RTX™ Secure SJ, NJ, and SV User Manual

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

- 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 attack if the unit is lost or stolen. No PINs or passwords are needed.
- TrayFree™ Trayless Technology for RTX – TrayFree bays make installing drives a breeze. It really is as easy as opening the door, sliding the drive in, and closing the door. No screws, no trays, it just works.

Table of Contents

1. Pre-Installation Steps

1.1 Check the Accessories with Your RTX Secure

Please contact CRU-DataPort if any items are missing or damaged. The box should contain the following items:

Accessories	Quantity
RTX Secure Unit	1
Power cord	1
Security Keys*	3
Lanyards for Security Keys*	3
Security Key ID Tag*	3
Security Key Labels*	6
Packet of Screws and Keys	1
Quick Start Guide and Warranty Information	1

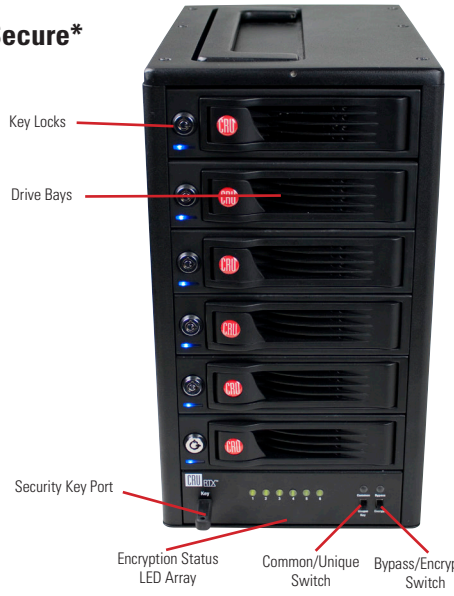
*Only packaged with models that include Security Keys

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*

*RTX Secure 600-SV model shown here. Number of bays available will be different depending on the specific model.



Back of the RTX Secure

**Host connection for "SV" model shown here. For information on host connections of other RTX Secure models, see section 1.3.

Hardened Bay

1.3 RTX Secure Host Connections

This table shows connection types available in the RTX Secure models covered by this user documentation. Other versions of the 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)

1.4 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 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 to prevent damage to the drive interfaces.

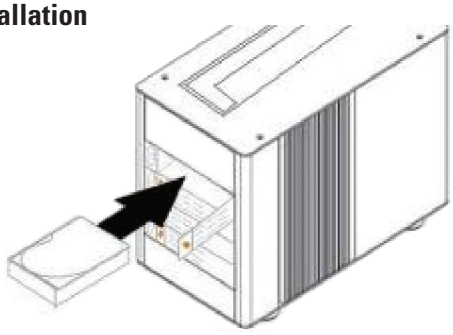
Encryption

- Though the Security Key port is mechanically identical to the standard Mini-USB port, inserting Security Keys into any other Mini-USB port will 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 can 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. 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 <u>all</u> 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. Other Configuration Options

3.1 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 of time 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.

3.2 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. Usage with Mac and Windows Operating Systems

4.1 Usage with Mac OS X

4.1.1 Compatibility

The RTX Secure supports 3.5" SATA hard drives.

4.1.2 Formatting a Drive

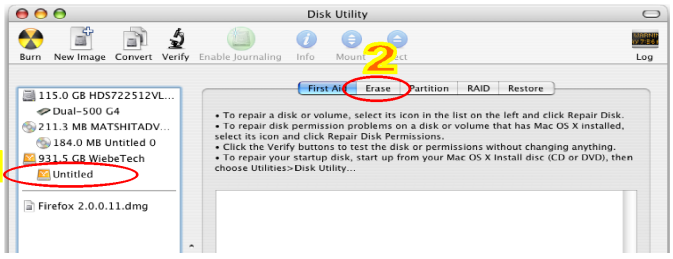
To format, use Mac OS X's Disk Utility (found in the applications folder).

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).

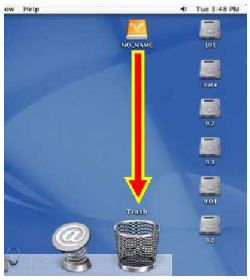
c. Select the format type. Most users prefer Mac OS Extended with Journaling (HFS+), which is required for compatibility with Time Machine (OS 10.5 or newer). If you need to use the RTX Secure with both Mac and Windows computers, select MS-DOS File System instead.

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



4.1.3 Mounting and Unmounting Volumes

If the hard drives installed in the RTX Secure are already formatted with the correct Security Key inserted into the Mini-USB Security Key Port, an icon representing the RTX Secure's volume will appear (mount) on the desktop. You can begin using the volume right away. If the volume 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 bin, or by selecting the volume then pressing Command-E. Disconnecting the unit without first unmounting the volume can result in data loss.

4.1.4 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 wish to boot from your RTX Secure hard drive only some of the time.

4.2 Usage with Windows Operating Systems

4.2.1 Compatibility

The RTX Secure supports 3.5" hard drives.

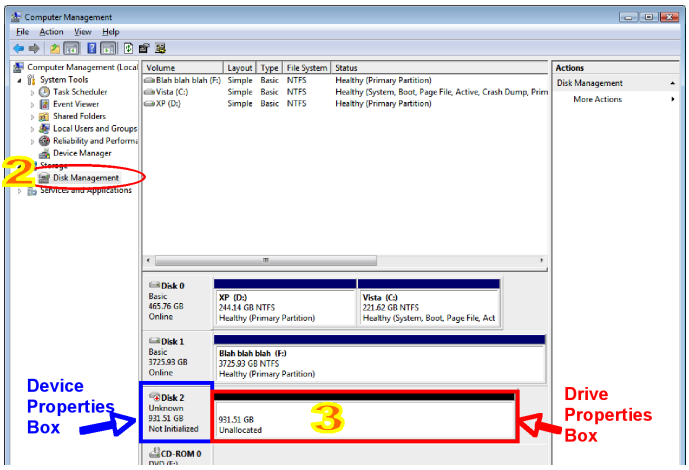
4.2.2 Formatting a Drive

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 to right). 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.

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 by double clicking on the My Computer icon on the desktop.

4.2.3 Mounting and Unmounting Volumes

If the hard drives inside of the RTX Secure are already formatted with the correct Security Key inserted into the Mini-USB Security Key Port, 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 the "My Computer" icon.

Unmount the drives in the RTX Secure by ensuring there are no processes accessing the enclosure (the HDD Access LED will not be blinking), and then power it down.

In order to hot swap drives, you will need to download a third party utility called Hotswap, available from www.mt-naka.com/hotswap/index_enu.htm. Install the utility and you will be able to use the enclosure as a removable device much like a USB/Firewire enclosure.

5. 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.

6. Frequently Asked Questions (FAQ)

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

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

Q: 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?

A: Check the encryption mode to make sure that it is set to Unique Encrypted Mode. 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. 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.

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

A: 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 2.3 for the proper procedure on starting up the RTX Secure with a Security Key.

If none of these solutions work, try removing each drive from the RTX Secure and reseating them in their TrayFree Bays.

Q: There is a problem with one bay's encryption status, but all other drives' statuses are fine.

A: Individual encryption errors indicate an encryption engine failure. If you experience this issue, please contact Technical Support.

Contacting Technical Support

Still need help? Please contact our Technical Support team through CRU-DataPort.com. Or call us toll free at (800) 260-9800.

7. Technical Specifications

Product Models	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
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
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.

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