5. Technical Specifications

Product Name	RTX Secure 410-3QR
Compatibility	3.5" SATA hard drives
Interface Types and Speeds	USB2 (via USB3 connector): up to 480 Mbps USB3: up to 3.2 Gbps eSATA: up to 3 Gbps FireWire 800: up to 800 Mbps
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	22 pounds (without drives), 28 pounds (with drives)
Product Dimensions	(274mm x 177mm x 268mm)
Technical Support	Contact us at www.cru-dataport.com/support. We also offer phone support at (800) 260-9800 or (360) 816-1800.

Limited Product Warranty
CRU-DataPort (CRU) warrants RTX 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 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, 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

RTX™ Secure 410-3QR Quick Start Guide

For the full user manual and more information about this product, visit www.cru-dataport.com.

Models Covered:
RTX Secure 410-3QR

1. Installation Steps

1.1 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.
d. You can optionally secure each bay door by inserting an RTX Key into its key lock and turning it 90 degrees clockwise. Doing so is not necessary to operate the RTX Secure.

Sticker Card

Use the stickers on the provided sticker card to label each drive if you plan to use Unique Encrypted Mode (see Section 1.2). This will prevent the drives from getting mixed up when they are removed from the bays.

1.2 Setting the Encryption Mode

Before powering on the RTX Secure, insert your Security Key into the Security Key port and select your desired encryption mode. 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 detected 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. 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 boxes 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 the inability to see some or all established RAID sets.

2. Operation Steps

a. Choose one of the connection types and connect a cable from your computer to the corresponding port on RTX.
b. Connect RTX Secure to a power outlet with the included power cord.
c. Install the hard drives into RTX Secure (See Section 1.1) if you have not already done so.
d. Set the desired encryption mode. (See Section 1.2).
e. If the drives being used in the RTX Secure are encrypted or intended to be encrypted, then insert the Security Key into the Mini-USB Security Key Port on the bottom of the RTX Secure.
f. Flip the power switch on the rear of the unit to turn on the RTX Secure.
g. 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.

3 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. 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. First, be sure to follow the instructions in Section 1.2.
b. After the RTX 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.
c. Press the Enter button again. The LCD screen will ask "Make New RAID?" Press Enter to do so.
d. The LCD will display "Select RAID Type". Press Up or Down to cycle through to your desired RAID type and press Enter.
e. 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.
f. The new configuration will be selected and RTX will reboot. The RAID is now created.

RAID is Not A Backup
Because your RTX Secure features a redundant RAID mode which protects 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 compromise your data. 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.

4. Encryption Information

- 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.