Restore Completed!

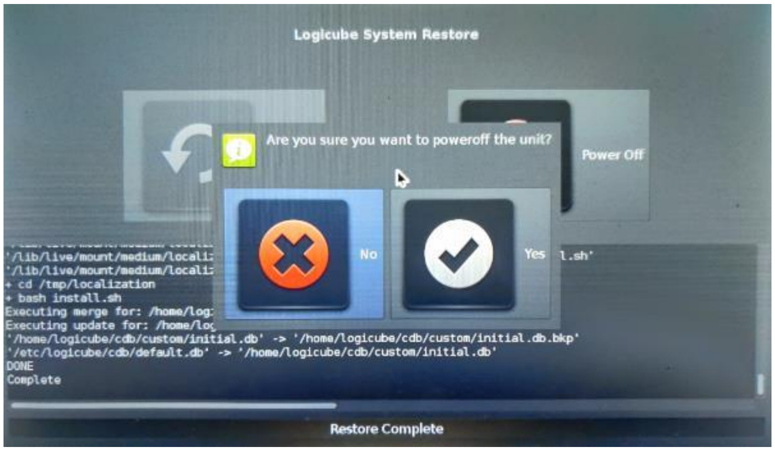
```
'/lib/live/mount/medium/localization/insta                      tion/install.sh'
'/lib/live/mount/medium/localization/READM                      /README'
+ cd /tmp/localization
+ bash install.sh
Executing merge for: /home/logicube/cdb/cu
Executing update for: /home/logicube/cdb/c
'/home/logicube/cdb/custom/initial.db' -> '/home/logicube/cdb/custom/initial.db.bkp'
'/etc/logicube/cdb/default.db' -> '/home/logicube/cdb/custom/initial.db'
DONE
Complete
```

10. The main System Restore screen will appear. Tap *Power Off*.



```
'/lib/live/mount/medium/localization/install.sh' -> '/mnt/tmp/localization/install.sh'
'/lib/live/mount/medium/localization/README' -> '/mnt/tmp/localization/README'
+ cd /tmp/localization
+ bash install.sh
Executing merge for: /home/logicube/cdb/custom/initial.db
Executing update for: /home/logicube/cdb/custom/initial.db
'/home/logicube/cdb/custom/initial.db' -> '/home/logicube/cdb/custom/initial.db.bkp'
'/etc/logicube/cdb/default.db' -> '/home/logicube/cdb/custom/initial.db'
DONE
Complete
```

11. A confirmation screen will appear. Tap *Yes*.



Are you sure you want to poweroff the unit?

```
'/lib/live/mount/medium/locali:                                 l.sh'
'/lib/live/mount/medium/locali:
+ cd /tmp/localization
+ bash install.sh
Executing merge for: /home/log:
Executing update for: /home/loc
'/home/logicube/cdb/custom/initial.db' -> '/home/logicube/cdb/custom/initial.db.bkp'
'/etc/logicube/cdb/default.db' -> '/home/logicube/cdb/custom/initial.db'
DONE
Complete
```

12. The ZXi-10G should gracefully shut down and will turn itself off. The System Restore process should now be complete. Disconnect the USB keyboard and USB System Restore flash drive and turn the ZXi-10G on to make sure it boots properly.

13. Follow the instructions in *Section 6.3* and *Section 6.4* to check for software and firmware updates.

6.3 Updating/Reinstalling the Software

> A System Restore is required for all ZXi-10G units that currently have a software version below v2.0 (v1.0 through v1.0u2).
>
> To check the currently installed software version, go to the STATISTICS screen and in the ABOUT ZXi-10G tab, look for "Version".
>
> Go back to Section 6.2 for the System Restore if the current software is below v2.0.

There are two methods available to update/reinstall the ZXi-10G software:

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

6.3.1 From Network (Over the Internet)

The ZXi-10G software can be updated/re-installed by connecting the ZXi-10G to a network with Internet access.

> It is recommended to disconnect all drives and drive adapters from the ZXi-10G before the update/reinstall process.

1. Connect the ZXi-10G to a network with Internet access and turn the ZXi-10G on.
2. From the main menu on the ZXi-10G, tap/click *Software Updates* on the left side.
3. Select *From Network*. The ZXi-10G 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/click the *OK* icon to continue.
   - *UP TO DATE* – This message will appear if the software version found is the same as the version currently installed. Tap the *OK* icon to continue.
   - *HTTP://UPDATES.LOGICUBE.CC10G/ FAILED: 500 CAN'T CONNECT TO UPDATES.LOGICUBE.COM:80* – This message will appear if the ZXi-10G cannot connect to the update site. When this message appears, double-check that you have an Internet connection to the ZXi-10G. For example, try a different network cable or network drop. If the message persists, try the following:
     - Go to the *About* tab in the *Statistics* screen and check the *N/W Interfaces* to make sure the ZXi-10G is connected to a network and has a valid *IPAddress*, or
     - Make sure the network the ZXi-10G is connected to has Internet access, or
     - Try using the "From USB DRIVE" option (see Section 6.3.2).
4. Tap the *Update* icon to begin the update/reinstall. The ZXi-10G should begin the update/reinstall process. Do not interrupt this process. It may take several minutes.

Once completed, a screen will appear stating the update is complete and will prompt you to turn the unit off then back on.

5. Turn the ZXi-10G off. Wait at least 5 seconds then turn the ZXi-10G back on.
6. Verify the software version by going to the Software Updates screen then go to section *6.4 Firmware Update* to check if there is a firmware update available.

6.3.2 From USB Drive (Through a software file download)

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

It is recommended to disconnect all drives and drive adapters from the ZXi-10G before the update/reinstall process.

1. Using a computer, download the latest software from the ZXi-10G product support page at https://www.logicube.com/knowledgebase/zxi-10g/.
2. Extract the contents of the downloaded zip file to the root of the USB flash drive.
3. Turn the ZXi-10G 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 leftmost USB port on the front).
4. From the main menu on the ZXi-10G, tap/click *Software Updates* on the left side.
5. Select *From USB Drive*. The ZXi-10G will 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.
    - *UPDATES NOT FOUND!* – The ZXi-10G did not find any software on the USB flash drive or could not detect the USB flash drive. If this message is seen, try the following:
        - Make sure the correct software was downloaded and the files were extracted to the root of the USB flash drive, or
        - Format and use a different USB flash drive, or
        - Try using the "From Network" option (see *Section 6.3.1*)
6. Tap the *Update* icon to begin the update/reinstall. The ZXi-10G should begin the update/reinstall process. Do not interrupt this process. It may take several minutes. Once completed, a screen will appear stating the update is complete and will prompt you to turn the unit off then back on.
7. Turn the ZXi-10G off. Wait at least 5 seconds then turn the ZXi-10G back on.
8. Verify the software version by going to the Software Updates screen then go to *Section 6.4 Firmware Update* to check if there is a firmware update available.

6.4 Firmware Update

ZXi-10G software releases may contain a firmware update. This section provides instructions on how to check if a firmware update is required, and how to perform the firmware update.

1. After the software is updated/re-installed on the ZXi-10G, tap/click *Software Updates* on the left side.
2. Tap the *Firmware Update* tab. One of two screens will appear:
    a. *FIRMWARE UPGRADE AVAILABLE* – Tap *Update*. 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 *OK* 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 60 seconds. When the firmware update finishes, the ZXi-10G 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.

6.5 PXEBOOT UPDATE

This screen is reserved for future use.

7: Remote Operation

7.0 Remote Operation - Introduction

Two 10GbE and one 2.5GbE 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 5.10.1.1* 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:
  - Telnet (Using a Telnet client over a network connection)
  - SSH (Using a Secure Shell Client over a network connection)

BROWSER COMPATIBILITY: Chrome, Firefox, or the new Chromium-based Edge browser 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://zxi10g-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://zxi10g-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 know command-line functions. This type of connection requires a Telnet or SSH client. There are many 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.
- Not all versions of Windows 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 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 zxi10g-*XXXXXX* where XXXXXX is the 6-digit serial number of the unit).
5. Log in 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.

7.2.2 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 zxi10g-XXXXXX*
   where XXXXXX is the 6-digit serial number of the unit, then press Enter. A login should appear.
5. Log in 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.

7.3 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 Hardware and Software Options - Introduction

The ZXi-10G has several available additional options including software options and additional adapters. For a complete list of available options, please visit https://www.logicube.com/shop/zxi-10g. This section lists the following options:

- 4-Port Drive Expansion Kit
- PCIe Expansion Module (for M.2 NVMe SSDs)
- Hash Verification Option
- SAS Option

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

8.1 4-Port Drive Expansion Kit

The optional expansion kit provides an additional 2 SAS/SATA and 2 SATA only targets.

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-10G Drive Station

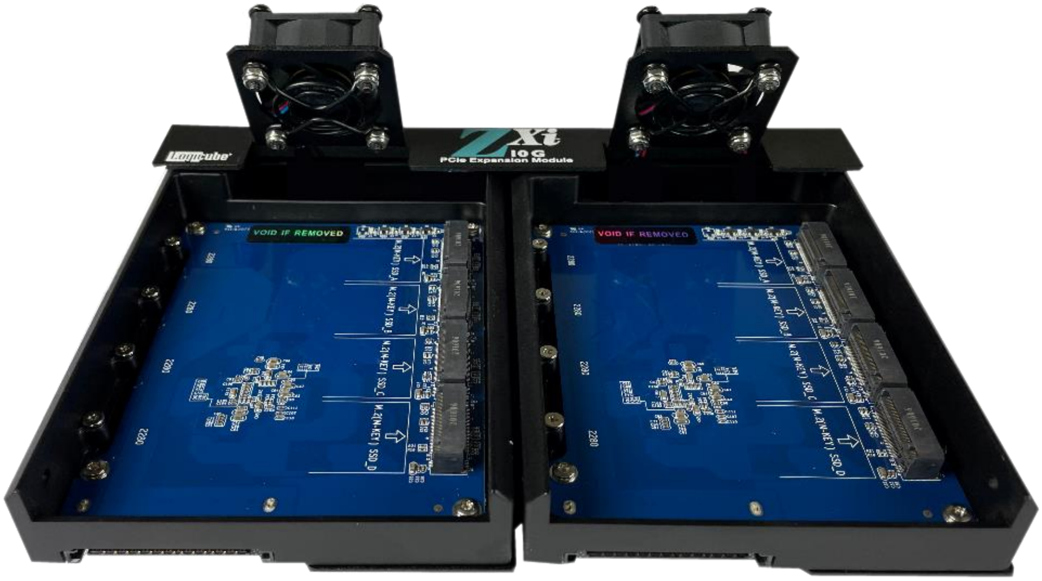
Follow these steps to attach the removable ZXi-10G drive stations to the ZXi-10G's expansion slots:

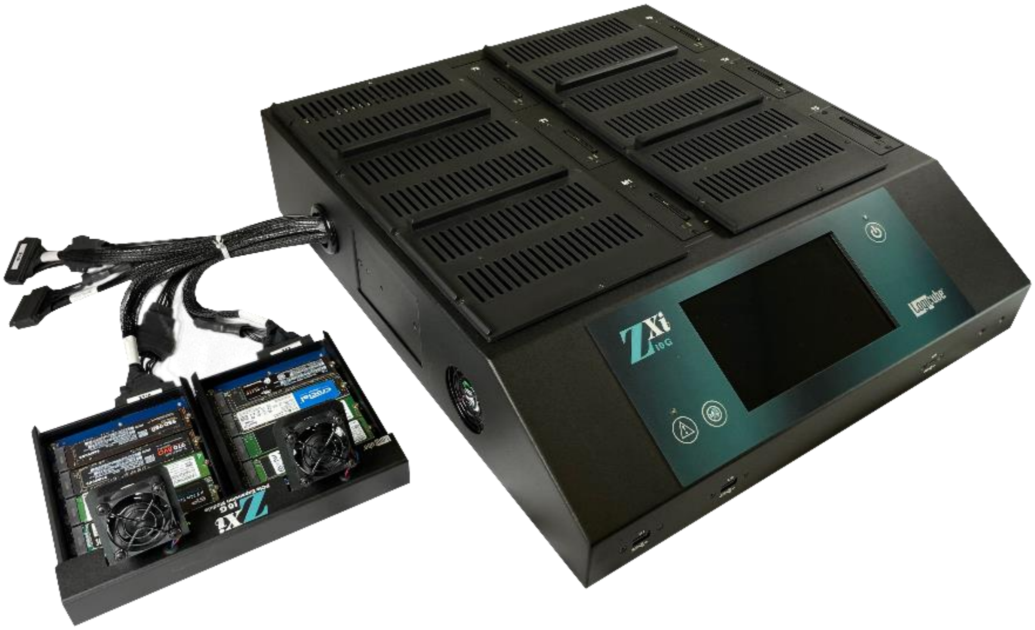
1. Remove the cover on one of the expansion ports (T6 through T9) using a Phillips head screwdriver. There are two screws on the cover (one on each side). Set the two screws aside as they will be used for the ZXi-10G drive station.
2. Connect the ZXi-10G drive station to the open port from step 1. When inserted properly, the ZXi-10G drive station should not be protruding or sticking out.
3. Use the two screws set aside from step 1 to tighten and set the ZXi-10G drive station in place.

8.2 PCIe Expansion Module

The Logicube PCIe Expansion Module is a hardware option that provides support for up to 8 M.2 NVMe SSDs on the ZXi-10G. Up to two modules can be connected to the ZXi-10G supporting a total of up to 16 M.2 NVMe SSDs

This expansion module is only compatible with the ZXi-10G. It is not compatible with the ZClone™ Xi (ZXi).





8.2.1 Instructions

IMPORTANT NOTE: The ports on the PCIe Expansion Module are not hot-swappable. Always make sure the ZXi-10G is turned OFF when connecting or disconnecting drives on the Module.

1. Make sure the ZXi-10G is turned off.
2. The PCIe Expansion Module has two connectors on the front of the module. On the left side of the ZXi-10G, connect the cable labeled P1 and P2 to the PCIe Expansion Module.
3. Turn the ZXi-10G on.

8.3 Hash Verification Option

This option, when activated, allows the ZXi-10G 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-10G software. See *Chapter 6* for details on how to load or reload the software.

8.4 SAS Option

This option, when activated, allows the ZXi-10G 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-10G software. See *Chapter 6* for details on how to load or reload the software.

9: USB Boot Client

9.0 USB Boot Client Introduction

A USB (iSCSI) Boot Client (bootable USB flash drive) is available. The bootable flash drive allows the cloning of a Master drive from a computer on the same network without booting the native Operating System on the computer and can be imaged without having to remove the drive from the computer. It also allows the cloning from a drive connected to the ZXi-10G (or a ZXi-10G image file) to another computer (as a Target) without having to disconnect or remove the drive.

9.1 Requirements

To create the USB Boot Client, the following are required:

- Your own 1 GB or larger capacity USB flash drive
- A computer with Microsoft Windows

To use the USB Boot Client with the ZXi-10G, the following are required:

- The ZXi-10G connected to a network (or directly to the computer to be cloned/imaged)
- The computer to be cloned/imaged with a wired connection to the same network (or directly to the ZXi-10G)

9.2 Creating the USB Boot Client

Here are the steps to create the USB Boot Client with the software necessary to be bootable, and when used to boot a computer, will allow the ZXi-10G to use the computer's drive as a Master or Target drive.

It is recommended to use Chrome, Firefox, or the new Chromium-based Edge web browser to download the files. Internet Explorer does not download *.img files properly.

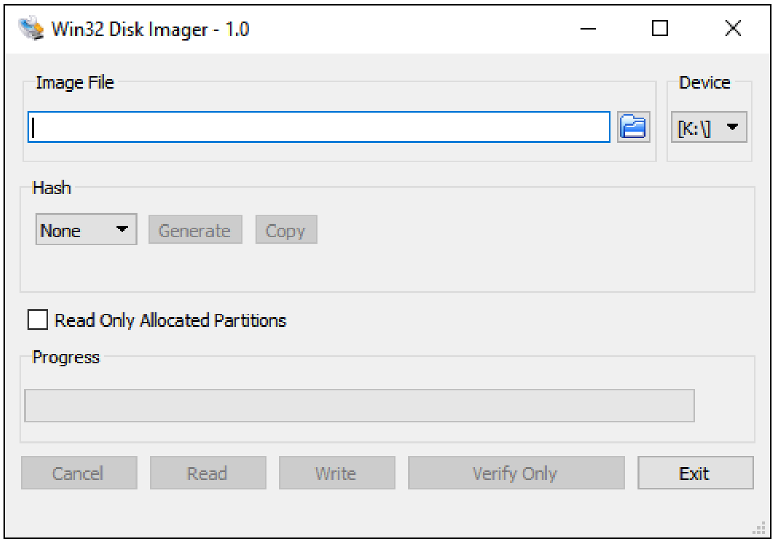
1. Using an Internet browser, browse to http://updates.logicube.com/iscsi/. Look for the following two files:
    - Win32DiskImager-1.0.0-binary.zip
    - The USB Boot Client image file – A file with a *.img file extension

    Balena Etcher may be used instead of Win32DiskImager. The instructions in this section are for Win32DiskImager.

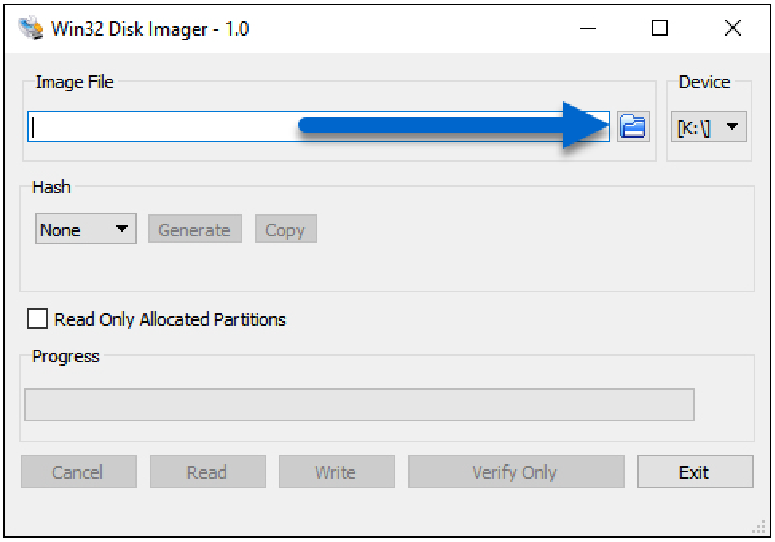
2. Download both files. If the image file will not download, right-click on the link and use the 'Save Target As…' or 'Save Link As' option and make sure it is saved with the *.img file extension.
3. Extract all the files within the win32diskimager-v1.0.0-binary.zip file to a folder or directory of your choosing.
4. Connect your USB flash drive that is at least 1 GB in capacity to the computer where the software was downloaded. It is recommended that all other USB drives are unplugged.

> ⚠ The contents of the USB flash drive will be overwritten. If there is data on the USB flash drive that should not be deleted, back up the contents of the USB flash drive or use another USB flash drive for this procedure.

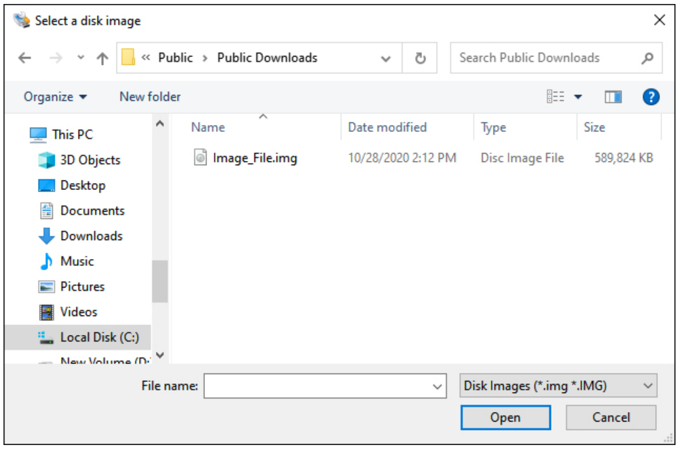
5. In the win32diskimager-v1.0.0-binary folder where the files were extracted, run the file *Win32DiskImager.exe*. The Win32 Disk Imager window will appear.



6. Click the folder icon to select a disk image.



7. In the folder where the files were downloaded (in step 2), select the USB Boot Client *.img file and click the *Open* icon.



Name	Date modified	Type	Size
Image_File.img	10/28/2020 2:12 PM	Disc Image File	589,824 KB

File name:
Disk Images (*.img *.IMG)

8. The Image file should now be seen in the Win32 Disk Imager screen under ‘Image File’.

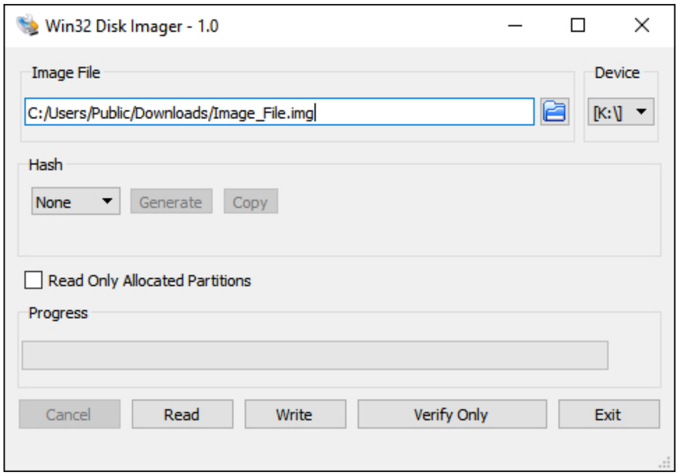


Image File: C:/Users/Public/Downloads/Image_File.img
Device: [K:\]
Hash: None
☐ Read Only Allocated Partitions

9. Under ‘Device’, select the drive letter for the USB flash drive that was connected during step 4 then click the *Write* icon.

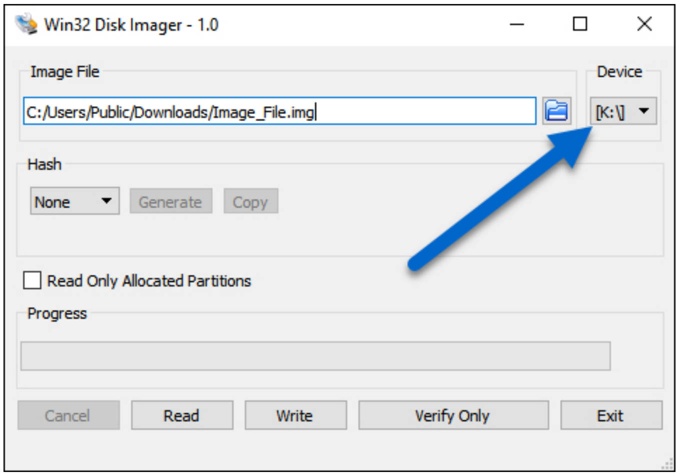
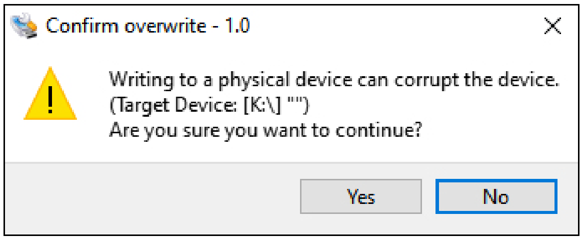


Image File: C:/Users/Public/Downloads/Image_File.img
Device: [K:\]
Hash: None
☐ Read Only Allocated Partitions

10. A confirmation screen will appear. Make sure that the "Target Device" is set to the correct drive letter. If it is the correct drive letter, click *Yes* to continue. If it is showing the wrong drive letter, click *No*. This will take you back to the previous screen where you can select the correct drive letter (back to step 9).


Confirm overwrite - 1.0

Writing to a physical device can corrupt the device.
(Target Device: [K:\] "")
Are you sure you want to continue?

11. The USB flash drive is now being prepared and the progress bar should be advancing.

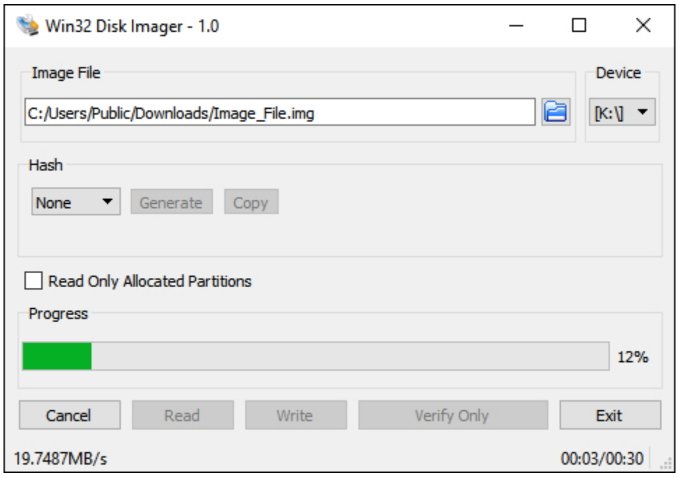

Win32 Disk Imager - 1.0

Image File: C:/Users/Public/Downloads/Image_File.img

Device: [K:\]

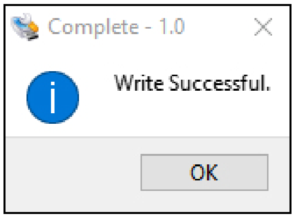
Hash: None

☐ Read Only Allocated Partitions

Progress: 12%

19.7487MB/s 00:03/00:30

12. When it is finished, a prompt should appear stating *Write Successful*. Click the *OK* button to continue. Close the Win32 Disk Imager window. The USB flash drive is now ready to be used.


Complete - 1.0

Write Successful.

9.3 Allowing drives to be used as Destination/Target

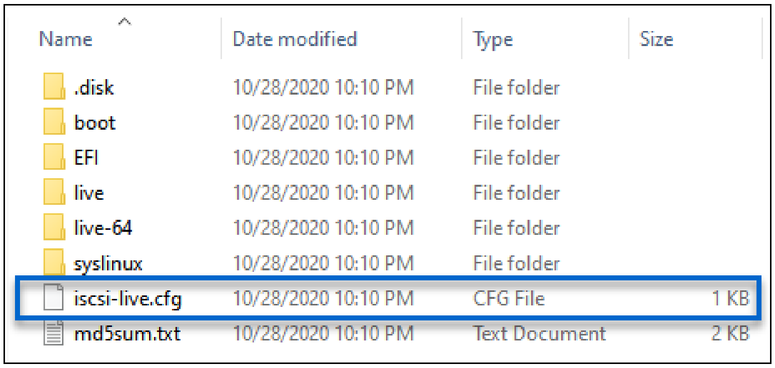
By default, the USB Boot Client allows drives to be used only as Master drives. Additional steps are required to allow drives to be used as Destination/Target drives.

1. With the USB Boot Client connected to a Windows computer, open File Explorer or Windows Explorer.

   For these steps, it is helpful to set File Explorer or Windows Explorer to show file extensions.

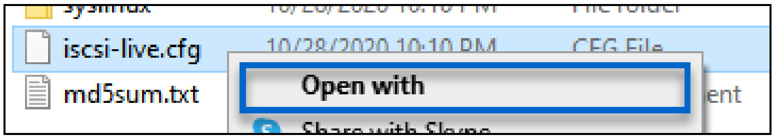
2. Browse to the ISCS_LIVE flash drive that was just created.

3. Look for the file “iscsi-live” or “iscsi-live.cfg”

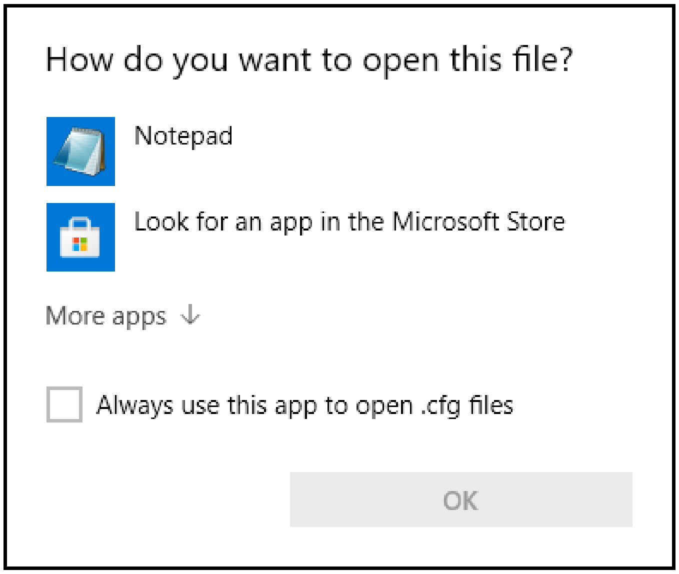


Name	Date modified	Type	Size
.disk	10/28/2020 10:10 PM	File folder	
boot	10/28/2020 10:10 PM	File folder	
EFI	10/28/2020 10:10 PM	File folder	
live	10/28/2020 10:10 PM	File folder	
live-64	10/28/2020 10:10 PM	File folder	
syslinux	10/28/2020 10:10 PM	File folder	
iscsi-live.cfg	10/28/2020 10:10 PM	CFG File	1 KB
md5sum.txt	10/28/2020 10:10 PM	Text Document	2 KB

4. Right-click the “iscsi-live.cfg” file and choose “Open with”.



5. Open the file using a text editor like Notepad or Wordpad. If Windows asks how the file should be opened, select Notepad or Wordpad.



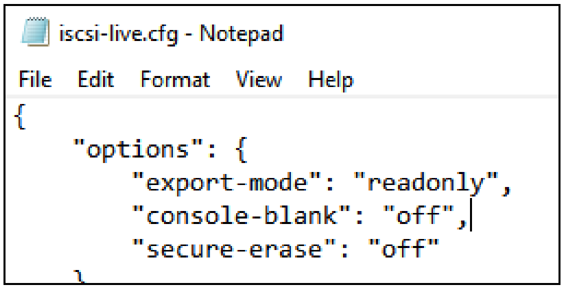
How do you want to open this file?

Notepad

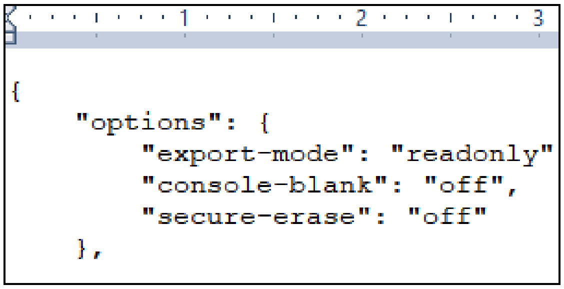
Look for an app in the Microsoft Store

□ Always use this app to open .cfg files

6. Notepad or Wordpad should open and you will see something similar to one of the two images below:

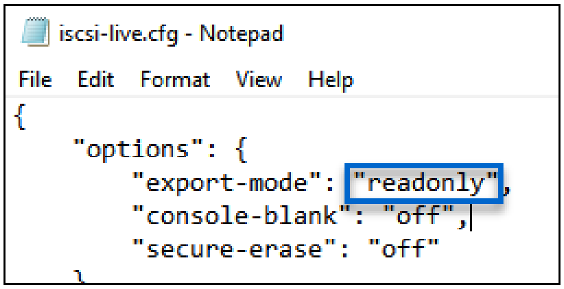


```
{
    "options": {
        "export-mode": "readonly",
        "console-blank": "off",
        "secure-erase": "off"
    }
```

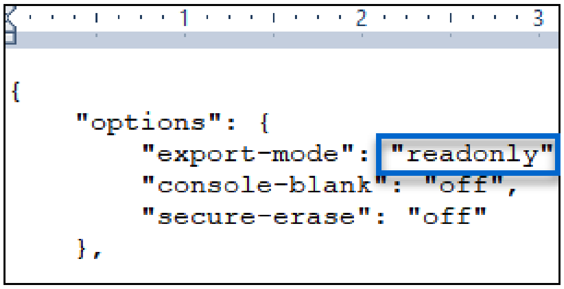


```
{
    "options": {
        "export-mode": "readonly"
        "console-blank": "off",
        "secure-erase": "off"
    },
```

7. Look for export-mode": "readonly".

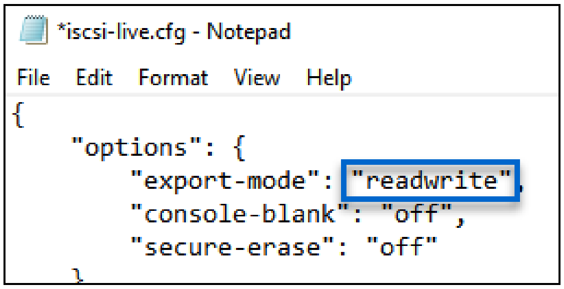


```
{
    "options": {
        "export-mode": "readonly",
        "console-blank": "off",
        "secure-erase": "off"
    }
```

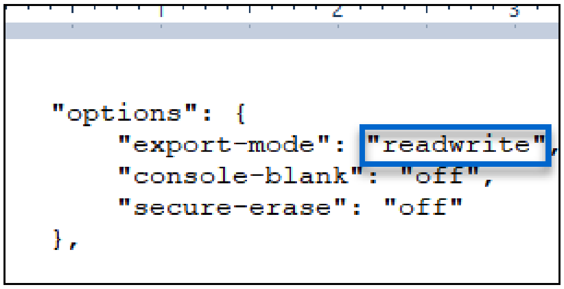


```
{
    "options": {
        "export-mode": "readonly",
        "console-blank": "off",
        "secure-erase": "off"
    },
```

8. Change the word "readonly" to "readwrite".



```
{
    "options": {
        "export-mode": "readwrite",
        "console-blank": "off",
        "secure-erase": "off"
    }
```



```
    "options": {
        "export-mode": "readwrite",
        "console-blank": "off",
        "secure-erase": "off"
    },
```

9. Save the file and close the text editor.

10. The USB Boot Client is now ready to be used. When booting a computer with this USB boot Client, all connected drives will appear as both Master and Destination/Target.

9.4 Using the USB Boot Client

Drives connected to the computer can be used by the supported Logicube Device as a Source/Master or Destination/Target (if *Section 5.0* was followed) over a network connection if the USB Boot Client is used to boot the computer. The USB Boot Client is set to DHCP and at this time, a static IP cannot be set.

For computers that do not have a built-in Ethernet adapter, a USB to Ethernet adapter may be used. Some laptops also have docks that have an Ethernet adapter that may work.

1. Some changes to the computer's BIOS or UEFI may be required to use the USB Boot Client. Boot into the computer's BIOS or UEFI and look for the following settings. Some computers may not have these settings. Once these have been set, save and exit the BIOS or UEFI:
    a. SATA Operation – Depending on the computer, this may be called something different. Typically, this would have up to three settings: Disabled, AHCI, and RAID. Make sure this is set to *AHCI*. The internal drive on the computer may not be detected by the USB Boot Client if this is set differently.
    b. Secure Boot – This setting needs to be set to *Disabled*. If it is not set to 'disabled', the USB flash drive with the Boot Client may not be seen/displayed as a boot option.
2. Connect the ZXi-10G to the same network the computer with the USB Boot Client will be used on (or directly connected to the computer using a network cable).

3. Connect the computer (with the USB Boot Client) to the same network the ZXi-10G is connected to.

4. Boot the computer with the USB Boot Client.

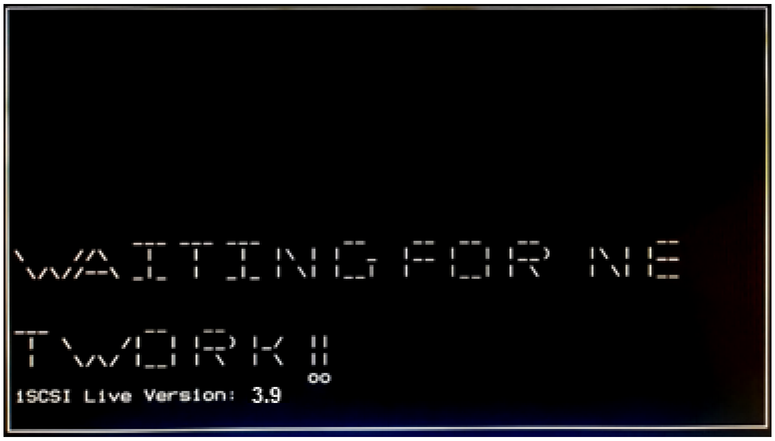
> Please contact the computer manufacturer if you do not know how to change the boot sequence to boot from a USB drive or to find out if the computer supports this function.

5. The USB Boot Client's boot menu will appear, and It should auto-select "iSCSI Target (64-bit)" after a few seconds. If not, select "iSCSI Target (64-bit)".

> The default (64-bit) should work with most computers. If it does not work, use the connected keyboard's DOWN arrow to select iSCSI Target (32-bit) to boot with the 32-bit version.

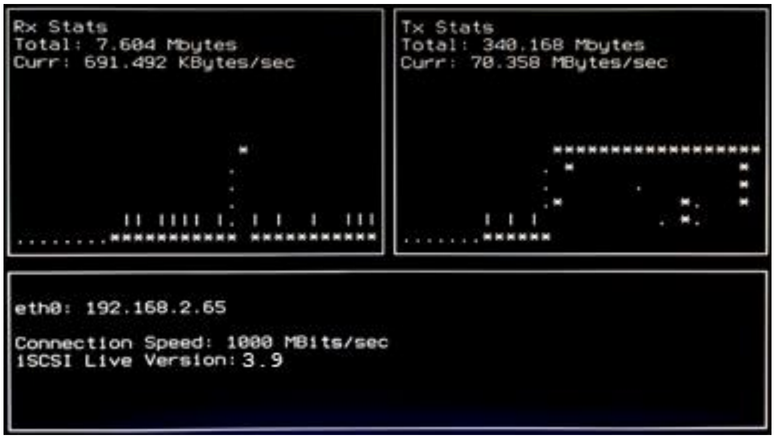
6. After about 30-120 seconds (depending on the speed of the computer), the USB Boot Client should finish booting up.

   - The following screen may appear if no network adapter or network connection is detected, or briefly while the network is being detected. If this screen appears for a long time, double-check the network adapter or network connection.



```
WAITING FOR NE
TWORK !!
iSCSI Live Version: 3.9
```

   - If a network adapter and network connection are detected, the following screen will appear:



```
Rx Stats                              Tx Stats
Total: 7.604 Mbytes                   Total: 340.168 Mbytes
Curr: 691.492 KBytes/sec              Curr: 70.358 MBytes/sec

eth0: 192.168.2.65

Connection Speed: 1000 MBits/sec
iSCSI Live Version: 3.9
```

7. Turn the ZXi-10G on. After the ZXi-10G boots up, you should see additional drives appear on the Source position depending on the Imaging mode chosen.

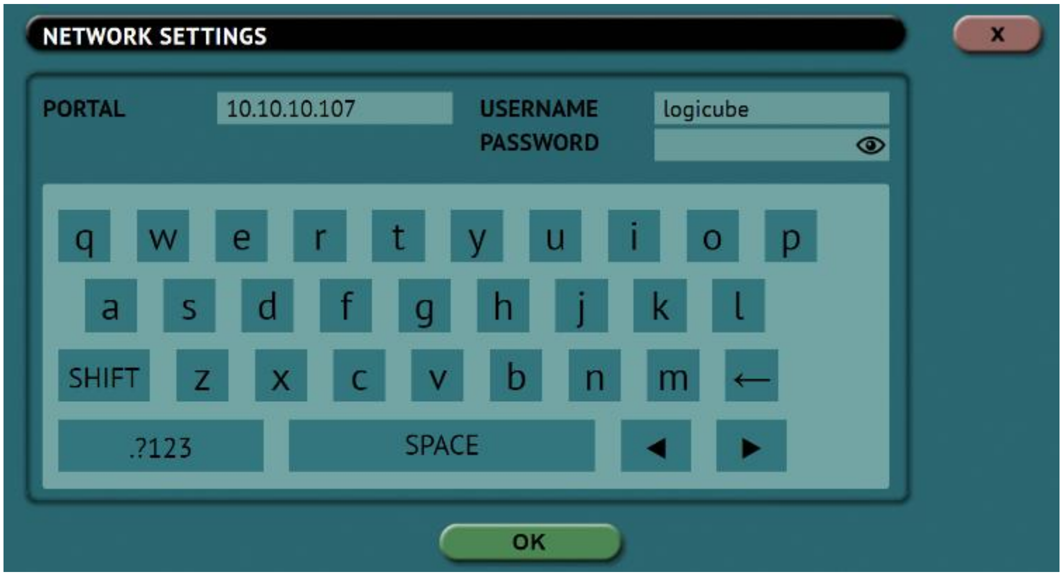
> The Logicube device will show the last two segments of the IP address. For example, I:2.65. The connected drive will show as *SDA*. If there are any additional connected drives, they will show as *SDB*, *SDC*, etc. For example, if there is one drive connected, it will show as I:2.65/SDA.

From here you can clone using the ZXi-10G using the normal cloning steps. When using the USB Boot Client, cloning speeds may vary depending on network performance.

9.5 Using the USB Boot Client Over Different Subnets

The USB Boot Client and the ZXi-10G can work over different subnets if both subnets can see each other on the network. Additional steps need to be taken when accessing a different subnet.

1. Follow the steps in *Section 9.4* to boot with the USB Boot Client.
2. Turn the ZXi-10G on.
3. Navigate to *Manage Repositories* and tap or click the *iSCSI* tab.
4. Tap or click *Network Settings*. In the *Network Settings* screen, enter the following information:
    a. PORTAL – The IP address of the iSCSI remote device (on the different subnet). Depending on your network setup, port 3260 may need to be added to the portal (for example 10.10.10.107:3260)
    b. USERNAME: logicube (all lower case).
    c. PASSWORD: leave this blank.



NETWORK SETTINGS

PORTAL 10.10.10.107

USERNAME logicube

PASSWORD

5. When finished, tap or click *OK*.

6. Tap or click *CONNECT* to connect to the remote device. Please note that the screen may stay on the “Connecting” screen for up to 60 seconds (or longer) depending on network speeds.
7. Once connected, you will see a “CONNECTED” screen appear. The remote device should now be seen on the Logicube device.

10: FREQUENTLY ASKED QUESTIONS

10.0 FAQs

Q. How many concurrent tasks can the ZXi-10G run?

A. The ZXi-10G can run up to 5 concurrent tasks.

Q. Can the ZXi-10G clone to smaller capacity Target drives?

A. Yes. For details on how to clone to smaller capacity Target drives, see *Section 4.0.1*.

Q. How many concurrent tasks can the ZXi-10G run?

A. The ZXi-10G can run up to 5 concurrent tasks.

Q. Do Target drives need to be wiped or formatted using the ZXi-10G?

A. It is not necessary to wipe Target drives before cloning. However, if the user requires wiping Target drives, Logicube recommends using the ZXi-10G to wipe Target drives. The ZXi-10G logs all wipe operations.

Q. Can the ZXi-10G clone Linux partitions?

A. Yes. ZXi-10G can clone Linux partitions using both Mirror mode and Clever Clone mode.

Q. Can the ZXi-10G clone a Hierarchical File System (HFS) or the new Apple File System (APFS)?

A. Yes, ZXi-10G can clone HFS or APFS using Mirror mode.

Q. How does the ZXi-10G handle bad sectors found on the Master drive?

A. ZXi-10G will retry the bad sector 7 times. After the 7th attempt, if the sector still cannot be read, it will skip that sector (by default) and list the sector in the log file.

Q. What operating system does ZXi-10G use?

A. ZXi-10G 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-10G features the ability to create up to 5 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-10G GUI select the Macro and the ZXi-10G 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-10G image to or from a network location?

A. Yes. The ZXi-10G includes two 10GbE and two Gigabit Ethernet ports. Users can designate a network share as a repository using CIFS, SMB, NFS, or iSCSI protocols.

Q. Does the ZXi-10G provide log files?

A. Yes, each operation/task produces a log file. The log file is viewable on the ZXi-10G screen (or remotely on a PC) in an HTML format. The log files can be exported to a thumb drive (the ZXi-10G 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-10G and are accessible by pressing the log file icon from the left-side navigation bar on the ZXi-10G screen.

Q. If I am imaging to or from USB enclosures, will the ZXi-10G's USB ports power my devices, or will an additional power source be required?

A. Each of the ZXi-10G'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-10G image to an external storage device such as a NAS (Network Attached Storage)?

A. Yes, ZXi-10G can image to external storage devices. The external device can be connected to ZXi-10G through the Gigabit Ethernet port or using the target ports (USB 3.0 or the SAS/SATA) built into ZXi-10G. 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-10G can be imaged directly to the external storage device.

11: 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 11 (Bullseye) (https://www.debian.org/)
Linux Kernel (5.10.46-4) (GPL v2) (http://www.kernel.org) (modified)
libcli (1.9.5) (LGPL v2.1) (https://github.com/dparrish/libcli) (modified)
ntfs-3g (1:2017.3.23AR.3-4) (GPL v2) (https://packages.debian.org/source/stretch/ntfs-3g) (modified)
sleuthkit (4.10.1+dfsg-1) (GPL v2/CPL v1.0/IBM-PL v1.0) http://www.sleuthkit.org/sleuthkit)
libewf (20210426-1) (GPL v2) (https://github.com/libyal/libewf)
exfat (1.3.0-2) (GPL v2) (http://opensource.samsung.com/) modified
PDFJS (1.0.907) (Apache License v2.0) (https://github.com/mozilla/pdfjs-dist) (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 ZXi-10G 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-10G and power it back up, this should clear any temporary loss of functionality.