Product Models	RTX Secure 410-SJ, RTX Secure 410-NJ, RTX Secure 410-SV, RTX Secure 610-SV, RTX Secure 610-NJ, RTX Secure 810-SJ, RTX Secure 810-SV
Host Interfaces	• RTX Secure "SJ" models: eSATA • RTX Secure "SV" models: single port-multiplied eSATA • RTX Secure "NJ" models: SFF-8470 multi-lane SAS/SATA 3Gb/s
Drive Types Supported	3.5-inch SATA (Serial-ATA) hard disk drives
TrayFree Technology	Yes
TrayFree Shock Absorbing Bays	Yes (4-bay and 6-bay variants only)
Operating System Requirements	• Windows XP, Vista, Windows 7 • Mac OS X 10.2.6 or later • Linux distributions using Kernel version 2.4 or above
Operating Temperature	50 – 85° Fahrenheit (10 – 30° Celsius)
Operating Humidity	5% to 95%, non-condensing
Power Switch	2 position: On / Off
Power Supply	• Input: 100-240VAC • Output: 220 Watts (4-bay models), 350 Watts (6-bay and 8-bay models)
Cooling Fan	8cm Ball Bearing Fan (two fans for 6-bay and 8-bay models)
Compliance	EMI Standard: FCC Part 15 Class A, CE EMC Standard: EN55022, EN55024 FIPS: FIPS 140-2, FIPS PUB 197
External Case Material	Aluminum alloy
Shipping Weights	• RTX Secure 4-bay Models: 23 pounds without drives, 29 pounds with drives • RTX Secure 6-bay Models: 25 pounds without drives, 34 pounds with drives • RTX Secure 8-bay Models: 28 pounds without drives, 40 pounds with drives
Dimensions	6.97" x 10.63" x 14.57" (177mm x 270mm x 370mm)
Technical Support	We don't expect anything to go wrong with your CRU product. But if it does, Tech Support is standing by and ready to help. Contact us at http://www.cru-dataport.com/support. We also offer phone support at (800) 260-9800.

Product Warranty
CRU-DataPort (CRU) warrants this product to be free of significant defects in material and workmanship for a period of two bnn 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

Tested to comply with FCC standards

FOR OFFICE OR COMMERCIAL USE

RTX™ Secure SJ, NJ, and SV Quick Start Guide

Visit http://www.wiebetech.com/techsupport.php to download a copy of the complete User Manual.
Additional product information can also be found at www.cru-dataport.com and www.wiebetech.com.

Models Covered:
RTX Secure 410-SJ
RTX Secure 410-NJ
RTX Secure 410-SV
RTX Secure 610-NJ
RTX Secure 610-SV
RTX Secure 810-NJ
RTX Secure 810-SV

1. RTX Secure Host Connections

This table shows connection types available in the RTX Secure models covered by this user documentation. Other versions of RTX Secure are available from our distributors and at www.cru-dataport.com.

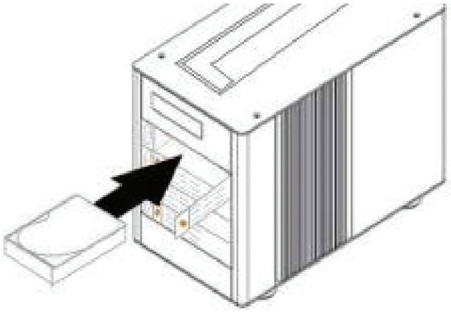
Connection	SJ Model	SV Model	NJ Model
eSATA	4 (4 bays)		
Port-Multiplied eSATA		1 (4 bays) 2 (6 & 8 bays)	
Multi-Lane SAS/SATA 3Gbps (SFF-8470)			1 (4 bays) 2 (6 & 8 bays)

2. Installation Steps

2.1 Hard Drive Installation

a. Pull the ejection handle on the TrayFree bay to open the bay door.
b. Insert a SATA hard drive into each bay. Make sure it is label-side up with the SATA connection on the drive inserted first.
c. Close 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 2.2). This will prevent the drives from getting mixed up when they are removed from the bays.

2.2 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 also not change the mode used at power up.

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.

2.3 Operating Your RTX Secure

a. Choose one of the connection types and connect the appropriate cable from your computer to the corresponding port on the RTX.

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

c. Install the hard drives into the RTX Secure (See Section 2.1) if you have not already done so.

d. Set the desired encryption mode. (See Section 2.2)

e. If the drives being used in the RTX Secure are encrypted or are 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.

When hard drives are first used with the RTX Secure they will show up as blank, unallocated drives and you’ll need to format the drives before you can use them. **Note that formatting a drive will erase all data on the drive, so be sure to back up your data before installing the hard drives into this enclosure and beginning this operation**. See Section 4 for instructions on how to format the drive with Mac or Windows operating systems.

3. 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 encryption key must be installed prior to powering on the RTX Secure for the data to be accessed 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.