Protecting Your Digital Assets™

User Manual for

TOUGHTECH® Q

(Revised May 14, 2012)

Models covered:

ToughTech Q

ToughTech Q with WriteLock™

ToughTech Secure Q

ToughTech Secure Q with WriteLock

Features

- **Fast speed** – ToughTech Q uses fast SATA drives and an Oxford 934 chipset to maximize data speeds.
- **Widely Compatible** –ToughTechs work right out of the box with no new drivers needed. They work with any modern operating system including Mac OS X, Windows XP/Vista/7 and most Linux distributions.
- **Easy to connect** – ToughTech Q offers four different connection options: FireWire 800, FireWire 400 (via included convertor cable), eSATA, and USB 2.0. Cables for each connection type are included.
- **Shock absorption** – Your car has shock absorbers, so why not your hard drive? ToughTech Q features FlexMount™ Anti-Shock Protection. FlexMount is a shock absorber between the drive and outer shell that protects your data against bumps and vibrations.
- **Cool and quiet** – ToughTech has an all-aluminum design meant to draw heat away from the hard drive. The entire product acts like a heat dissipater, helping to keep your drive cool. And because it doesn't need a fan, ToughTech is quiet.
- **Government-strength encryption** – The Secure model includes a hardware-based real time encryption engine using AES, the government approved encryption standard. Just plug in the hardware key and your ToughTech Secure is usable like any other external drive with no speed loss. If your product is lost or stolen, you can rest assured that no one will be able to access the data without the key.
- **Optional write-protection –** ToughTech models with WriteLock allow you enable and disable write protection to ensure the security of your important data.

Table of Contents

1. Pre-Installation Steps

1.1 Check the accessories with your ToughTech Q.

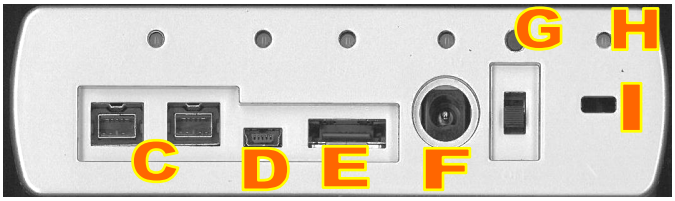
ToughTech Q	
ToughTech enclosure	1
eSATA cable	1
USB cable	1
FireWire 800 cable	1
FireWire 800 to 400 cable	1
Screws for hard drive	4
AC adapter	1
Quick Start Guide and Warranty info	1

ToughTech Secure Q	
ToughTech enclosure	1
eSATA cable	1
USB cable	1
FireWire 800 cable	1
FireWire 800 to 400 cable	1
Screws for hard drive	4
AC adapter	1
Quick Start Guide and Warranty info	1
Encryption Keys	3

1.2 Identify the parts of your ToughTech Q.

Front

A = Power/Access indicator LED
B = Encryption key slot & LEDs (Secure model only)
C = FireWire 800 (1394b) ports
D = USB 2.0 port
E = eSATA port
F = Power input (from AC adapter)
G = WriteLock enable button (for models with WriteLock only)
H = WriteLock LED (for models with WriteLock only)
I = Kensington lock security slot



Rear

1.3 Warnings and notices

Please read the following before beginning installation.

- (Secure model only) Only use the encryption key with the encryption slot on the front of ToughTech Secure. Never insert the key into a mini-USB port, such as the one on the rear of ToughTech Secure! Inserting an encryption key into a mini-USB port will damage the key and render it useless, which can lead to loss of data.
- The main circuit board of the HDD enclosure is susceptible to static electricity. Proper grounding is required to prevent electrical damage to the enclosure or other connected devices, including the computer host. Always place the HDD enclosure on a smooth, flat surface and avoid all dramatic movement, vibration and percussion.
- Avoid placing the HDD enclosure close to magnetic devices (such as a speaker), high-voltage devices (such as a hair dryer), or near a heat source, including any place where the product will be subject to direct sunlight. Do NOT allow water to enter the HDD enclosure.
- The operating system may NOT detect the HDD enclosure if it does not support the interface of your HDD enclosure. If so, installation of an appropriate driver on the host computer is required.

2. Installation Steps

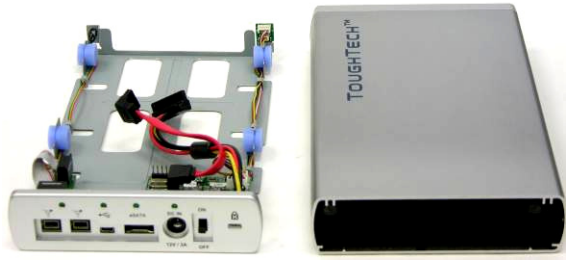
2.1 Hard drive installation

These instructions are only necessary if you're installing your own hard drive inside the ToughTech. If you purchased the product with a hard drive pre-installed, you may skip to the next section (Connecting ToughTech to a Computer).

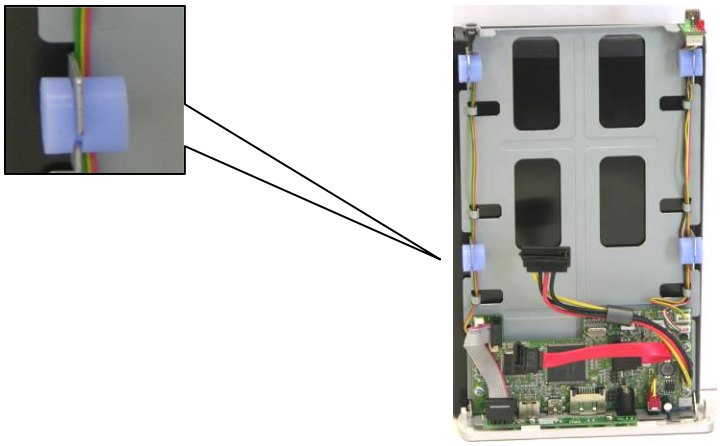
2.1.1 If the rear panel is secured with screws, remove them using a small Phillips screwdriver. (For your convenience, empty enclosures are usually shipped with these screws already removed. They should be located in the same plastic bag as the hard drive screws.)

2.1.2 Push the bottom panel out of the housing. Adequate pressure must be applied to slide it out.

When disassembled, the enclosure will appear similar to the picture below.



2.1.3 Ensure that the shock absorbers are installed in the mounting brackets with the “thin” side facing outward.



2.1.4 Rest your 3.5” SATA hard drive in the tray. Connect ToughTech’s data and power cables to the receptacles on the hard drive, as shown in the pictures below.

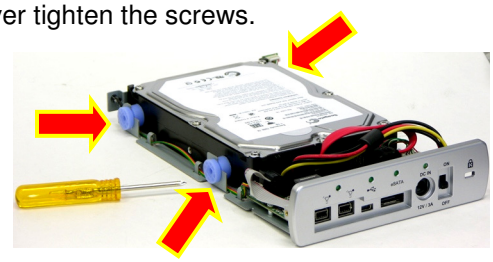
SATA Power

SATA Data

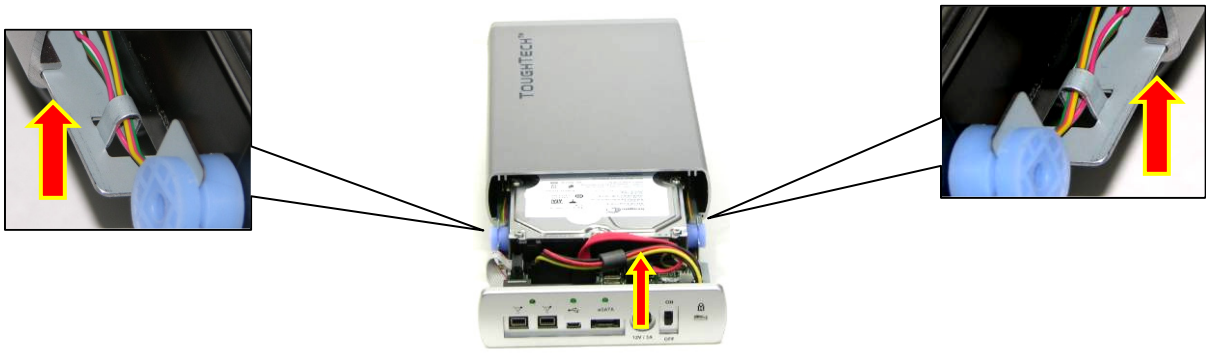
2.1.5 Locate the plastic bag containing four auto-limiting screws included in the package.

Auto-limiting Screw

2.1.6 Insert and tighten each of the four drive screws, making sure that the holes in the shock absorbers line up with the screw holes on the sides of the drive. The shock absorbers will compress slightly, but do not over tighten the screws.



2.1.7 Align the edges of the hard drive platform with the internal rails of the outer housing, and carefully slide the platform into the enclosure.



2.1.8 Fasten the rear panel to the enclosure housing by replacing the screws removed in step 1.

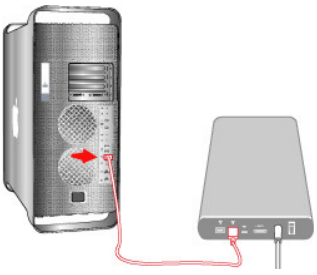
ToughTech is now assembled and ready for connection to a computer.

2.2 Connecting ToughTech to a computer

2.2.1 Connect the USB, FireWire, or eSATA connector into the corresponding port on ToughTech.

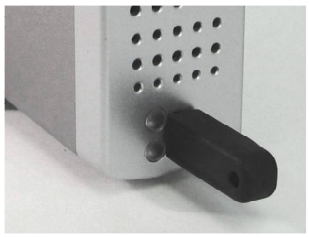
2.2.2 Connect the AC power adapter to the rear of ToughTech. Plug the other end into a grounded electrical outlet.

2.2.3 Plug the other end of the data cable to an available port on your computer. Turn on the power switch; ensure that the green power LED indicator is active. The power LED will blink whenever the drive is accessed.



NOTE: Most computers do not have a built-in eSATA connection. If you wish to connect this way, you may need to install an expansion card inside your computer to add eSATA connectivity. Such cards are sold by WiebeTech and other dealers of computer hardware.

2.2.4 (For the "Secure" model only) Insert the encryption key into the slot on the front of the product. The green encryption LED will light indicating that the drive is now unlocked. If you do not plug in the key, your computer will not see the drive and the red encryption LED will remain lit while ToughTech waits for a key.



After the drive mounts to the computer, you may unplug the key. It will not be needed again until you cycle power on ToughTech.

2.2.5 Your ToughTech is now ready to use! If your hard drive is already formatted, you can begin using it right away. If the hard drive is brand new or its format is not compatible with your computer, you'll need to format the drive before you can use it.

3. WriteLock Information

The information in this section applies only to ToughTech models with the WriteLock feature.

The WriteLock feature lets you "lock down" your data with write-protection. Write-protection is enabled and disabled with a few simple steps.

3.1 Enabling write protection

3.1.1 Turn the power off using the power switch.

3.1.2 Press and hold the WriteLock enable button while switching the power back on. The yellow WriteLock LED will turn on. (In "Secure" models, the encryption key must be inserted for the LED to light.)

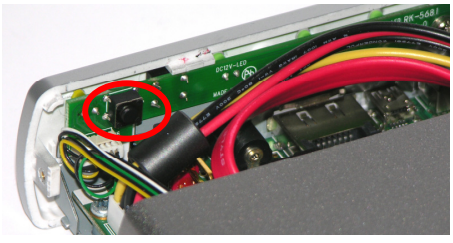
The unit is now in write-protect mode. While in write-protect mode, the data on the drive cannot be deleted or altered.

3.2 Disabling write protection

3.2.1 Switch the power off

3.2.2 Slide the bottom panel out of the housing.

3.2.3 Locate the WriteLock disable button on the inside of the rear panel (circled in red in the picture at right).



3.2.4 Press and hold the WriteLock disable button while switching the power back on. The WriteLock LED on the rear panel will turn off. (In "Secure" models, the key must be inserted for the LED to light.) The unit is now in read/write mode.

With WriteLock, you can prevent the data on ToughTech from being altered when ToughTech changes hands. By adding evidence tape over ToughTech's chassis screws, you'll be able to tell if the unit has been opened. Thus, you'll know if the write-protect mode could have been changed while ToughTech was in another person's possession.

4. Encryption Information

The information in this section applies only to the "Secure" models of ToughTech.

ToughTech Secure employs hardware-based AES 128 or 256 encryption to protect your data from unauthorized access. AES (Advanced Encryption Standard) is a government approved encryption algorithm (FIPS PUB 197). With ToughTech Secure you'll get guaranteed full-disk hardware based encryption, with no loss of speed.

Encryption is performed automatically by ToughTech Secure's real-time encryption engine. Your computer will see the volume available as a normal full-speed drive. If your drive is lost or stolen, however, you can rest assured that without the proper AES Encryption Key, no one will be able to view its contents.

4.1 How to use ToughTech Secure Q with a key

Using ToughTech Secure is very easy.

- Connect the external drive to your computer via FireWire, USB, or eSATA.
- Insert your AES Encryption Key into ToughTech Secure.
- Wait for the green LED to light up on the front of ToughTech Secure. This confirms the key is accepted.
- You can now remove the AES Encryption Key. It's not needed again until the power is cycled.

The ability to remove the key after power up helps you keep your physical key safe.

4.2 AES encryption keys

Your ToughTech Secure comes with 3 identical, programmed keys. These three keys exist so you can

- Keep one with you (for your own use)
- Keep a backup on site in a safe location
- Keep a backup off site in a safe location

These keys will be completely unique to you. If one of your keys is compromised, via theft or loss, you should consider replacing your key set. For your convenience, we offer replacement pre-programmed key sets, which contain unique encryption keys.

4.3 AES encryption key programmer

It is possible for you to create your own keys, should you wish to do so. To program a new encryption key, you will need the AES Encryption Key Programmer (sold separately). While we do not retain copies or records of customers' keys, some customers' security protocols may demand that they have more control over the key itself. There are also situations where more than three keys are needed - for granting access to more than one person, for example. And we're also aware of situations where encryption keys must change on a timed schedule. These customers will be interested in the AES Encryption Key Programmer, which will create or copy their AES Encryption Keys.

5. Usage with Mac and Windows Operating Systems

5.1 Usage with Mac OS X

5.1.1 Compatibility

ToughTech uses 3.5-inch SATA (Serial-ATA) hard drives only. ToughTech does not require drivers for FireWire or USB operation under Mac OS X. ToughTech does not require drivers for eSATA operation, but eSATA host cards do. If installing an eSATA host card into your Mac, use the card manufacturer's drivers and instructions. ToughTech's USB 2.0 port is backwards compatible with USB 1.1 hosts.

5.1.2 Formatting a drive

If you purchased your ToughTech pre-populated with a hard drive, this step should not be necessary unless you wish to change the format or erase the drive. To format, use Mac OS X's Disk Utility (found in the applications folder).

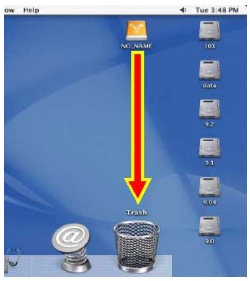
a) Click on the drive in the window to the left (see picture below).

b) Click the Erase tab in the window to the right (see picture below).

c) Select the format type. Most users prefer Mac OS Extended with Journaling (HFS+), which is required for compatibility with Time Machine (OS 10.5 or newer). If you need to use your ToughTech with both Mac and Windows computers, select MS-DOS File System instead.

d) Enter a name for the new volume and then click "Erase" to start the process.

5.1.3 Mounting and unmounting volumes



If the hard drive installed in ToughTech is already formatted, an icon representing the drive's volume will appear (mount) on the desktop. You can begin using the volume right away. If the drive is unformatted, a message will appear on the desktop saying that the disk is unreadable. You can use OS X's Disk Utility to easily format the drive (see section above).

Unmount the volume before powering down the unit by dragging the volume's icon to the trash bin, or by selecting the volume then pressing Command-E. Disconnecting the unit without first unmounting the volume can result in data loss.

5.1.4 Booting from your ToughTech

Some Macs do support booting from a FireWire device. To activate this feature, you must first install OS X on the external volume. The easiest way to do this is to clone an existing system drive using a utility such as Carbon Copy Cloner or Super Duper. Next, go to System Preferences → Startup Disk. A window will list the available bootable volumes. Select the volume from which you wish to boot. Another method is to hold down the Option key during boot up. A screen should appear that allows you to select the volume you wish to use. This is useful if you wish to boot from your ToughTech only some of the time.

5.2 Usage with Windows operating systems

5.2.1 Compatibility

ToughTech uses 3.5-inch SATA (Serial-ATA) hard drives only. ToughTech is fully plug-and-play under Windows XP, Vista, or 7 when using FireWire or USB. No drivers are needed. The USB2 port is USB 1.1 compatible. ToughTech does not require drivers for eSATA operation, but eSATA host cards do. If installing an eSATA host card into your computer, use the card manufacturer's drivers and instructions.

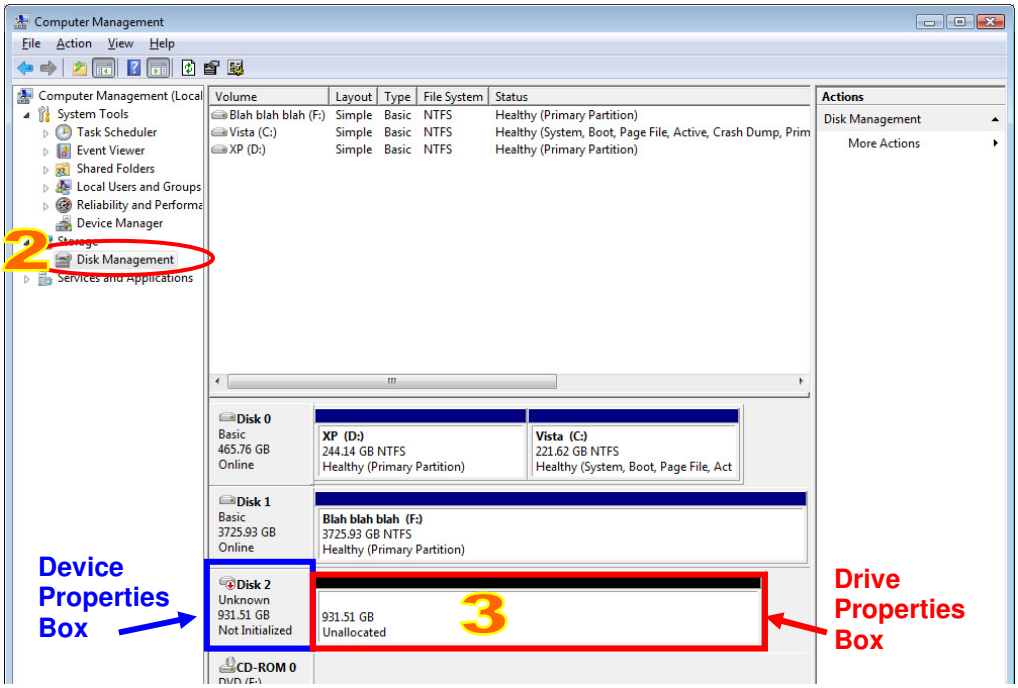
5.2.2 Formatting a drive

If you purchased your ToughTech pre-populated with a hard drive, this step should not be necessary unless you wish to change the format or erase the drive. To format, use the Disk Management utility.

a) Right-click on My Computer, then select Manage. The Computer Management window will open.

b) In the left pane of this window, left-click on Disk Management.

c) The drive should appear in the list of Disks in the lower middle/right pane (see picture below). You may need to scroll down to see it. If the drive is already formatted, you can identify it easily by its volume name. If it's unformatted, the Drive Properties Box will say "Unallocated" and you'll need to initialize the disk before formatting it. Initialize the disk by right-clicking the Device Properties Box and selecting Initialize Disk.



d). To format the drive, right-click the Drive Properties Box and select Format.

e) If you are prompted to select a partition type, select MBR for volumes 2TB or smaller, or GPT for volumes larger than 2TB. Note: Windows XP does not support GPT or volumes larger than 2TB.

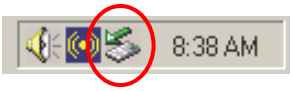
f) Click through several more windows, leaving the default settings, until you see a window that allows selection of a file system. Choose NTFS and enter a name for the new volume. Be sure to check the box labeled "Perform a quick format" unless you want to completely erase any data on the drive and have time to wait. A quick format should take less than a minute, while standard formatting may take several hours.

g) Click "Next" and then "Finish" to start the format process. When the format is complete, the Drive Properties Box will update to show the new volume name. The new volume can now be found in My Computer.

5.2.3 Mounting and ejecting volumes

If the hard drive attached to the ToughTech is already formatted, you can begin using the volume right away. When the ToughTech is properly connected and turned on, a window may open to allow you access to the volume. If no window appears, you can find the volume by double-clicking the "My Computer" icon.

(Windows XP)



Eject the ToughTech before powering it down by single-clicking the green arrow icon on the task bar, then selecting "Safely remove…." Windows will indicate when it is safe to disconnect the ToughTech. Disconnecting the unit without first ejecting it can result in data loss.

5.2.4 Booting from your ToughTech

Some PC motherboards support booting from an external device. To activate this feature, you will need to adjust the motherboard's BIOS settings. Check with your motherboard's manufacturer or owner's manual for details.

6. Encryption FAQs

Q: What do I do if I lose a key?

A: If the privacy of your data is not a concern, you can continue using your product with your remaining keys. But then, if data privacy were not important, you probably wouldn't own the Secure version of the product. If you can't account for all your keys, your data is not 100% secure. Anyone who finds a key will be able to access your data. Therefore, we recommend that you purchase a new set of programmed keys.

Q: What would happen if I were to plug the key into the USB port on the rear of ToughTech?

A: Do not plug the encryption key into any mini-USB port, including the one on the rear of ToughTech Secure! Although the key will fit in such a slot, they are not electrically compatible. You could damage both the port and the key, rendering the key useless and your data inaccessible.

Q: How do I use a new (or different) key with my Secure product?

A: First, you'll need to back up all your data. Access the data using your old key, and then copy everything you wish to save to a different drive. Next, insert the new programmed key and cycle power on the product. The drive will appear to the computer as an unformatted drive. If you proceed to format the drive, it will be usable again, but only when the new key is used. You can now transfer your data back to the Secure product.

Q: Does your company keep records of the keys you create and ship with products?

A: No, we do not keep any records of the random secret electronic key codes stored on the security keys. The codes are composed of randomly generated 128 or 256-bit numbers which are never stored anywhere except on the security keys themselves.

Q: What do I do if I lose all the keys? Can I retrieve my data? Can you retrieve my data for me?

A: Loss of all keys will make it virtually impossible to recover your data, even for professional data recovery services. The only way to retrieve any data would be to crack the encryption. With AES 128 and 256, that would take a super computer many years to accomplish. There is no "back door" on our encryption products. It is therefore very important that you manage your keys carefully. It is a good idea to keep one key with you, a backup key in a safe location, and another backup in a location off site.

7. General FAQs

Q: When I operate my ToughTech continuously, the case feels very hot. Is this bad for my drive?
A: ToughTechs employ a passive cooling system which conducts heat away from the drive to the aluminum case so that it can be safely dissipated into the surrounding air. This can cause the case to feel very warm, but keeps the drive from reaching dangerous temperatures. It is recommended that ToughTechs not be stacked, and that you leave enough air space around the case for the passive cooling to work efficiently.

Q: After enabling write-protection on my ToughTech with WriteLock, I'm still able to copy a file to the drive. Is the file really there?
A: No. The file only appears to have been copied, but was not actually written to the drive. You can verify this by cycling power on ToughTech. You will find that the copied file no longer appears.

Q: I just connected my eSATA product to my computer for the first time. I turned on the power, but the drive did not spin up. Is the drive dead?
A: SATA drives will not power up if a SATA cable is plugged into them, but no valid connection is established with a host. To test this, unplug the SATA cable, but leave the power plugged in. If the drive spins up in this configuration, then the problem can be attributed to the SATA host (i.e. eSATA host card).

Q: It is possible to boot to the external drive(s) in this product?
A: Only if that feature is supported by the eSATA host to which you are connecting. Individual motherboards and third-party host cards may or may not support this feature. If this feature is important to you, you should read the technical specifications of any host card you're considering to make sure it supports booting.

Q: Do I need to install FireWire drivers for this device?
A: You do not need to install any drivers for FireWire usage with Windows 98SE, ME, 2000, XP, Vista, Windows 7, Mac OS 9.2 or Mac OS X.

Q: I lost my AC adapter. Where can I get a replacement?
A: The AC adapters for all current products (and most discontinued products) are available for purchase on our website. Third party AC adapters can also be used with products as long as they have REGULATED POWER. Be sure to check with the manufacturer of the adapter for this specification. Also check to make sure the volts and amps are correct for the product, as well as the pin configuration (for DIN connectors).

For additional FAQs, please visit cru-dataport.com

8. Technical Specifications

Product Name	ToughTech Q [with WriteLock] ToughTech Secure Q [with WriteLock]
Interface Types & Speeds	• eSATA port: up to 3000 Mbps • FireWire 800: up to 800 Mbps • FireWire 400 (using convertor cable): up to 400 Mbps • USB 2.0: up to 480 Mbps
Chipset	Oxford 934
Drive Compatibility	3.5" SATA hard drives
Data Connectors	One (1) eSATA port One (1) mini-USB port Two (2) 9-pin 1394b (FireWire 800) ports (daisy-chainable)
Encryption	Hardware based AES 128 or 256 encryption engine ("Secure" model only)
Kensington Security Slot	Yes
Operating System Requirements	• Windows 7, Vista, or XP • Mac OS X • Linux distributions that support the connection type used
External Power Supply	100-240VAC +12V / 3A (included)
Compliancy	FCC, CE, RoHS
Shipping Weight	4 pounds without drive; 6 pounds with drive (includes accessories)
Product Dimensions	9" x 5.25" x 1.5" (229mm x 133mm x 38mm)
Support	We don't expect anything to go wrong with your product. But if it does, Tech Support is standing by and ready to help. Contact us at (866) 744-8722 or through cru-dataport.com

Product Warranty
CRU-DataPort (CRU) warrants this product to be free of significant defects in material and workmanship for a period of one year from the original date of purchase. CRU's warranty is nontransferable and is limited to the original purchaser.

Limitation of Liability
The warranties set forth in this agreement replace all other warranties. CRU expressly disclaims all other warranties, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose and non-infringement of third-party rights with respect to the documentation and hardware. No CRU dealer, agent, or employee is authorized to make any modification, extension, or addition to this warranty. In no event will CRU or its suppliers be liable for any costs of procurement of substitute products or services, lost profits, loss of information or data, computer malfunction, or any other special, indirect, consequential, or incidental damages arising in any way out of the sale of, use of, or inability to use any CRU product or service, even if CRU has been advised of the possibility of such damages. In no case shall CRU's liability exceed the actual money paid for the products at issue. CRU reserves the right to make modifications and additions to this product without notice or taking on additional liability.

FCC Compliance Statement: "This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation."

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a home or commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at this own expense.

In the event that you experience Radio Frequency Interference, take the se steps to resolve the problem:

1) Ensure that the case of your attached drive is grounded.
2) Use a data cable with RFI reducing ferrites on each end.
3) Use a power supply with an RFI reducing ferrite approximately 5 in. from the DC plug.
4) Reorient or relocate the receiving antenna.

Tested to comply with FCC standards
FOR HOME OR OFFICE USE