RTX® Secure 410-3QR User Manual

Models Covered:
RTXS410-3QR

- Hardware-based AES 256-bit Encryption – Offers affordable military-grade AES 256-bit data protection that encrypts the entire hard drive–including boot sector, OS, temp, and swap files.
- Meets Industry Standards – All CRU Secure 256-bit product architecture and encryption engine designs meet FIPS140-2, level 3 per certification number 1471, and all CRU AES 256-bit security chips are NIST & CSE validated (FIPS PUB 197).
- Easy-to-Use Security – One physical Security Key is used for all bays and the Security Key can be stored separately from the unit to make the RTX Secure less vulnerable to compromise if the unit is lost or stolen. No PINs or passwords are needed.
- Quadruple Connectivity – RTX Secure 410-3QR is compatible with four different interfaces; USB3, USB2, eSATA, and FireWire 800.

Table of Contents

1. Pre-Installation Steps

1.1 Check the Accessories with Your RTX Secure

The following list contains the items that are included with this device. Please contact CRU if any items are missing or damaged:

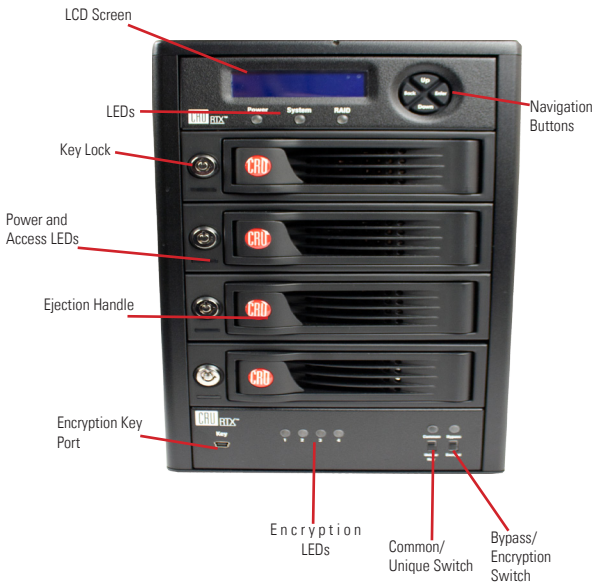
Accessories	Quantity
RTX Secure 410-3QR Enclosure	1
Power cord	1
USB3 Cable	1
USB2 Cable	1
FireWire 800 Cable	1
eSATA Cable	1
ProSoft Data Backup CD*	1
Security Keys	3
Lanyards for Security Keys	3
Security Key ID Tag	3
Security Key Labels	6
Packet of Keys	1

*Exclusively packaged with all SKUs that include hard drives

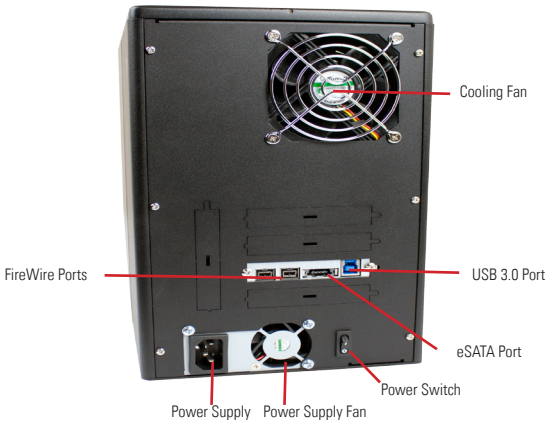
1.2 Identifying Parts

Take a moment to familiarize yourself with the parts of RTX Secure. This will help you to better understand the remaining instructions.

Front of the RTX Secure 410-3QR



Back of the RTX Secure 410-3QR



1.3 Warnings and Notices

Please read the following before beginning installation.

General Care

- The main circuit board of the HDD is susceptible to static electricity. Proper grounding is strongly recommended to prevent electrical damage to the enclosure or other connected devices, including the computer host. Avoid all dramatic movement, tapping on the unit, and vibration.

- Avoid placing hard drives close to magnetic devices, high voltage devices, or near a heat source. This includes any place where the product will be subject to direct sunlight. Do NOT allow water to make contact with the drives or enclosure.

- Before starting any type of hardware installation, please ensure that all power switches have been turned off and all power cords have been disconnected to prevent personal injury and damage to the hardware.

- To avoid overheating, the RTX enclosure should be operated in a well-ventilated area and in such a way that sufficient airflow is maintained across the controller chips.

- Remove the drives before transporting the RTX enclosure to prevent damage to the drive interfaces.

RAID

- Use only hard drives that are in perfect condition. Avoid using drives that have ever developed bad sectors during previous usage. This could lead to possible device failure or loss of data.

- RTX Secure 410-3QR supports SATA hard drives of various specifications and different capacities. However, we recommend using drives of the same brand and type for optimal performance. If drives of different capacities are used in a RAID, the capacity of the smallest drive will determine how much of each drive is used. The additional capacity on the larger drives will not be used by the RAID.

- RAID level 0 will allow you to use the full combined capacity of the drives, and offers the best data transfer speeds. However, RAID 0 offers no protection for the data. If one drive fails in a RAID 0, the data on all of the drives is irretrievably lost. Before creating a RAID, investigate the various RAID types and choose the one that is best for your needs.

- Always back up data before switching RAID types. **Switching RAID types will destroy current data. You must reformat your drives afterward.**

Encryption

- Though the Security Key port is mechanically identical to the standard Mini-USB port, inserting Security Keys into any other Mini-USB port may damage the keys and render them useless. Please only use Security Keys in RTX Secure products.

- Likewise, inserting a Mini-USB cable or other device into the RTX Secure Security Key port on the carrier may cause internal damage and potentially lead to loss of data.

- Any time power is cycled on the RTX Secure, the Security Key should be installed prior to recycling the power in order to access the data on the drive.

2 Introduction to RAID

A RAID (Redundant Array of Independent Disks) is an array of multiple hard drives that are combined in a way that provides faster performance and/or data safety. Your RTX unit is capable of creating and managing several different varieties of RAID. You may choose your preferred RAID level based on factors such as disk capacity, desired data safety, and desired performance.

2.1 Summary of RAID Levels

The RTX Secure 410-3QR supports RAID Levels 0, 1, 5, and 10. RAID Level 5 is most commonly used by those seeking an optimal balance of speed and data safety.

RAID Level	Description	Required No. of Drives*	Data Redundancy
0	Also known as striping. Data distributed across multiple drives in the array. *There is no data protection.*	2	No data protection
1	Also known as mirroring. All data replicated on two separate disks. This is a high availability solution, but due to the 100% duplication, only half the total disk capacity is available for data storage.	2	1 drive
5	Also known as Block-Interleaved Distributed Parity. Data and parity information is subdivided and distributed across all disks. Can withstand the failure of one drive. The total capacity of all but one of the drives is available for data storage.	3 or 4	1 drive
10	Also known a stripe of mirrors. Data is striped across two separate disks and mirrored to another disk pair.	4	1 drive**

* The RAID level becomes available as a menu option when exactly these numbers of hard drives are installed inside of the RTX enclosure.

**If both drives in either the RAID 0 or RAID 1 set fail, then the entire RAID will fail. If only one drive in each of the RAID 0 and RAID 1 sets fail, then the RAID is preserved.

2.2 Hot Spares (Host Standby)

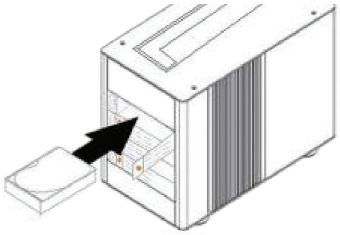
Hot spares are connected as part of your RAID and are switched into operation when a drive fails. RAID 5 will support hot spares when configured with three hard drives (displayed as a "RAID5 3d" on the LCD). When a drive fails, the RTX enclosure will immediately rebuild the RAID. After that a new drive will need to be inserted in place of the failed one. Replacement drives should preferably be the same model and capacity as the failed one.

3 Installation Steps

3.1 Hard Drive Installation

a. Pull the ejection handle on the TrayFree bay to open the bay door.

b. Insert a SATA hard drive into the bay. Make sure it is label-side up with the SATA connection on the drive inserted first toward the rear of the enclosure.



c. Shut the bay door.

Sticker Card

Use the stickers on the provided sticker card to label each drive if you plan to use Unique Encrypted Mode (see Section 3.2). This will prevent the drives from getting mixed up when they are removed from the bays.

3.2 Setting the Encryption Mode

The RTX Secure has three modes that determine how it handles Security Keys. The status of the mode is determined at power up. After the unit has been successfully mounted by the system, the Security Key may be removed and stored in a safe location. Changing the position of the switches on the bottom of the RTX after the unit has successfully been mounted will not change the mode used at power up.

Note: Always ensure that the correct encryption mode is selected before powering on the RTX Secure. Failure to do so may result in a failed RAID alarm. This will not affect your data, which will become accessible once the correct encryption mode is set.

Unique Encrypted Mode

This is the most secure mode of operation. A Security Key is required to access data, and each bay is loaded with its own unique 256-bit security value from the Security Key. These security values are all stored in one Security Key. Each time a hard drive is loaded into the RTX Secure, it must be loaded into the same bay. Flip the left switch on the bottom panel down to "Unique" and the right switch down to "Encrypted."

Common Encrypted Mode

This mode allows hard drives to be located in different bays within the unit after the array is formatted. A Security Key is required to access data. Each bay uses the same security value from the Security Key. Flip the left switch on the bottom panel up to "Common" and the right switch down to "Encrypted." The Encryption Display Common Key LED will illuminate.

Bypass Mode

A Security Key is not required to access data. This option cannot be used with encrypted hard drives. Flip the right switch on the bottom panel to "Bypass." This option disables the Common/Unique switch. The Encryption Display Bypass LED will illuminate and the drive bay Encryption Active LEDs will remain off.

Note: When switching the encryption mode, the RAID controller will still see a valid volume even when it shouldn't. You must rebuild the RAID whenever you change the encryption mode. Failure to do so will not result in the loss of data, but will result in the inability to see some or all established RAID sets.

3.3 Operating The RTX Secure

a) Connect the RTX Secure to a power outlet with the included power cord.

d) Install the hard drives into the RTX Secure (See Section 3.1).

e) Set the desired encryption mode (See Section 3.2).

f) Insert the Security Key into the Mini-USB Security Key Port on the bottom of the RTX Secure if the drives being used in the RTX Secure are encrypted or intended to be encrypted.

g) Turn on the RTX Secure by flipping the switch on the rear of the unit.

h) When using the Unique or Common Encrypted Modes, wait for each LED along the bottom panel of the RTX Secure to light green. These encryption status LEDs correspond to one of the TrayFree Bays above them with the leftmost LED representing the top bay and the rightmost LED representing the bottom bay. When all encryption status LEDs that correspond to a bay with a drive inside are lit green, encryption is activated and the Security Key may be removed and stored in a safe location.

i) Configure your drives with at least one RAID set. Follow the appropriate setup instructions in Section 6.

Once a RAID set has been created, it will show up as a blank, unallocated volume and you'll need to format it before you can use it. **Note that formatting a volume or creating a RAID set will erase all data on the hard drive, so be sure to back up your data before installing the hard drives into this enclosure and before beginning this operation.** See Section 10 for instructions on how to format the volume with Mac or Windows operating systems.

3.4 Optional Configuration Settings

Missing Security Key Notification

After the RTX Secure performs its power-on self-test and there is no Security Key inserted, there is a five-second period where the encryption status LEDs will blink red and orange. During this period of time, a Security Key can still be inserted. When the RTX Secure detects the key's insertion, it will continue its power on sequence.

Hot Swapping Encrypted Hard Drives

Hot swapping of hard drives is supported by the RTX Secure as a default feature. Make sure the correct Security Key is installed when hot swapping an encrypted hard drive. If the Security Key is not installed or an incorrect Security Key is detected, the bay will not power up and the bay's Encryption Status LED will flash orange.

4 LED Behavior

LED	Behavior
Unit Power	Glows green when the power switch is in the "on" position.
System	• Glows **green** when system is performing as expected. • Glows **amber** when a drive or the enclosure interior reaches the preset warning temperature. • Glows **red** when a drive or the enclosure interior exceeds the preset warning temperature.
RAID	• Glows **green** when system is performing as expected. • Glows **amber** when the RAID is degraded or is being rebuilt. • Glows **red** when the RAID has failed or is invalid.
Drive Power	Glows **green** when the drive is in the unit and receiving power.
Drive Activity	Glows **amber*** when the drive is being accessed, either reading or writing from the drive.

* The Drive Activity LED is controlled directly by the hard drive. When certain models of hard drives are used, the amber glow may remain constant or will not light. This is considered normal operation.

5 LCD Menu Screens

Use the Navigation Buttons to change screens.

Screen	Description
Mode	Shows the RAID level used.
Status	Indicates the overall health of the RAID. Available status messages are Normal or Degraded.
Disk	Indicates the status of the individual disk in the numbered hard drive slot: • **OK**: Indicates that the hard drive is in use or ready to use • **No Disk**: Indicates that the hard was removed or not installed • **Unused**: A new drive was installed and is not used by the RAID • **Failing:** Indicates the drive is malfunctioning.
Disk Temp	Displays temperature of the individual disk in the numbered slot.
Sys Temp	Displays overall temperature inside the system.
Fan Status	Indicates whether the fan is operating normally or has failed and is in need of a replacement. Contact Technical Support if the fan has failed to arrange for a repair.
Change RAID Mode	Allows you to change the RAID level (see section 6.2).

6 RAID Configuration

You may skip this section if you purchased the RTX Secure 410-3QR pre-configured with drives. The RTX Secure 410-3QR ships with RAID 5 as the default mode.

The RTX Secure 410-3QR offers four options for RAID configuration. See Section 2.1 for details on the available options. Stop all data transfers before setting or changing RAID types or rebuilding a degraded array.

Failure to do so can result in the loss of data. To set up or change the RAID type, disconnect all data cables and reboot the RTX. After the unit has initialized, the LCD will display the drives' mode and status.

6.1 Creating a New RAID

Use the LCD and menu selection buttons to complete these steps if you did not purchase your unit pre-configured. **Changing RAID levels will erase any data on the drives. Make a backup copy of any data you wish to keep before changing the RAID.**

a. Disconnect the RTX enclosure from the computer.

b. Insert four hard drives (preferably all the same make, model, and capacity) into the RTX enclosure and flip the power switch on the rear of the unit.

c. After the RTX enclosure boots up, it will begin alarming and the LCD will display the error "Error: Not a RAID Set". Press the **Enter** button to silence the alarm.

d. Press the **Enter** button a second time and the LCD screen will ask "Make New RAID?" Press **Enter** to confirm.

e. The LCD will display "Select RAID Type". Press **Up** or **Down** to cycle through to your desired RAID type and press **Enter**.

f. The screen will display "Will Erase all Data OK?" **Pressing Enter will result in the loss of all data on the drives.** Ensure all data is backed up, then press **Enter**.

g. The new configuration will be selected and the RTX enclosure will reboot. The RAID is now created.

6.2 Changing the RAID Type

a. Disconnect the RTX enclosure from the computer.

b. Press the **Up** button to cycle the LCD menu to the "Change RAID Mode" screen and press the **Enter** button.

c. The LCD will display "Select RAID Type". Press **Up** or **Down** to cycle through the available options to your desired RAID type and press **Enter**.

d. The screen will display "Will Erase all Data OK?" **Pressing Enter will result in the loss of all data on the drives.** Ensure all data is backed up, then press **Enter**.

e. The new configuration will be selected and the RTX enclosure will reboot. The RAID is now created.

f. The RTX enclosure has been configured and is ready for operation. Follow the instructions for the appropriate operating system usage instructions to initialize and format the drives.

6.3 Adding a New Drive to a RAID

The Security Key must be present when any failed drives are replaced. If the Security Key is not installed or an incorrect Security Key is detected, the bay will not power up and the bay's Encryption Status LED will flash orange, preventing the RAID from rebuilding.

Always ensure that the correct encryption mode is selected before powering on the RTX Secure. Failure to do so may result in a failed RAID alarm. But don't worry, your data will remain intact and will be accessible once the correct encryption mode is set.

NOTE: Any data on the new hard drive will be destroyed when the drive is added to the RAID.

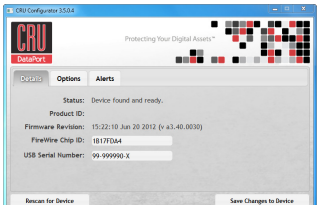
RAID 0

Never remove a drive from a RAID 0 as this will cause the loss of all data. In the event of a disk failure for a RAID 0, the RAID will be destroyed. Add a drive and then press the Up button to create a new RAID. Follow the display prompts to build a new array.

RAID 1, 5, and 10

In the event of a disk failure or removal, the RAID will continue to function in a degraded state. Add a new disk to the RTX Secure 410-3QR to rebuild the RAID. After the new drive has been detected, the RTX enclosure will ask to add a new disk. Press the Enter button to do so. The disk will be added to the RAID and the RAID will begin to rebuild. The LCD screen will display the percent complete for the rebuild. Rebuild times vary, a 1TB hard drive takes just over 3 hours to rebuild. You can toggle to the approximate time remaining by pressing enter on the front panel.

7 Buzzer and Temperature Configuration

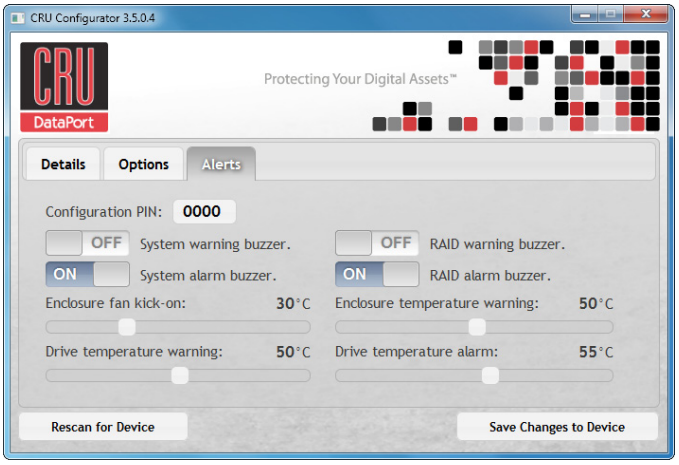


The RTX Secure 410-3QR is compatible with CRU Configurator 3.5 or higher, which allows IT administrators to change internal settings to meet individual needs. Configurator allows the user to set the password, enable and disable audible alarms, and change temperature alarms and warnings settings. To download Configurator and the full Configurator manual, visit www.wiebetech.com/software/configurator.php.

7.1 Accessing Configurator

In order for Configurator to access the RTX enclosure, connect RTX Secure 410-3QR to the computer via USB 2 or FireWire.

7.2 Customizable Options



The following options are available on the **Alerts tab** of the Configurator:

Configuration PIN

This feature allows you to set a PIN to prevent unauthorized configuration. The default PIN is 0000. The RTX enclosure only requires you to enter a PIN if a different value has been set.

Buzzers

Place a check in the boxes to indicate which warning/alarm buzzers you want to be activated or remove a check from the boxes next to the buzzers you want to deactivate. When a buzzer sounds, press **Enter** on the front of the RTX enclosure to temporarily silence it until the RTX enclosure is next rebooted.

System Warning Buzzer

This buzzer will sound when a drive reaches the temperature set using the **Drive temperature warning slider** below. This buzzer is disabled by default. As a visual alert, the System Status LED will glow amber when the temperature is reached, regardless of whether the buzzer is enabled or not.

System Alarm Buzzer

This buzzer will sound on 3 occasions:

- When a drive reaches the temperature set using the **Drive temperature alarm slider** below
- When the enclosure reaches the temperature set using the **Enclosure temperature warning slider** below
- When the fan fails

As a visual alert, the System Status LED on your RTX enclosure will glow red when any of these three situations occur, regardless of whether the buzzer is enabled or not.

RAID Warning Buzzer

This buzzer will sound when the RTX enclosure is in degraded RAID mode (a drive has failed and is in need of rebuild or the RAID is rebuilding). This buzzer is disabled by default. The RAID Status LED will glow amber if this occurs, regardless of whether the buzzer is enabled or not.

RAID Alarm Buzzer

This buzzer will sound when the RAID has failed or is invalid. The RAID Status LED will glow red if this occurs, regardless of whether the buzzer is enabled or not.

Temperature Sliders

When your RTX enclosure reaches a certain temperature, buzzers will sound if they are enabled (see the Buzzers subsection above) and the fan will kick on. You may want to change these default temperatures according to your environment. With these sliders, you can change the default temperatures of the:

- Enclosure fan kick-on
- Enclosure temperature warning
- Drive temperature warning
- Drive temperature alarm

8 Usage with Mac and Windows Operating Systems

8.1 Usage with Mac OS X

8.1.1 Formatting a Drive

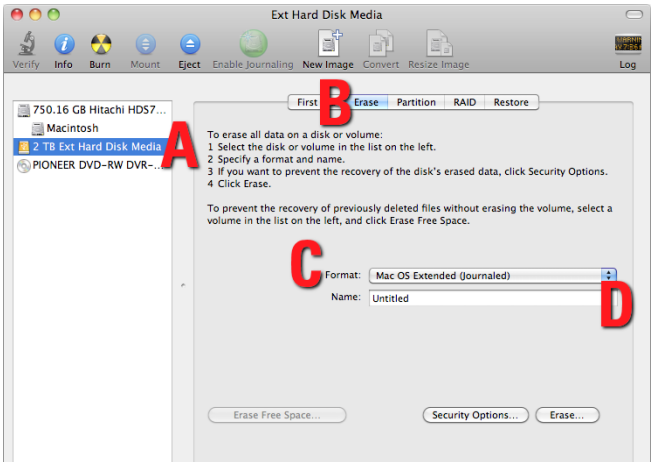
To format, use Disk Utility (pictured above, right), which can be found in the Applications folder.

a. Click on the drive in the window to the left.

b. Click the **Erase tab** in the window to the right.

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 RTX 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.



8.1.2 Mounting and Unmounting Volumes

If the hard drive installed in the RTX enclosure 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. 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**, or by selecting the volume then pressing **Command-E**. Disconnecting the unit without first unmounting the volume can result in data loss.

8.1.3 Creating a Boot Drive

To activate this feature, you must first install OS X on the hard drive in your carrier. 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 are only sporadically booting from the RTX hard drive.

8.2 Usage with Windows Operating Systems

8.2.1 Formatting a Drive

When you first mount a drive to a Windows operating system, a pop-up window will ask you if you would like to format it. Click **Format Disk** and skip to Step F. If the prompt does not pop up, use the Disk Management utility by following these steps:

a. Right-click on the **My Computer icon** on the desktop (Windows XP) or the **Computer button** in the Start Menu (Windows Vista, 7, Server 2008, Server 2008 R2, Server 2012), then select **Manage**. For Windows 8, select your **Desktop**, then open **Windows Explorer** from the toolbar. Right-click on **Computer** in the left-hand navigation pane and select **Manage**. The Computer Management window will open.

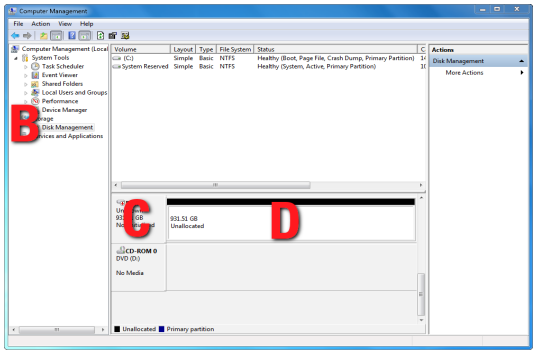
b. In the left pane of this window, left-click on **Disk Management** (labeled 'B' in the picture below).

c. The drive should appear in the list of Disks in the lower middle/right pane. 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 the Device Properties Box (labeled 'C' in the picture below) says "Not Initialized", you'll need to initialize the disk before formatting it.

Right-click on the **Device Properties Box** and select **Initialize Disk**. 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 for volumes larger than 2TB.

d. To format the volume, right-click the **Drive Properties Box** (labeled 'D' in the picture below) and select **New Partition…** (Windows XP) or **New Simple Volume...** (Windows Vista, 7, 8, Server 2008, Server 2008 R2, Server 2012).



e. Unless you wish to customize the settings in these dialog prompts, Click **Next** on the Select Partition Type (shows up in Windows XP only), Specify Volume/Partition Size, and Assign Drive Letter or Path dialog prompts, leaving the default settings.

f. You will now 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 **Quick Format**, which will ensure that the formatting process takes less than a minute.

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 by double-clicking on the My Computer icon on the desktop (Windows

XP), by clicking on the Computer button in the Start Menu (Windows Vista, 7, Server 2008, Server 2008 R2), or by clicking on "Computer" in the navigation pane of a Windows Explorer window (Windows 8, Windows Server 2012).

8.2.2 Mounting and Unmounting Volumes

If the hard drive inside of the RTX Secure are in a RAID which is already formatted, you can begin using the volume right away. When the RTX Secure is properly connected and turned on, a window may open to allow you access to the volume. If no window appears, find the volume by double-clicking on the My Computer icon on the desktop (Windows XP), by clicking the Computer button in the Start Menu (Windows Vista, 7, Server 2008, Server 2008 R2), or by clicking on Computer in the navigation pane of a Windows Explorer window (Windows 8, Windows Server 2012).

Unmount the RTX Secure before powering it down by left-clicking the green arrow icon on the task bar (in Windows XP) or the USB plug icon with the green checkmark on the Desktop task bar (Windows Vista, 7, 8, Server 2008, Server 2008 R2, Server 2012), and then selecting the proper device from the menu that pops up. You may have to click on the "Show Hidden Icons" arrow on the task bar to find the correct icon. Windows will indicate when it is safe to disconnect the RTX Secure. Disconnecting the unit without first ejecting it can result in data loss.

9 RAID Is Not A Backup

Because your RTX Secure features redundant RAID modes which protect against a hard drive mechanical failure, it is an excellent part of any backup strategy. However, a RAID is not, in itself, a backup strategy. Many things besides hard drive failure can damage or erase your data:

- Corruption caused by unexpected disconnection during data access (e.g. a cable is unplugged during a data transfer, or the computer crashes or loses power while writing to the drives)
- Corruption or destruction caused by viruses or other malware
- Sabotage by a disgruntled employee or acquaintance
- Theft of your RTX Secure
- Natural disasters such as fire, flooding, etc.

Considering these possibilities, any single copy of your important data must always be considered at risk. That's why backing up is so important. Follow the 3-2-1 backup rule. Data should exist in three different places on two different storage media and at least one of those copies should be maintained offsite.

Without an effective backup strategy, recovering data may be impossible, or the cost of data recovery may be quite expensive. The CRU warranty does not cover costs associated with data loss (nor do the warranties of other hard drive manufacturers).
Plan accordingly and backup data to minimize downtime!

10 Encryption

- The RTX Secure uses full disk hardware encryption to encrypt the entire contents of the drive—including the boot sector, operating system and all files—without performance degradation.
- The Security Key must be installed prior to powering on the RTX Secure for the data to be decrypted on the drive. If the key is externally connected to the Mini-USB Security Key Port and is not internally installed, then once it has been accepted, it may be removed and stored in a safe location. Always store Security Keys apart from the data so that in the event that the drive is lost or stolen, the data is protected.
- When a drive is formatted using an encryption key, the same or a duplicate key must be used in order to access the data. There is no "back door" to access the data; lost keys make data recovery virtually impossible.

11 FAQ

Why won't my hard drives mount on my computer?

If the drives are encrypted, make sure that Bypass Mode is not engaged at power up. If it is, set the encryption mode to the appropriate mode and then recycle power on the enclosure. If the drives are not encrypted, then make sure that Bypass mode is engaged, or the drives will not mount.
If the encryption mode is correct, check to make sure you are using the correct Security Key. Then refer to Section 3.3 for the proper procedure on starting up the RTX Secure with a Security Key.
Next, try removing each drive from the RTX Secure and reseating them in their TrayFree Bays.If you are connected via eSATA, make sure you have eSATA drivers properly installed in your OS.

I've attached my RTX Secure 410-3QR and can see the volume, but it shows up twice. Which one is real?

If you are seeing your RTX Secure volume mounted twice, chances are the unit is connected to the computer using both the eSATA and FireWire connections. When this is the case, the OS may attempt to mount the RTX Secure twice resulting in two volumes appearing. Simply unmount the volumes, turn off the RTX Secure, and unplug one of the connections to resolve the problem.

Is there a way to use Bypass Mode on certain bays and use an encryption mode on others?

There is no way to bypass individual bays and set others to use an encryption key.

RTX Secure is complaining that my RAID is degraded or failed, and replacing disks does not solve the issue. Why?

Check the encryption mode to make sure that Unique Encrypted Mode is selected. When the drives are encrypted with unique encryption keys, but the RTX Secure is set to Common Encrypted Mode, only the top bay drive will mount, and consequently the RTX Secure will complain that the RAID has degraded or failed. But don't worry, your data will remain intact and will be accessible once the correct encryption mode is set. This is because the Security Key

can hold a unique 256-bit security value for up to 8 bays and only the first value on the Security Key is used when the RTX Secure is set to use Common Encrypted Mode. As a result, the first bay will be accessible, but all other bays will fail the encryption check since the first security value will not match the security values used to encrypt the other drives.

I used to see all of the drives in the RTX Secure mount on my computer, but now only the top bay drive mounts. Why?
Check the encryption mode to make sure that Unique Encrypted Mode is selected. When the drives are encrypted with unique encryption keys, but the RTX Secure is set to Common Encrypted Mode, only the top bay drive will mount, and consequently the RTX Secure will complain that the RAID has degraded or failed. But don't worry, your data will remain intact and will be accessible once the correct encryption mode is set. This is because the Security Key can hold a unique 256-bit security value for up to 8 bays and only the first value on the Security Key is used when the RTX Secure is set to use Common Encrypted Mode. As a result, the first bay will be accessible, but all other bays will fail the encryption check since the first security value will not match the security values used to encrypt the other drives.

12 Technical Specifications

Product Name	RTX Secure 410-3QR
RAID Levels	RAID 0, 1, 5, 10
Interface Types & Speeds	• USB2: up to 480 Mbps • USB3: up to 3.2 Gbps • eSATA: up to 3 Gbps • FireWire 800: up to 800 Mbps
Compatibility	3.5" SATA hard drives (SATA1, SATA2, and SATA3)
LED Indicators	• Power Indicator • System Indicator • RAID Indicator • Bay Power Indicator (one per bay) • Disk Activity Indicator (one per bay)
Controller Display	LCD screen with backlight/control panel
Operating System Requirements	• Windows 8, 7, Vista, or XP • Windows Server 2012, 2008, and 2003 product families • Mac OS X 10.4.x or higher • Linux distributions that support the connection type used
Power Switch	2 position: On / Off
Power Supply	Input: 100-240VAC Output: 120 Watts
Compliance	EMI Standard: FCC Part 15 Class A, CE EMC Standard: EN55022, EN55024
Shipping Weight	13 pounds (without drives) 18 pounds (with drives)
Dimensions	10.63" x 6.89" x 7.87" (270mm x 175mm x 200mm)
Technical Support	Contact us at www.cru-inc.com/support. We also offer phone support at (800) 260-9800 or (360) 816-1800.

Limited Product Warranty
CRU-DataPort (CRU) warrants this product to be free of significant defects in material and workmanship for a period of three years 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 A 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.

In the event that you experience Radio Frequency Interference, you should take the following 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 inches from the DC plug.
4) Reorient or relocate the receiving antenna.

FC Tested to comply with FCC standards
FOR OFFICE OR COMMERCIAL USE