RTX™ Secure IR User Manual

Models Covered:
RTX Secure 610-IR
RTX Secure 810-IR

- 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. Default GUI Login Information

The following login and password information can be used to easily log into the GUI (See Section 8 for instructions on how to log in to and use the GUI).

Administrator Account
This account has read and write privileges.
Username: admin
Password: 1234

User Account
This account has read-only privileges.
Username: user
Password: 1234

2. Pre-Installation Steps

2.1 Check the Accessories with Your RTX Secure

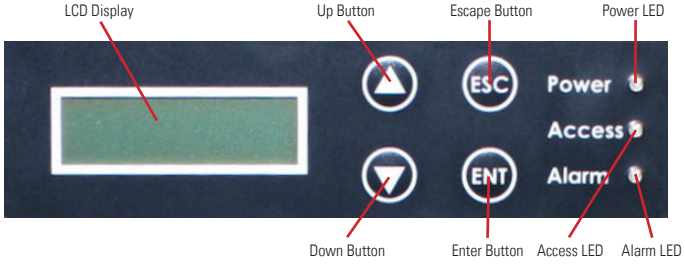
Please contact CRU-DataPort if any items are missing or damaged. The box should contain the following items:

Accessories	Quantity
RTX Secure Unit	1
Power cord	1
Ethernet Cable	2
Security Keys	3
Lanyards for Security Keys	3
Security Key ID Tag	3
Security Key Labels	6
Packet of Keys	1

*Only packaged with SKUs that include hard drives

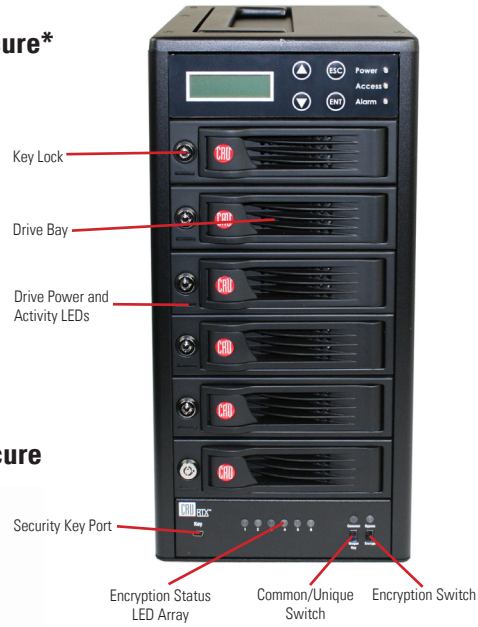
2.2 Identifying Parts

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

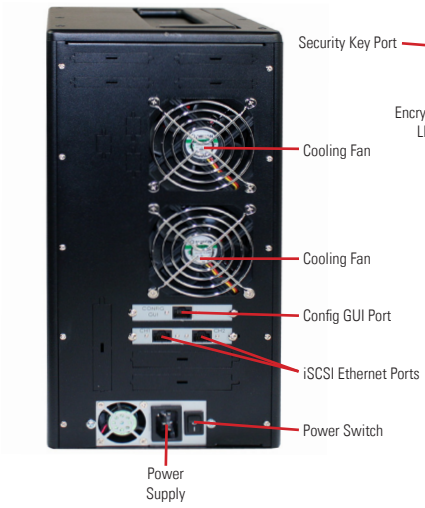


Front of the RTX Secure*

*RTX Secure 610-IR model shown here. Number of bays available will be different depending on the specific model.



Back of the RTX Secure



2.3 Warnings and Notices

Please read the following before beginning installation.

General Care

- The main circuit boards of the HDD carriers are 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 the HDD carriers 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 carrier or receiving frame.
- 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 Secure 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 Secure 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.

- The RTX Secure 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 afterwards.

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 on the carrier 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.

2.4 Terminology

RAID	A redundant array of independent hard disks. There are different RAID levels with different degrees of data protection, data availability, and performance.
JBOD	All disks act as independent drives. JBOD needs at least one hard drive.
Physical Disk (PD)	Belongs to the member disk of one specific RAID group.
RAID Group (RG)	A collection of removable media. One RG consists of a set of VDs and owns one RAID level attribute.
Virtual Disk (VD)	Each RG can be divided into several VDs. The VDs from one RG have the same RAID level, but may have different volume capacity.
Logical Unit Number (LUN)	A unique identifier for a SCSI device which enables computers to differentiate among separate SCSI devices.
GUI	Graphical User Interface.
RAID cell	The number of subgroups of PDs in an RG.
Dedicated Spare (DS)	A spare disk dedicated to one specific RG and is used when another disk in the RG fails.
Global Spare (GS)	A spare disk that is shared among all RGs and is used when another disk in an RG fails.
World Wide Name (WWN)	A unique identifier that identifies a particular PD.
Challenge Handshake Authentication Protocol (CHAP)	An optional security mechanism to control access to the RTX Secure through its iSCSI data ports.
Internet Storage Name Service (iSNS)	This protocol allows automated discovery, management, and configuration of iSCSI devices on a TCP/IP network.

3. 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.

3.1 Summary of RAID Levels

The RTX Secure supports RAID Levels 0, 1, 3, 5, 6, 0+1, 10, 30, 50, 60, & JBOD. RAID Level 5 is most commonly used by those seeking an optimal balance of speed and data safety.

RAID Level	Description	Min. Drives	Data Redundancy	Data Transfer Rate
0	Also known as striping. Data distributed across multiple drives in the array. There is no data protection.	2	No data protection	Very high
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	Reads higher than a single disk; Writes similar to a single disk

RAID Level	Description	Min. Drives	Data Redundancy	Data Transfer Rate
3	Also known as Bit-Interleaved Parity. Data and parity information is subdivided and distributed across all disks. Parity must be equal to the smallest disk capacity in the array. Parity information normally stored on a dedicated parity disk.	3	1 drive	Reads are similar to RAID 0
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	1 drive	Reads are similar to RAID 0
6	Two parity bits are used to create double redundancy. Can withstand the failure of two drives. The total capacity of all but two of the drives is available for data storage.	4	2 drives	Slightly less than RAID 5
0+1	Also known as a mirror of striped drives. Data and parity information is subdivided and distributed across all disks. Parity must be equal to the smallest disk capacity in the array. Parity information normally stored on a dedicated parity disk.	4	1 drives*	Transfer rates are similar to RAID 0
10	Also known as a stripe of mirrors. Data is striped across two separate disks and mirrored to another disk pair.	4	1 drives*	Transfer rates are similar to RAID 0
30	Also known as a Striping Dedicated Parity Array. RAID 30 breaks up data into smaller blocks, and then stripes the blocks of data to each RAID 3 RAID set.	6	2 drives**	Transfer rates are similar to RAID 0
50	RAID 50 combines the straight block-level striping of RAID 0 with the distributed parity of RAID 5	6	2 drives**	Transfer rates are similar to RAID 0
60	RAID 60 combines the straight block-level striping of RAID 0 with the distributed double parity of RAID 6	8	4 drives***	Transfer rates are similar to RAID 0
JBOD	Just A Bunch of Disks. This is not an actual RAID level because each disk is treated as its own entity.	1	No data protection	Very high

* One drive from each the RAID 0 and RAID 1 sets can fail without loss of data. If both drives in either the RAID 0 or RAID 1 set fail, then the entire RAID will fail.

** One drive from each of the striped RAID sets could fail without loss of data. If two drives in the same striped RAID set fail, then the entire RAID will fail.

*** Two disks from each of the RAID 6 sets could fail without loss of data. If three disks in the same striped RAID 6 set fail, then the entire RAID will fail.

4. Introduction to iSCSI

4.1 What is iSCSI?

iSCSI is a technology that allows a data storage device to be accessed over a TCP/IP network using SCSI protocols. When your computer's OS receives a request for data access, it generates a SCSI command and then sends an IP packet across a network or direct Ethernet connection. A software utility known as an iSCSI initiator is used to generate the SCSI commands. Such a utility must be installed on the computer before it can access an iSCSI storage device (See Section 9 for installation instructions).

4.2 What is the Benefit of iSCSI?

An iSCSI storage device can be placed anywhere throughout a network, so the device can reside at a great distance from the computer which accesses it. It is also a very fast connection when used on a gigabit network, achieving speeds of 100 megabytes (MB)/sec or more. The connection it uses (RJ45—standard Ethernet port) is commonly found on desktop and laptop computers, so there is no need to purchase potentially expensive host bus adapters to provide a connection.

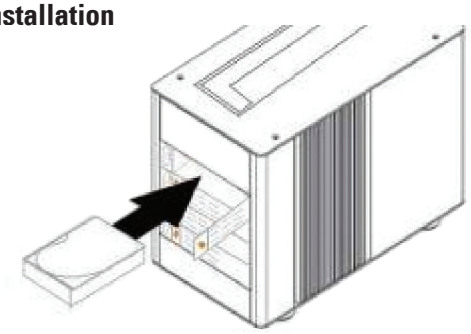
4.3 What is iSCSI Not?

iSCSI storage devices are not Network Attached Storage (NAS) devices. They have no built-in server capabilities and therefore cannot be accessed by more than one computer at a time. Multiple computers can only access the data if the iSCSI device is first attached to a single computer which is then set up as a server.

5 Installation Steps

5.1 Hard Drive Installation

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



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

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. Locking the bay doors 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 5.2). This will prevent the drives from getting mixed up when they are removed from the bays.

5.2 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.

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. But don't worry, your data will remain intact and will be 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 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 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 Bypass LED will illuminate and the drive bay Encryption Status 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.

5.3 Operating RTX Secure

a. Connect the RTX Secure to a computer or network using the included Ethernet cables. Plug one cable into the "CH-1" port. You can optionally plug a second cable into the "CH-2" port if having a redundant connection or increased performance is needed.

b. If you haven't yet set up network access, connect another Ethernet cable into the "Config GUI" port.

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

d. Install the hard drives into the RTX Secure (See Section 5.1).

e. Set the desired encryption mode (See Section 5.2).

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. Flip the power switch on the rear of the unit to turn on the RTX Secure.

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 the RTX Secure for network access by following the appropriate setup instructions in Section 7.

j. Configure your drives with at least one RAID set. Follow the appropriate setup instructions in Section 8. CRU DataPort recommends manually creating the RAID set (Section 8.3) or using the Volume Creation Wizard (Section 8.7.1).

k. Configure the RTX Secure for access using the instructions in Section 9 for setting up an iSCSI initiator.

Once a RAID set has been created and the user connects to the RTX Secure through an iSCSI initiator, it will show up as a blank, unallocated volume and you'll need to format it in the RTX Secure before you can use it. **Note that formatting a volume or creating a RAID set will erase all data on the volume, 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.

6 Other Configuration Options

6.1 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 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.

6.2 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.

6.3 Recovering from a Failed RAID

If one hard drive of a RAID set with data redundancy has failed or has been unplugged or removed, then the status of the RAID Group will report that the RAID is degraded and the RTX Secure will automatically search for a spare disk to rebuild the RAID. The RTX Secure will first search for a dedicated spare disk, then a global spare disk, and finally, if neither is found, it will wait for the user to remove the failed hard drive and insert a working replacement.

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.

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. But don't worry, your data will remain intact and will be accessible once the correct encryption mode is set.

7 Network Configuration

7.1 Connecting the RTX Secure to Your Network or Computer

a. Plug an Ethernet cable into the "Config GUI" port on the rear of the RTX Secure.

b. Connect the other end of the Ethernet cable to your network. This usually means plugging it into a router or hub. In an office environment, you may have a network jack built into your office wall. If a network connection is not available, you can connect the Ethernet cable directly to an RJ45 (Ethernet) port on your computer.

c. Connect the power cable to the rear of the RTX Secure and to a grounded electrical outlet.

d. Turn on the RTX Secure's power using the switch on the rear panel.

7.2 Using the LCD to Configure the Config GUI Port

RTX has both an LCD interface and a GUI. The LCD interface has only basic functionality and is mainly used to configure the IP address of the Config GUI port. Once the Config GUI has been configured, the GUI can be used to fully configure the RTX Secure.

7.2.1 Navigating the LCD menu

Use the four function keys, ▲(Up), ▼ (Down), ESC (Escape) and ENT (Enter) to manipulate the LCD interface. After pressing ENT (Enter) key, you can use the ▲ (Up) and ▼ (Down) keys to select a function. If there is an alarm or error message, the LCD will display the related information.

7.2.2 LCD Functions

System Info	Displays the details of RAM and firmware.
Alarm Mute	Turns off the alarm sound when an error occurs.
Reset/Shutdown	Resets or shuts down the controller.
Quick Install	To use "Quick Install" to set up a volume by three steps. CRU-DataPort does not recommend using the Quick Install option to set up your RTX Secure. For quick set-up of a RAID, refer to Section 8.6.1.
Volume Wizard	Smart steps to create a volume. Please refer to Section 8.6.1 for detailed operation steps in the web GUI.
View IP Setting	Display the current IP address, subnet mask, and gateway.
Change IP Config	Sets the IP address, subnet mask, and gateway. You can choose to use DHCP server (for IP address allocation) or manually specify the IP address.
Reset to Default	Restores factory defaults: Default Administrator Name: **admin** Default Administrator Password: **1234** Default User Name: **user** Default User Password: **1234** Default IP address: **192.168.0.1** Default subnet mask: **255.255.255.0** Default gateway: **192.168.0.254**

7.2.3 RTX Secure LCD Menu Diagram

Use the following chart for reference when following the instructions in Section 7.2.4 for setting up the RTX Secure according to your network type.

1st Menu Screen	2nd Menu Screen	3rd Menu Screen	4th Menu Screen	5th Menu Screen	6th Menu Screen
CRU-DataPort RTX	[System Info.]	[Firmware Version x.x.x]			
		[RAM Size xxx MB]			
	[Alarm Mute]	[ENT:OK ESC: Back]			
	[Reset/ Shutdown]	[Reboot]	[ENT:OK ESC: Back]		
		[Shut-down]	[ENT:OK ESC: Back]		

1st Menu Screen	2nd Menu Screen	3rd Menu Screen	4th Menu Screen	5th Menu Screen	6th Menu Screen
CRU-DataPort RTX	[Quick Install]	RAID 0 RAID 1 RAID 3 RAID 5 RAID 6 RAID 0+1 xxx GB	[Apply The Config]	[ENT:OK ESC: Back]	
	[Volume Wizard]	[Local] RAID 0 RAID 1 RAID 3 RAID 5 RAID 6 RAID 0+1	[Use default algorithm]	[Volume Size] xxx GB	[Apply The Config] [ENT:OK ESC: Back]
	[View IP Setting]	[IP Config] [Static IP]			
		[IP Address] [DHCP IP]			
		[IP Subnet Mask] [255.255.255.0]			
		[IP Gateway] [192.168.010.254]			
	[Change IP Config]	[DHCP]	[ENT:OK ESC: Back]		
		[Static IP]	[IP Address]	Adjust IP address	
			[IP Subnet Mask]	Adjust Submask IP	
			[IP Gateway]	Adjust Gateway IP	
			[Apply IP Setting]	[ENT:OK ESC: Back]	
	[Reset to Default]	[ENT:OK ESC: Back]			

7.2.4 Instructions for Differing Network Connection Types

DHCP-Enabled Network

On DHCP networks, a new IP address is dynamically assigned to RTX's Config GUI port as soon as the network detects it. You can determine this address by checking the LCD interface on the front of the RTX Secure. It will appear in this format: xxx.xxx.xxx.xxx. Simply type this IP address into a web browser on your computer. This will access the RTX Secure's GUI, which you will use to configure the unit.

NOTE: Not sure what type of network you have? If the IP address displayed on the LCD starts with 169.254, this indicates that the network is probably not DHCP-enabled. Use the instructions for a static network.

Static Network

a. Check your computer's IP address, subnet mask, and gateway. Mac users can find this information in System Preferences → Network.

   To do this in Windows, open Network and Sharing Center in the Control Panel (Also called "View Network Status and Tasks" under the "Network and Internet" category). On the left pane, select "Change adapter settings". Right-click on your network (likely called Local Area Connection) and select Properties. On the new window that opens, select "Internet Protocol Version 4 (TCP/IPv4)" and click the Properties button. Your computer's IP address, subnet mask, and gateway will be displayed.

b. On the RTX Secure's LCD interface, press ENT and then scroll up or down to "Change IP Setting". Press ENT.

c. Scroll up or down to find "Static". Press ENT.

d. Change the IP address to closely match what your computer is using. Or, if you are on a business network, have your IT administrator assign you an IP address.

NOTE: The IP address you select must NOT be in use by another device.

   For example, if your computer's IP address is 192.168.0.9, you might change the RTX Secure's IP to 192.168.0.7. **On smaller networks, each of the first three octets must be the identical to your computer's IP address!** When changing the IP address you'll notice that a box flashes over the digit to be changed. While the digit is selected, press ▲ (Up) or ▼ (Down) to change it. Press ENT to move to the next digit.

e. After the IP address is set, enter the subnet mask address **exactly** as it is shown on your computer's TCP/IP settings.

f. Next, enter the gateway address **exactly** as it is shown on your computer's TCP/IP settings.

g. Confirm the settings change. To confirm, press ▲ (Up) for "Yes" and then press ENT again.

h. Type the RTX Secure's new IP address into a web browser on your computer. This will access the RTX Secure's GUI, which you will use to configure the unit.

Direct Connection to a Computer

The instructions are similar to those for a static network (see above), except that your computer will not have an IP address assigned if it's not a part of a network. Since the RTX Secure and your computer must have similar IP addresses, you will assign an IP address to your computer based upon the default IP address of the RTX Secure.

a. Check the RTX Secure's LCD to find out the IP address of the Config GUI configuration port. It will appear in this format: xxx. xxx.xxx.xxx.

b. Next, change your computer's IP address so that all but the last three digits match the RTX Secure's address. For example, if the RTX Secure's IP address is 169.254.12.62, you might assign your computer the number 169.254.12.63 (assuming no other computer on the network is already using that number). The process of changing your computer's IP address varies depending on its operating system.

   Mac users can go to System Preferences → Network.

   For modern Windows operating systems, open Network and Sharing Center in the Control Panel (Also called "View Network Status and Tasks" under the "Network and Internet" category). On the left pane, select "Change adapter settings". Right-click on your network (likely called Local Area Connection) and select Properties. On the new window that opens, select "Internet Protocol Version 4 (TCP/IPv4)" and click the Properties button. By default, your computer is probably set to receive a new IP address automatically. Change the setting to manual configuration and then type in the IP address.

c. Using the same process as the previous step, change the computer's Subnet Mask setting to match the RTX Secure's Subnet Mask setting.

d. Finally, use the RTX Secure's LCD interface to change the RTX Secure's Gateway setting. It should match the IP address you assigned to your computer. When changing the gateway address you'll notice that a box flashes over the digit to be changed. While the digit is selected, press ▲ (Up) or ▼ (Down) to change it. Press ENT to move to the next digit. After the gateway address is set, press ENT all the way to the end and confirm the settings change. To confirm, press ▲ (Up) for "yes" and then press ENT again.

e. Launch a web browser and type the RTX Secure's IP address into the URL bar, as if it were a website. This will access the RTX Secure's GUI, which you will use to configure the unit (See Section 8).

The tables below show example settings. The first table shows the type of settings that will appear by default. The next table shows how the settings might look after you've made changes.

Before Making Changes		
	RTX Secure	**Computer**
IP Address	169.254.12.62	(Blank)
Mask	255.255.000.000	(Blank)
Gateway	000.000.000.000	(Blank)

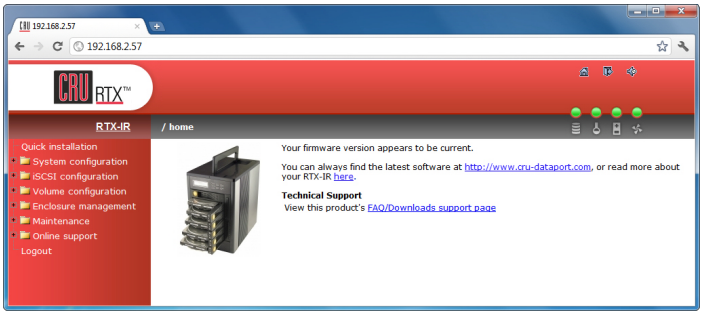
After Making Changes		
	RTX Secure	**Computer**
IP Address	169.254.12.62	169.254.12.63
Mask	255.255.000.000	255.255.000.000
Gateway	169.254.12.63	(Blank)

Connecting From Home to Office

The RTX Secure can also be used over the Internet. If you are connecting to an RTX Secure at your office from home, you will need to contact your IT administrator to set up a VPN client in order to log in to the office network. Once you have logged in to the office network, you can access the RTX Secure just as if you were actually at your office (see instructions for DHCP-enabled Network, Static Network, or Direct Connection to a Computer, depending on how your office network is configured).

8 Using the GUI

You will use the web browser-based GUI to set up a RAID and create logical volumes on RTX. After setting up access to the GUI and accessing it through a web browser (see Section 7.2 for instructions), the GUI's main page should load, displaying a picture of RTX with several options to the left. When you click on any option, you will be prompted for a username and password. The default administrator username is "**admin**" and the default password is "**1234**".



8.1 GUI Indicators

The top right hand corner of the GUI window displays several indicators.

RAID Light
Green indicates that the RAID is working properly. Red indicates a RAID error. If no RAID is set up, the light will remain green.

Temperature Light
Green indicates normal. Red indicates abnormal system temperature and probable overheating.

Voltage Light
Green indicates normal. Red indicates abnormal voltage status like a power surge or a bad power supply.

Fan Light
Green indicates that the fan is working properly. Red indicates a malfunctioning fan that needs to be replaced.

8.2 GUI Menu Structure

- Quick installation
- System configuration
  - System settings
  - IP address
  - Login settings
  - Mail settings
  - Notification settings
- iSCSI configuration
  - Entity property
  - NIC
  - Node
  - Session
  - CHAP account
- Volume configuration
  - Volume creation wizard
  - Physical disk
  - RAID group
  - Virtual disk
  - Logical unit
- Enclosure management
  - SES configuration
  - Hardware monitor
  - S.M.A.R.T.
- Maintenance
  - System information
  - Upgrade
  - Reset to factory default
  - Import and export
  - Event log
  - Reboot and shutdown
- Online support
  - Product Information and Specs
  - FAQ and Downloads
- Logout

8.3 Manually Creating a RAID Set

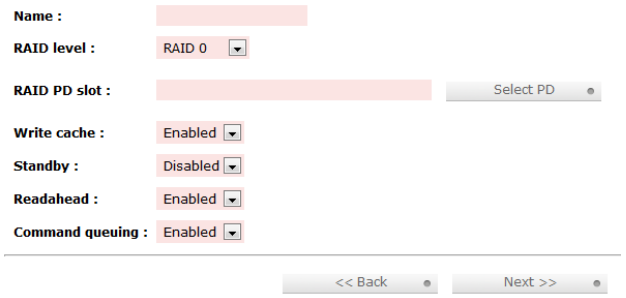
Use these sets of instructions to create a RAID set. To quickly create a RAID 0, 1, 3, 5, 6, or 0+1 set using the Volume Creation Wizard, see Section 8.6.1.

8.3.1 Creating a RAID Group

To manually create a RAID set, you will first need to create a new RAID Group.

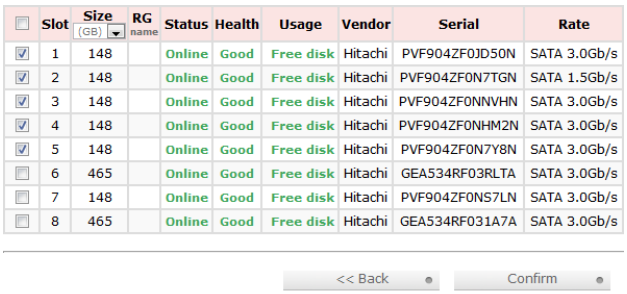
a. Click the "Create" button at the bottom of the page to open the RAID Group creation screen.

b. Enter a name for the new RAID Group in the first field, and then select your desired RAID type or JBOD from the dropdown box. CRU-DataPort recommends RAID 5 for maximum performance, capacity, and security. For more information on RAID, see Section 3. Click "Select PD" to select the drives that will be added to the RAID Group.



NOTE: Drives must be marked as Free Disks before they can be added to a RAID Group. To set drives to Free Disks, see Section 8.7.2, subsection "Modifying Physical Disks".

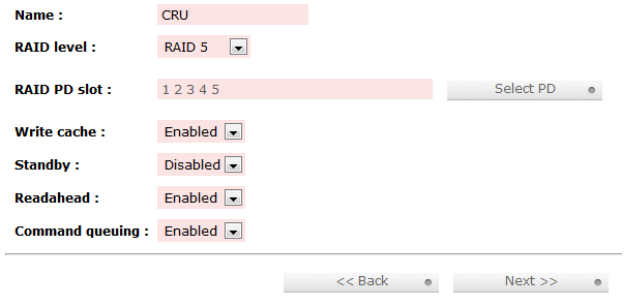
c. All available Free Disks will be displayed. Check the drives that you wish to add to the RAID Group, then click "Confirm".



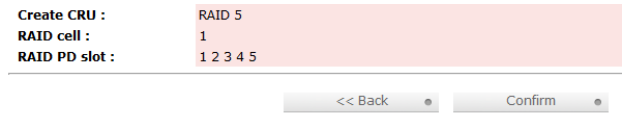
	Slot	Size (GB)	RG name	Status	Health	Usage	Vendor	Serial	Rate
☑	1	148		Online	Good	Free disk	Hitachi	PVF904ZF0JD50N	SATA 3.0Gb/s
☑	2	148		Online	Good	Free disk	Hitachi	PVF904ZF0N7TGN	SATA 1.5Gb/s
☑	3	148		Online	Good	Free disk	Hitachi	PVF904ZF0NNVHN	SATA 3.0Gb/s
☑	4	148		Online	Good	Free disk	Hitachi	PVF904ZF0NHM2N	SATA 3.0Gb/s
☑	5	148		Online	Good	Free disk	Hitachi	PVF904ZF0N7Y8N	SATA 3.0Gb/s
☐	6	465		Online	Good	Free disk	Hitachi	GEA534RF03RLTA	SATA 3.0Gb/s
☐	7	148		Online	Good	Free disk	Hitachi	PVF904ZF0NS7LN	SATA 3.0Gb/s
☐	8	465		Online	Good	Free disk	Hitachi	GEA534RF031A7A	SATA 3.0Gb/s

<< Back Confirm

d. The selected Physical Disks will now be displayed in the RAID Group creation screen. Enable or Disable Write Cache, Standby, Readahead, and Command Queuing based on your needs. Most RAID Groups will be fine with the default settings. Then click "Next" to proceed to the confirmation screen.

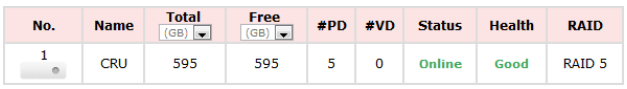


e. On the confirmation screen, verify that the RAID level is correct and all of the disks you selected are displayed under "RAID PD slot", then click "Confirm" to create the RAID Group.



f. The RAID Group will now display on the main RAID Group screen. To finish manually creating a RAID set, a Virtual Disk still must be created and a Logical Unit must be attached. Go to the next section, "Creating a Virtual Disk".

If you opted to create JBOD drives, skip to Section 8.3.3, "Manually Attaching a Logical Unit" as Virtual Disks have already been created for each JBOD drive.

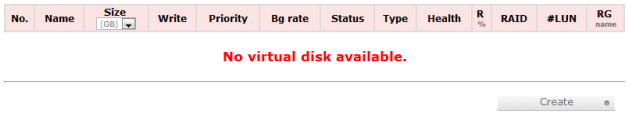


No.	Name	Total (GB)	Free (GB)	#PD	#VD	Status	Health	RAID
1	CRU	595	595	5	0	Online	Good	RAID 5

8.3.2 Creating A Virtual Disk

After a RAID Group has been created, you can create associated Virtual Disks. You must create at least one Virtual Disk to access the drives of the RTX Secure with a computer.

a. Click the "Create" button at the bottom of the page to open the Virtual Disk creation screen.

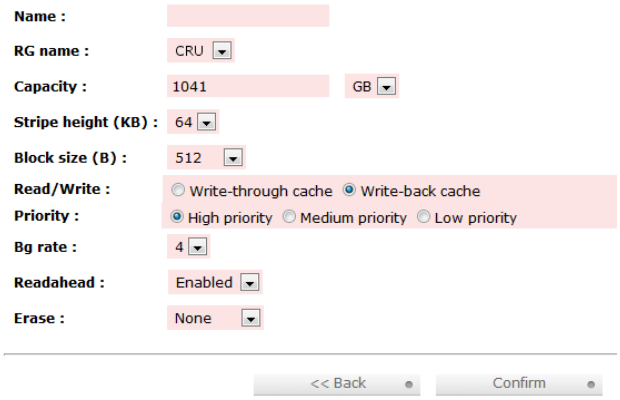


No.	Name	Size (GB)	Write	Priority	Bg rate	Status	Type	Health	R %	RAID	#LUN	RG name

No virtual disk available.

Create

b. You will see the screen below. Fill in the information and then click "Confirm". Each field is explained below the picture.



Name
Enter a name for the Virtual Disk.

RG Name
Choose the RAID Group to which the Virtual Disk will be added

Capacity
Enter the capacity of the Virtual Disk. The default uses the maximum capacity of the associated RAID Group. If you wish to create multiple Virtual Disks on the selected RAID Group, you will need to reduce the capacity below the maximum so that there is space left on the RAID Group for additional Virtual Disks.

Stripe Height (KB)
Determines how the RTX Secure organizes the RAID. Normally the default option is preferred.

Block Size
Determines the minimum file size for files that will be stored on the Virtual Disk. Higher block sizes can result in more wasted space if many small files are saved to the drive, but are necessary to take advantage of high capacity RAIDs. **If you are creating a Virtual Disk over 2TB in size for use with MacOS 10.4.x or older, or for use with Windows XP, you must increase the block size to 4096KB to take advantage of the full capacity of the Virtual Disk. For more information, see Section 14.**

Read/Write
Allows selection of cache type. Normally the default option is preferred.

Priority
Determines the priority that the RTX Secure will give to RAID activities (rebuild and initialization) versus priority given to file transfers. "High priority" will result in slower file transfers during initialization, but provide for faster initialization.

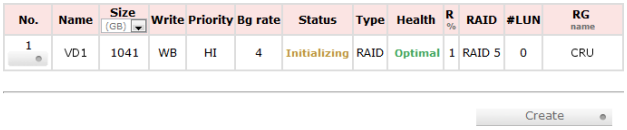
BG Rate
Background Task Priority. The higher the number, the more priority will be given to background input/output.

Readahead
Choose whether file prefetching should be enabled.

Erase
Wipes out the original data in the Virtual Disk to prevent the OS from recognizing it. The options are "None", "First 1GB", and "Full Disk."

c. The Virtual Disk will now display on the main Virtual Disk screen. If you have enabled an Erase option, **do not** shut down or reboot the RTX Secure while the Virtual Disk is initializing or the erase process will stop.

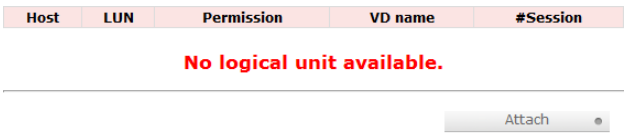
To finish manually creating a RAID set, at least one Logical Unit must be attached. Go to the next section, "Manually Attaching a Logical Unit".



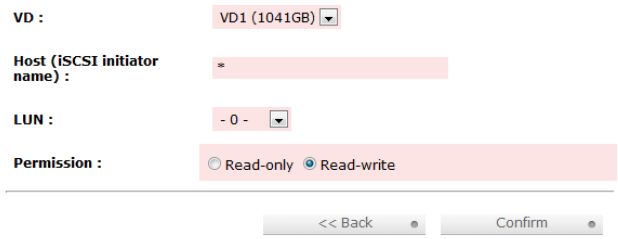
8.3.3 Attaching a Logical Unit

You will need to attach at least one Logical Unit to a Virtual Disk to access its RAID Group, although multiple Logical Units can be attached to the same Virtual Disk.

a. Click the "Attach" button to attach a Logical Unit to a Virtual Disk.



b. You will see the screen below. Fill in the information. Select the Virtual Disk to which you wish to attach a Logical Unit. The Host name can remain as an asterisk if you want any host to access the Virtual Disk. Otherwise, change the field to limit access to specific hosts. Then select the LUN that will be used. The default setting on this is acceptable. Finally, select the permissions that hosts accessing this Logical Unit will have. Then click "Confirm".



c. The main Logical Unit Screen will now display the Logical Unit you have just created. If you've been following the instructions for manually creating a RAID set, you have now completed setup. Once the RAID set has finished initializing, you will be able to access it through iSCSI initiator software (see Section 9 for installation and connection instructions).

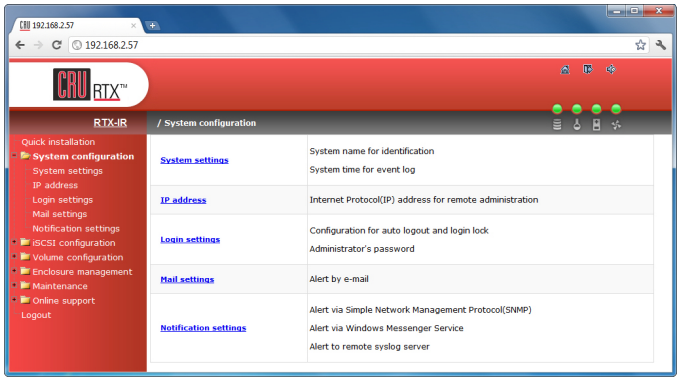
8.4 Quick Installation

CRU-DataPort does not recommend using the Quick Installation option to set up your RTX Secure. For quickly setting up a RAID, refer to Section 8.7.1.

Quick Install uses all physical disks in the RTX Secure and the maximum amount of space they contain to create a RAID Group using one Virtual Disk. There will be no space set aside for spares. If some disks are used in other RAID Groups, Quick Install cannot be run.

8.5 System Configuration

The System Configuration menu gives access to a number of options used to configure the RTX Secure system properties. Click on "System Configuration" to access the following menu options: System Settings, IP Address, Login Settings, Mail Settings, and Notification Settings.



8.5.1 System Settings

System Settings allows you to view and change the system name, change the date and time, and turn the System Indication LED on or off.

System Name

The default system name is "RTX-IR" . To change the system name, simply click in the box displaying the system name and highlight or delete the part of the name you wish to change, then type the new name and click the "Confirm" button at the bottom of the page.

Date and Time

The Date and Time option allows you to change the date and time settings of the RTX Secure. To change the date or time, check the "Change date and time" check box and then click in the field that you wish to change. Highlight or delete the information, then type in the new information and click the "Confirm" button at the bottom of the page.

To change the time zone, click the drop down box and then scroll up or down until you reach the correct time zone. Then choose that time zone and click the "Confirm" button at the bottom of the page.

After confirming, a dialog box will appear verifying that changes have been made.

Alternatively, an NTP (Network Time Provider) can be used to sync the RTX Secure's time information with that of a standardized server. To use an NTP, click the NTP check box, then input the server information in the server field.

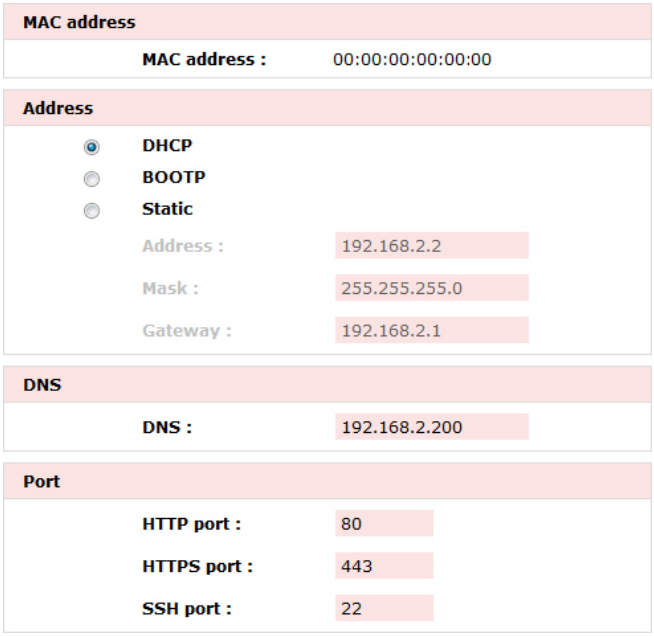
Click the "Confirm" button at the bottom of the page to update the time settings. A dialog box will appear to inform you that the changes have been made. The updated settings will reflect the time settings of the NTP.

System Indication

To turn the System Indication LED on or off, select the "Confirm" button in the System Indication box. After confirming, a dialog box will appear verifying that changes have been made. To reverse this action, press the "Confirm" button again.

8.5.2 IP Address

The IP Address option lists the RTX Secure's MAC address and allows you to view and modify the IP information of the Config GUI port on the RTX Secure. This option does not allow the administrator to configure the IP address of the individual data ports. This must be done using the LCD interface on the front of the RTX Secure (see Section 7.2).



An RTX Secure configured for DHCP.

8.5.3 Login Settings

The Login Settings page allows you to configure the Auto Logout and Login Lock features, as well as change the administrator account and user passwords.

Login Configuration

- Auto Logout will automatically log the user out of the system after a set period of 5 minutes, 30 minutes, or 1 hour of inactivity.

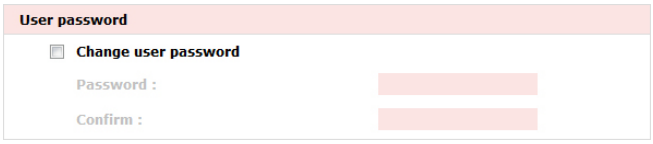
- Login Lock prevents multiple users from using the GUI simultaneously. Both features are disabled by default. To enable a feature, click on the dropdown menu associated, select the new option, and click the "Confirm" button.

Admin Password

The Admin Password option allows you to change the password for the administrator account, which is used to access and modify the settings in the GUI. **The default username is 'admin' and the password is '1234'.** To change the password, click on the "Change admin password" check box. Then enter the old password in the first field. Type the new password in the second and third field and finally click the "Confirm" button at the bottom of the page.

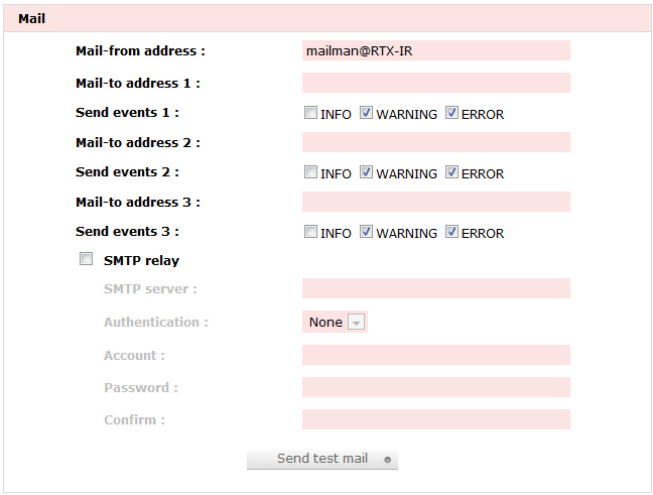
User Password

The User password option allows you to change the password for the user account, which is used to view, but not modify the settings in the GUI. **The default username is 'user' and the password is '1234'.** To change the password, click on the "Change user password" check box. Then enter the old password in the first field. Type the new password in the second and third field and finally click the "Confirm" button at the bottom of the page.



8.5.4 Mail Settings

The RTX Secure can be configured to send email to up to 3 addresses when events, warnings, and errors occur. Contact your IT administrator to set up an email address for the RTX Secure and to input the proper SMTP settings.



8.5.5 Notification Settings

Notification Settings allows you to configure the Simple Network Management Protocol (SNMP), Windows Messenger events, the System Log server, Event Log filters, and enable or disable the internal buzzer.

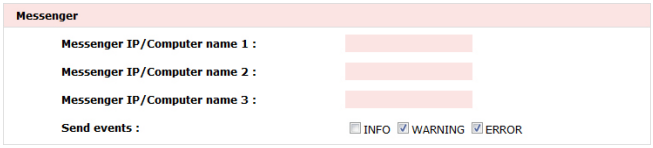
SNMP (Simple Network Management Protocol)

SNMP can be configured to send trap messages to up to three different addresses on the network. To add an address, simply enter the IP address of the receiving server or computer, then click the "Confirm" button at the bottom of the page. Note: The receiving server must be configured to receive SNMP messages.

For more information on SNMP, you may wish to consult the third party website: www.systemdisc.com/snmp

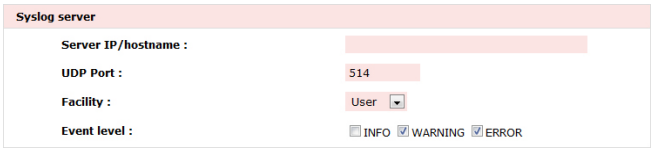
Messenger

The RTX Secure can be configured to send instant messages to up to 3 addresses when events, warnings, or errors occur.



Syslog Server (System Log Server)

The Syslog Server option allows configuration for error, warning, and information reporting via a port on the server. Enter the server IP under Server IP/hostname and the port used in the UDP Port line (the default port is 514). The Facility can be changed between "User", "Kern", and "Local1" through "Local7" using the dropdown box. Select the check boxes for "Info", "Error", and "Warning" that pertain to the information that you want to have reported.



Event Log Filter

The Event Log Filter allows you to display event messages. To configure what types of messages are displayed, select the check boxes for "Info", "Error", and "Warning" that pertain to the information that you want to have reported. The options for Pop Up Events will display those events as a pop-up notification in your

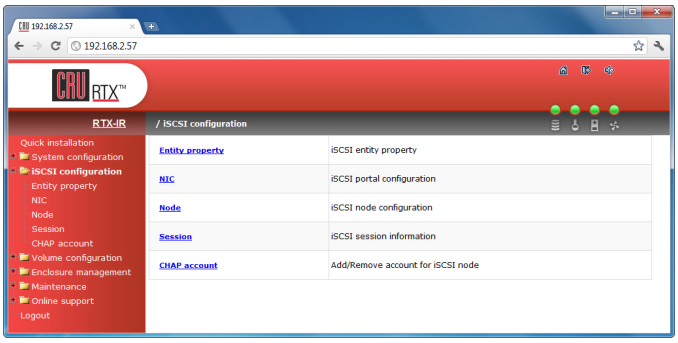
browser. The options for Show on LCM will display the selected events in the RTX Secure IR's LCD screen.

Buzzer

To disable the buzzer, place a checkmark next to "Always disable buzzer," and click the "Confirm" button at the bottom of the page.

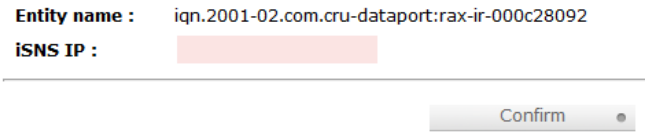
8.6 iSCSI Configuration

The iSCSI configuration menu options are generally used to modify the connection properties of the RTX Secure. Click on "iSCSI configuration" to access the following menu options: Entity Property, NIC, Node, Session, and CHAP Account.



8.6.1 Entity Property

The Entity Property option allows you to add an Internet Storage Name Service (iSNS) server IP address to the iSNS server group, to which the iSCSI initiator can send queries. Simply enter the iSNS IP address in the iSNS IP field and click "Confirm". Note: Setting an iSNS is not necessary to use the RTX Secure.



8.6.2 NIC

Click on "NIC" to view the IP settings of the two gigabit Ethernet data ports. You will see the following information:

Name	LAG	LAG No	DHCP	IP address	Netmask	Gateway	Jumbo frame	MAC address	Link
LAN1	No	N/A	Yes	192.168.2.2	255.255.255.0	192.168.2.1	Disabled	00:00:00:00:00:00	Up
LAN2	No	N/A	No	192.168.2.3	255.255.255.0	192.168.2.254	Disabled	00:00:00:00:01:00	Down

NIC Column Descriptions	
Name	LAN1 corresponds to the port labeled CH-1 (Channel 1) on the back of the RTX Secure, while LAN2 corresponds to the port labeled CH-2 (Channel 2).
LAG	Displays whether Link Aggregation is enabled or disabled.
LAG NO	Displays the LAG number.
DHCP	Shows whether the channel has DHCP enabled.
IP Address	Displays the IP address currently in use by the channel.
Netmask	Displays the subnet mask being used by the channel.
Gateway	Displays the IP gateway. In a DHCP network, it will display the IP of the router to which the RTX Secure is connected.
Jumbo Frame	Displays whether jumbo frames are enabled or disabled. The maximum jumbo frame size is 3900 bytes.
MAC Address	Displays the MAC address of each channel.
Link	Displays the status of each channel. If an Ethernet cable is connecting the RTX Secure to a network or computer, the Link will display "Up".

Hover your mouse cursor over the appropriate button in the "Name" column to reveal a menu of configurable options.

IP Settings for iSCSI Ports

Click on this option in order to enable DHCP or to manually set up a channel's IP Address, Netmask, and Gateway. Fill in the appropriate information and then click the "Confirm" button.

Set the Default Gateway

Sets the selected channel as the default gateway for the RTX Secure. To disable the default gateway, hover your mouse cursor over the appropriate button in the "Name" column again and select the "Disable default gateway" option. Only one channel can be the default gateway.

Enable Jumbo Frames

Enables jumbo frames for the associated channel. To disable jumbo frames, hover your mouse cursor over the appropriate button in the "Name" column again and select the "Disable jumbo frames" option. The maximum jumbo frame size is 3900 bytes.

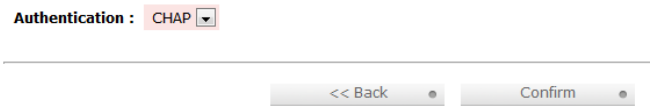
Ping Host

Opens a dialog box in which the user can input the host's IP address to initiate a ping test.

8.6.3 Node

The Node option displays the RTX Secure's entity name, which will be seen by the iSCSI initiator, and allows you to toggle CHAP (Challenge Handshake Authorization Protocol) on or off.

CHAP is disabled by default. To turn on CHAP, click the "Authenticate" button. This will bring up a screen with a dropdown box. Click the dropdown box and select "CHAP", then click the "Confirm" button.



After turning on CHAP authentication, you must set up at least one CHAP account (see Section 8.6.5).

8.6.4 Session

The session function allows you to view information on a session initiated by an iSCSI initiator application (see Section 9), including Initiator Name, TPGT, Error Recovery Level, and Error Recovery Count.

Hover your mouse over the button in the "No." column and click on "List connection." It will list all the connections of the session.

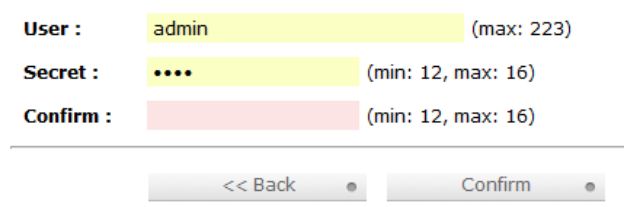
8.6.5 CHAP Account

CHAP (Challenge Handshake Authentication Protocol) is a common iSCSI authentication method. When CHAP is enabled, the RTX Secure will require authentication at login through an iSCSI initiator (see Section 9). Authentication also occurs at various times during the connection, by way of transferring the username, initiator password (also called "initiator secret"), and target password (also called "target secret"). The RTX Secure uses the same value for initiator secret and target secret. For added security, the authentication information is hashed and a token is sent instead of the information itself.

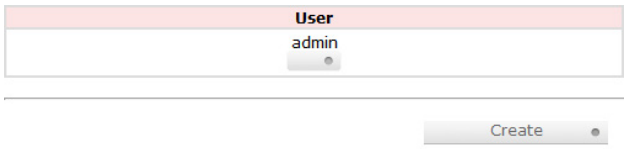
a. To use CHAP, you will need to turn on CHAP authentication (see Section 8.6.3) and then follow the steps there to set up a CHAP account.

b. After clicking on the "CHAP Account" option, you will see the following screen:

Click "Create" to create a new user. This brings up a screen with fields for User, Secret, and Confirm. Enter a user name in the first field, and a 12-16 character password to use as the secret in the second and third fields. Click the "Confirm" button.



c. The new CHAP account will appear on the main CHAP account screen:

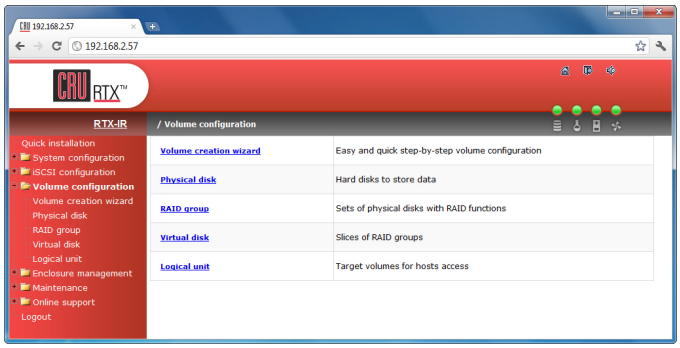


Modifying the CHAP Account

Hover your mouse cursor underneath the username to bring up a menu. Select "Modify user information" to change the username and password, or select "Delete" to remove the user. A confirmation box will appear. Click "OK" and the username will be deleted from the RTX Secure.

8.7 Volume Configuration

The Volume Configuration menu provides the options you will use to set up one or RAID volumes of varying levels on the RTX Secure. Click on Volume Configuration to view the following menu options: Volume Creation Wizard, Physical Disk, Volume Group, User Data Volume, Cache Volume, and Logical Unit.



The following diagram describes the relationship of RAID components in the RTX Secure.

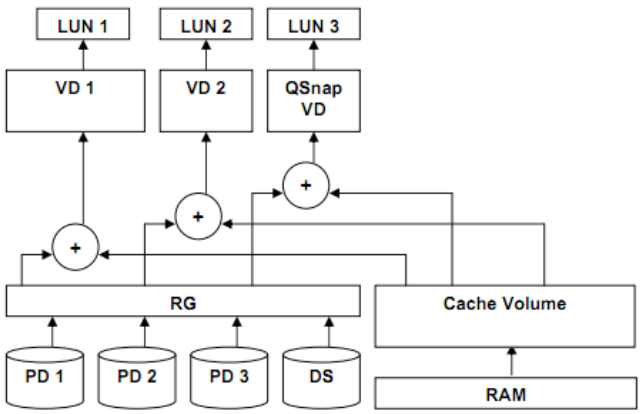


Figure 1.2.3.1

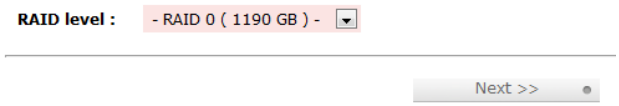
Each RAID Group can be divided into several Virtual Disks. The Virtual Disks in one RAID Group share the same RAID level, but may have different volume capacity. All Virtual Disks share the Cache Volume to execute a data transfers. A Logical Unit Number (LUN) is a unique identifier that the computer uses to distinguish and access SCSI devices.

8.7.1 Volume Creation Wizard

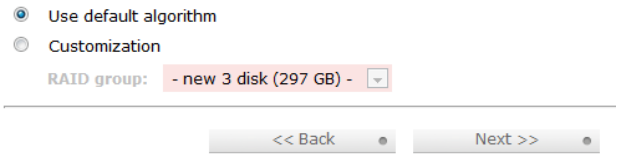
Click on the "Volume Creation Wizard" option to easily set up your RTX Secure with a RAID 0, 1, 3, 5, 6, or 0+1 set. For using higher RAID types or configuring the drives for JBOD access, see Section 8.3.

If any disks are not assigned to a Virtual Disk, it will walk you through a series of steps to create a RAID set. If there are previous RAID Group or Virtual Disk configurations present, the wizard may limit the choices you can select in the following steps.

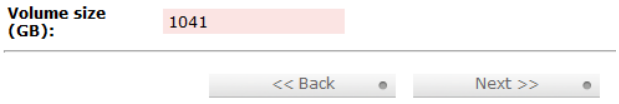
a. Select your desired RAID Level from the drop-down box, then click the "Next" button. The drop-down box displays the drive capacity next the RAID Level.



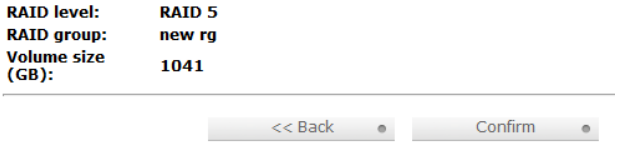
b. Choose how many disks you wish to use in the new RAID Group. The default algorithm uses all of the disks not already assigned to a RAID Group. Or you can choose how many disks you want the new RAID Group to use by selecting the "Customization" radio button and then using the drop-down box to select the number of disks. The drop-down box displays the drive capacity next the number of disks.



c. On the next screen, fill in the size in MB for how large you want the new RAID Group to be, then click the "Next" button. The maximum size is filled in by the wizard automatically, so in most cases you simply need to click the "Next" button.

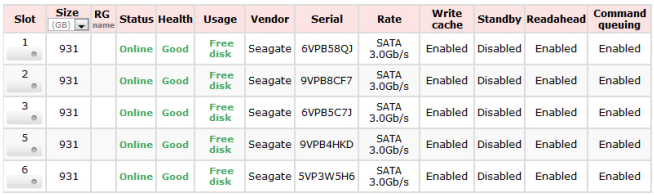


d. Step 4 summarizes the choices you have made. If anything is incorrect, select the "Back" button and navigate backwards through the steps to change your options. If everything looks fine, click "Confirm." The GUI will navigate to the Virtual Disk page which now shows a new Virtual Disk with the name similar to "QUICK#####". Your Virtual Disk is now initializing and may take several hours to complete.



8.7.2 Physical Disk

Click the Physical Disk option to view and modify the status of the drives installed in the RTX Secure.



Slot	Size (GB)	RG name	Status	Health	Usage	Vendor	Serial	Rate	Write cache	Standby	Readahead	Command queuing
1	931		Online	Good	Free disk	Seagate	6VPB58QJ	SATA 3.0Gb/s	Enabled	Disabled	Enabled	Enabled
2	931		Online	Good	Free disk	Seagate	9VPB8CF7	SATA 3.0Gb/s	Enabled	Disabled	Enabled	Enabled
3	931		Online	Good	Free disk	Seagate	6VPB5C7J	SATA 3.0Gb/s	Enabled	Disabled	Enabled	Enabled
5	931		Online	Good	Free disk	Seagate	9VPB4HKD	SATA 3.0Gb/s	Enabled	Disabled	Enabled	Enabled
6	931		Online	Good	Free disk	Seagate	5VP3W5H6	SATA 3.0Gb/s	Enabled	Disabled	Enabled	Enabled

Physical Disk Column Descriptions	
Slot	The slot number of the hard drive. "1" corresponds to the top bay of the RTX Secure, "8" to the bottom bay. Hover your mouse cursor over the button below the slot number to bring up configuration options for that particular hard drive, which are detailed below.
Size	The logical capacity of the drive. Can be displayed in megabytes (MB) or gigabytes (GB).
RG Name	The name of the RAID Group to which the drive is assigned, if any.
Status	Displays the operational status of the disk. • **Online** → The hard drive is online. • **Rebuilding** → The hard drive is being rebuilt. • **Transitioning** → The hard drive is being migrated or is being replaced by another disk during rebuilding. • **Scrubbing** → The hard drive is being scrubbed.
Health	Displays general operational health of the disk. • **Good** → The hard drive is good. • **Failed** → The hard drive has failed. • **Error Alert** → The hard drive's S.M.A.R.T. monitoring system is reporting an error. • **Read Errors** → The hard drive has unrecoverable read errors.
Usage	Displays how the disk is currently being used. • **RAID Disk (RD)** → The hard drive has been assigned to a RAID Group. • **Free Disk (FD)** → The hard drive is free for use. • **Dedicated Spare (DS)** → The hard drive has been set as a dedicated spare of a RAID Group. • **Global Spare (GS)** → The hard drive has been set as a global spare of all RAID Groups.
Vendor	Displays the manufacturer of the hard drive.

Serial	Displays the serial number of the hard drive.
Rate	Displays the transfer speed of the hard drive. • **SATA 1.5Gb/s** → SATA1 disk • **SATA 3.0Gb/s** → SATA2 or SATA3 disk
Write Cache	The hard drive's write cache is enabled or disabled. The default setting is Enabled.
Standby	The hard drive will automatically spin down to save power. The default setting is Disabled.
Readahead	The hard drive has file prefetching enabled. The default setting is Enabled.
Command Queuing	Newer hard drives can queue multiple commands and handle them one by one. The default setting is Enabled.

Modifying Physical Disks

Hover your mouse cursor over the button below the slot number to bring up a series of options for that particular hard drive.

Set Free Disk

Frees the disk from the RAID Group it is attached to and makes it free for use. If the disk is not currently attached to a RAID Group, this option is grayed out.

Set Global Spare

Sets the disk as a spare disk for all existing RAID Groups.

Set Dedicated Spare

Opens a page that allows the administrator to attach the disk as a spare to a specific RAID Group.

Disk Scrub

Scrubs the disk with specific data patterns to securely erase its data.

Upgrade

Opens a page that allows the administrator to upgrade the hard drive firmware. The administrator may simultaneously upgrade all the hard drives in the RTX Secure that are identical to the one selected.

Turn on Indication LED

Turns on the indication LED for the bay in which the physical disk resides.

More information

Displays more details about the hard drive.

8.7.3 RAID Group

The RAID Group screen displays information about all existing RAID Groups. For instructions on how to create a RAID Group, see Section 8.3.1.

No.	Name	Total (GB)	Free (GB)	#PD	#VD	Status	Health	RAID
1	CRU	595	595	5	0	Online	Good	RAID 5

The RAID Group screen displays the following information:

RAID Group Column Descriptions	
No.	The RAID Group number. Hover your mouse cursor over the button below the RAID Group number for configuration options.
Name	The name of the RAID Group.
Total	The total capacity of the RAID Group. The drop-down box allows the user to view the capacity in either MB or GB.
Free	The capacity of the RAID Group that hasn't yet been assigned to a Virtual Disk. The drop-down box allows the user to view the capacity in either MB or GB.
#PD	The number of hard drives in the RAID Group.
#VD	The number of Virtual Disks that have been created as part of the RAID Group.
Status	The status of the RAID Group. • **Online** → The RAID Group is online. • **Offline** → The RAID Group is offline. • **Rebuild** → The RAID Group is currently being rebuilt. • **Migrate** → The RAID Group is currently being migrated. • **Scrubbing** → The RAID Group is being scrubbed. • **Parity Checking** → The RAID Group's parity is being checked.
Health	The health of the RAID Group. • **Good** → The RAID Group is good. • **Failed** → The RAID Group has failed. • **Degraded** → The RAID Group is not healthy and incomplete, due either to a removed hard drive or a failed drive.
RAID	The RAID level of the RAID Group.

Modifying RAID Groups

Hover your mouse cursor over the button below the RAID Group number to bring up a series of options for that particular RAID Group.

Migrate

Allows the administrator to change the RAID Group's RAID level or add disks to the RAID without data loss. The total size of the new RAID Group must be larger or equal to the original RAID Group or the action will trigger an "Invalid RG config" error.

Move

Allows the administrator to change which disks on which the RAID Group exists without losing data. The total size of the new RAID Group must be larger or equal to the original RAID Group or the action will trigger an "Invalid RG config" error.

Activate
Activate RAID Group disk roaming. This option can only be executed when the RAID Group status is offline.

Deactivate
Deactivate the RAID Group disk roaming. This option can only be executed when the RAID Group is online.

Confirm Parity Check
Regenerates parity for the RAID Group. This option allows the administrator to regenerate parity when a parity/data inconsistency is found, or to check parity/data consistency only. Only applies to RAID sets with parity.

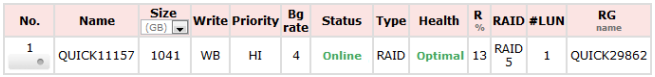
Delete
Deletes the RAID Group.

Set Disk Property
Enable or disable write caching, standby, readahead, and command queuing.

More Information
Displays more details about the RAID Group.

8.7.4 Virtual Disk

The Virtual Disk screen displays any existing Virtual Disks and allows you to create and delete Virtual Disks. For instructions on how to create a Virtual Disk, see Section 8.3.2.



No.	Name	Size (GB)	Write	Priority	Bg rate	Status	Type	Health	R %	RAID	#LUN	RG name
1	QUICK11157	1041	WB	HI	4	Online	RAID	Optimal	13	RAID 5	1	QUICK29862

The following information is displayed:

Virtual Disk Column Descriptions	
No.	The Virtual Disk number. Hover your mouse cursor over the button below the Virtual Disk number for configuration options.
Name	The name of the Virtual Disk.
Total	The total capacity of the Virtual Disk. Can be displayed in MB or GB.
Write	The write status of the Virtual Disk. • **WT** → Write Through • **WB** → Write Back • **RO** → Read Only
Priority	Displays the priority that the RTX Secure will give to RAID activities (rebuild, initialization) versus priority given to file transfers. • **HI** → High Priority • **MD** → Medium Priority • **LO** → Low Priority
BG Rate	Background Task Priority. **4 / 3 / 2 / 1 / 0** → The default value is 4. The higher the number, the more priority will be given to background input/output.
Status	The status of the Virtual Disk. • **Online** → The Virtual Disk is online. • **Offline** → The Virtual Disk is offline. • **Initiating** → The Virtual Disk is being initialized. • **Rebuild** → The Virtual Disk is being rebuilt. • **Migrate** → The Virtual Disk is being migrated. • **Rollback** → The Virtual Disk is being rolled back. • **Parity Checking** → The Virtual Disk is undergoing a parity check.
Type	Indicates that the Virtual Disk is part of a RAID Group.
Health	The health of the Virtual Disk. • **Optimal** → The Virtual Disk is working well and there is no failed physical disk within the RAID Group. • **Degraded** → At least one disk from the RAID Group that the Virtual Disk belongs to is failed or removed from the RTX Secure. • **Failed** → The RAID Group that the Virtual Disk belongs to has failed and cannot recover from data loss. • **Partially Optimal** → The Virtual Disk has experienced recoverable read errors. After passing a parity check, the health status will change to Optimal.
R%	Shows the percentage completed of an initialization or RAID rebuild.
RAID	Displays the RAID level.
#LUN	The number of Logical Unit Numbers that are attached to the Virtual Disk.
RG Name	The name of the RAID Group to which the Virtual Disk belongs.

Modifying Virtual Disks
Hover your mouse cursor over the button below the Virtual Disk number to bring up a series of options for that particular Virtual Disk.

Extend
Extend the Virtual Disk capacity.

Confirm Parity Check
Regenerates parity for the RAID Group. This option allows the administrator to regenerate parity when a parity/data inconsistency is found, or to check parity/data consistency only. Only applies to RAID sets with parity.

Delete
Deletes the Virtual Disk.

Set Property
Allows the administrator to change the Virtual Disk name, change the write status, priority, background task priority, and enable or disable Readahead.

Attach LUN
Attach a Logical Unit Number to the Virtual Disk.

Detach LUN
Detach a Logical Unit Number from the Virtual Disk.

List LUN
Lists all Logical Unit Numbers attached to the Virtual Disk.

More Information
Displays more details about the Virtual Disk, including the LUNs that have been attached to it.

8.7.5 Logical Unit

The Logical Unit is what your computer will use to access and manage SCSI devices. For instructions on how to attach a Logical Unit to a Virtual Disk, see Section 8.3.3.

Host	LUN	Permission	VD name	#Session
*	0	Read-write	VD1	0

Attach

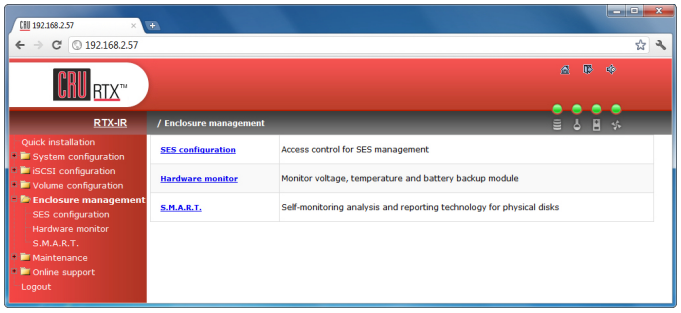
The following information is displayed:

Logical Unit Column Descriptions	
Host	The host address which can access the attached Virtual Disk. An asterisk indicates that any host may access the attached Virtual Disk. Hover your mouse cursor over the button below the Host for configuration options.
LUN	The Logical Unit Number (LUN).
Permission	Displays the permissions given to hosts accessing the RAID set through this Logical Unit. • **Read-Write** → Has permissions to read and write to the disks. • **Read-Only** → Has permission to read but not write to the disks.
VD Name	The name of the associated Virtual Disk.
#Session	The number of host sessions currently accessing the Logical Unit.

Modifying Logical Units
Hover your mouse cursor over the button below the Host to bring up a series of options for that particular Logical Unit.

Detach
Detaches the Logical Unit from a Virtual Disk and deletes it.

8.8 Enclosure Management
Enclosure management gives access to the following menu options: SES Configuration, Hardware Monitor, and S.M.A.R.T.



8.8.1 SES Configuration

SCSI Enclosure Services, or SES, is a command set that is used to manage and sense the state of the power supplies, cooling devices, displays, indicators, and individual drives of a SCSI device. The RTX Secure is an SES compliant enclosure. However, in order to use manage the RTX Secure using SES you must have the appropriate software installed on your computer. An example is SMARTMon, a S.M.A.R.T. disk monitor, offered by Santools at www.santools.com.

To enable SES on the RTX Secure, you must have a Virtual Disk set up and a Logical Unit attached. Once you have done this, navigate to SES Configuration and simply click the "Enable" button, then click "Confirm". The SES-enabled LUN will show up on the main SES screen.

Host	LUN
*	0

Disable

8.8.2 Hardware Monitor

The Hardware Monitor displays information about the voltages and temperatures of the RTX Secure.

Temperature : (C)

Type	Item	Value	Status
Voltage	Onboard +1.2V	+1.18 V (min = +1.08 V, max = +1.32 V)	OK
	Onboard +3.3V	+3.34 V (min = +3.04 V, max = +3.56 V)	OK
	Onboard +5V	+5.07 V (min = +4.60 V, max = +5.40 V)	OK
	Onboard +12V	+12.23 V (min = +11.04 V, max = +12.96 V)	OK
	Onboard +1.8V	+1.84 V (min = +1.62 V, max = +1.98 V)	OK
Temperature	Core Processor	+45.0 (C) (hyst = +0.0 (C), high = +80.0 (C))	OK
	iSCSI NIC	+49.0 (C) (hyst = +0.0 (C), high = +65.0 (C))	OK
	Location 1	+42.5 (C) (hyst = +0.0 (C), high = +65.0 (C))	OK
Cooling	FAN1	1824 RPM	OK
	FAN2	2033 RPM	OK

Auto shutdown : ☑

Confirm

Auto Shutdown
When this checkbox is enabled, the RTX Secure will automatically shut down if any of each items' voltage or temperature strays outside of the minimum or maximum displayed values. Auto shutdown is enabled by default to protect the hardware of the RTX Secure.

8.8.3 S.M.A.R.T.

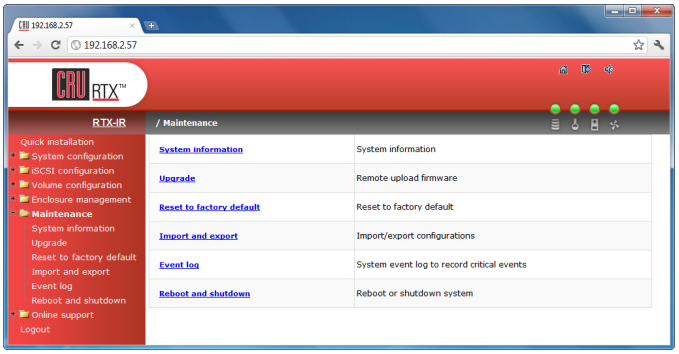
S.M.A.R.T. (Self-Monitoring Analysis and Reporting Technology) is a diagnostic tool for hard drives that gives advanced warning in some cases of hard drive failure. S.M.A.R.T. measures various attributes of a hard drive at all times to detect if certain values have moved outside of a certain range. The S.M.A.R.T. option allows you to view the S.M.A.R.T. status of all of your hard drives.

Slot	Read error rate	Spin up time	Reallocated sector count	Seek error rate	Spin up retries	Calibration retries	Temperature
1	117(6)	95(0)	100(36)	72(30)	100(97)	N/A	28
2	111(6)	95(0)	100(36)	72(30)	100(97)	N/A	29
3	119(6)	95(0)	100(36)	71(30)	100(97)	N/A	30
5	117(6)	94(0)	100(36)	71(30)	100(97)	N/A	31
6	107(6)	95(0)	100(36)	63(30)	100(97)	N/A	32

RTX Secure's S.M.A.R.T. technology only supports SATA drives. SAS drives do not have this function and will display "N/A" in the GUI.

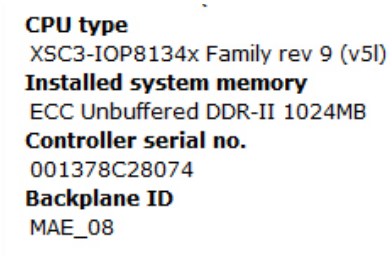
8.9 Maintenance

The Maintenance screen gives access to the firmware and configuration functions: System Information, Upgrade, Reset to Factory Default, Import and Export, Event Log, and Reboot and Shutdown.



8.9.1 System Information

Click on System Information to display the RTX Secure's hardware profile information.

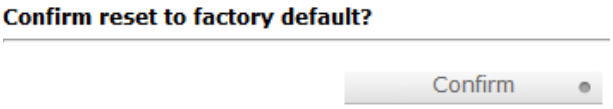


8.9.2 Upgrade

The upgrade function allows you to upgrade the firmware of the RTX Secure. **DO NOT USE THIS FUNCTION WITHOUT SPECIFIC INSTRUCTION FROM CRU-DATAPORT TECHNICAL SUPPORT.** Doing so could result in malfunction of your RTX Secure.

8.9.3 Reset to Factory Default

The Reset to Factory Default option allows you to restore settings to the factory defaults. Click on the "Confirm" button to verify.

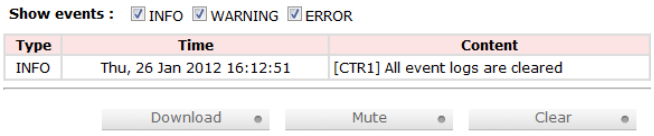


8.9.4 Import & Export

The Import & Export function allows you to import or export a firmware configuration file. **DO NOT USE THIS FUNCTION WITHOUT SPECIFIC INSTRUCTION FROM CRU-DATAPORT TECHNICAL SUPPORT.** Doing so could result in malfunction of your RTX Secure.

8.9.5 Event Log

The Event Log allows you to view event messages. Check or uncheck the checkboxes of "Info", "Warning", and "Error" filter the events displayed. Click the "Download" button to save the entire event log as a text file. Click the "Clear" button to clear all event logs. Click the "Mute" button to stop the alarm if it is engaged.



8.9.6 Reboot and Shutdown

The Reboot and Shutdown feature allows you to reboot or shutdown the RTX Secure's RAID and LCD controllers. Note: Choosing "Shutdown" will not shut down the physical components of the RTX Secure (fans, drives, power supply). However, it will flush data from the cache to the physical drives, which is recommended to prevent data corruption before physically shutting down using the power switch on the back of the unit.

8.10 Online Support

This screen contains helpful links to cru-dataport.com, including one for the "Product Information and Specs" of your unit and one for "FAQs and Downloads".

8.11 Logout

This screen allows you to log out of and exit the GUI.

9 iSCSI Initiator Software

9.1 Software Installation

This is a required step. Any computer must have initiator software installed before it can connect to an iSCSI device such as the RTX Secure. Both freeware and commercial software utilities are available for this purpose.

Note: Initiator software is not required for additional computers that share files with the host computer attached to the RTX Secure. In such a scenario, the host computer acts as a server to the other computers. Only the computer directly accessing the RTX Secure needs initiator software.

NOTE: Initiator software is not required for additional computers that share files with the host computer. In such a scenario, the host computer acts as a server to the other computers. Only the computer directly accessing the RTX Secure needs initiator software.

9.1.1 Windows

Users can download free Microsoft iSCSI Initiator software at the following URL:

www.microsoft.com/download/en/details.aspx?id=18986

Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2008 R2 users already have the Microsoft iSCSI Initiator installed by default, which can be launched by double-clicking on the iSCSI Initiator icon in the Administrative Tools folder in the Control Panel.

9.1.2 MacOS X

Studio Network Solutions makes globalSAN iSCSI initiator, a free-to-try utility for MacOS X, available here:

www.studionetworksolutions.com/support/faq.php?pi=11&fi=51

ATTO Technologies also makes a commercial iSCSI initiator for MacOS X:

www.attotech.com/xtend.html

9.1.3 Linux

Open-iSCSI initiator software is available for Linux users to download.

Website: www.open-iscsi.org/
Readme: www.open-iscsi.org/docs/README

9.2 Access the RTX Secure Using iSCSI Initiator Software

9.2.1 Basic Access Instructions

The process for using initiator software to access the RTX Secure varies depending on the software used. Read the documentation accompanying the software for details. However, the general steps are as follows:

a. Launch the initiator application.

b. Type in the IP address of the CH-1 or CH-2 connection on the RTX Secure (depending which connection link is shown as "Up" on the NIC screen (this as well as the address is determined in Section 8.6.2). This will be a different IP address than the one used to access the GUI.

c. The RTX Secure volume will mount to your computer and appear as an internal SCSI drive. Newly-created volumes will need to be formatted before they can be used. If you purchased the RTX Secure with drives preinstalled by CRU-DataPort, the volume(s) will already have been created and formatted appropriately for your computer.

Below are additional instructions for two common iSCSI Initiator utilities:

9.2.2 Microsoft iSCSI Initiator for Windows

This software can by launched by double-clicking on the iSCSI Initiator icon in the Administrative Tools folder in the Control Panel.

Windows XP, Windows Vista, and Windows Server 2008

a. If you have set up CHAP in the RTX Secure GUI (Section 8.6.5), input the proper information by clicking on "General" tab and then clicking on the "Secret" button.

b. Select the "Discovery" tab. Under Target Portals, click the "Add" or "Add Portal…" button and enter the IP address for the RTX Secure's CH-1 or CH-2 port (depending which connection link is shown as "Up" on the NIC screen in the GUI (this as well as the address is determined in Section 8.6.2).

c. Next, select the "Targets" tab. You should see the RTX Secure in the list of available targets.

d. Select the RTX Secure target and click "Log on." Leave the default settings alone and click "OK".

If the log-on is successful you'll now be able to use the RTX Secure just like any other disk attached to your computer.

Windows 7 and Windows Server 2008 R2

a. After you launch the initiator, input the IP address for the RTX Secure's CH-1 or CH-2 port (depending which connection link is shown as "Up" on the NIC screen in the GUI (this as well as the address is determined in Section 8.6.2).

b. Click on the "Quick Connect…" button.

If the log-on is successful you'll now be able to use the RTX Secure just like any other disk attached to your computer.

NOTE: The Quick Connect feature does not support advanced connection types like CHAP. For instructions on connecting to an iSCSI target using advanced settings, visit the following URL:

http://technet.microsoft.com/en-us/library/ee338480(v=ws.10).aspx#BKMK_ConnectAdvanced

9.2.3 GlobalSAN iSCSI Initiator for MacOS

This software can be launched by double-clicking on the globalSAN iSCSI icon in System Preferences.

a. After you launch the initiator you'll see the globalSAN window pop up. Press the Add button ("+") and choose Portal from the dropdown menu to add a new portal.

b. On the Add Portal dialog box, enter the IP address for the RTX Secure's CH-1 or CH-2 port depending which connection link is shown as "Up" on the NIC screen (this as well as the address is determined in Section 8.6.2), and then click OK.

c. If you have set up CHAP in the RTX Secure GUI (Section 8.6.5), input the proper information by clicking on the "Authentication Settings" button.

d. Select the new target in the list to the left, then select the appropriate connection from the list that opens up on the right side and click the "Connect" button.

If the log-on is successful you'll now be able to use the RTX Secure just like any other disk attached to your computer.

10 Usage with Mac and Windows Operating Systems

10.2 Usage with Windows Operating Systems

10.1.1 Compatibility

The RTX Secure supports 3.5" SATA hard drives.

10.1.2 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), then select "Manage". The Computer Management window will open.

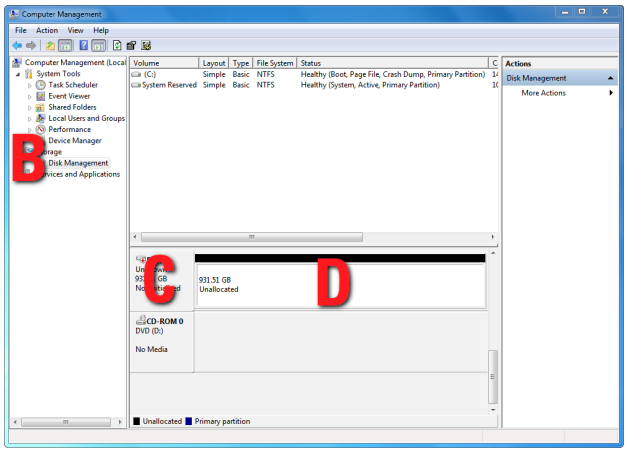
b. In the left pane of this window, left-click on Disk Management (labeled 'B' in the picture below).

c. The volume should appear in the list of Disks in the lower middle/right pane. You may need to scroll down to see it. If the volume 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 volume before formatting it.

Initialize the volume by right-clicking the Device Properties Box (labeled 'C' in the picture below) and selecting "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 or 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, Server 2008, Server 2008 R2).



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" unless you want to completely erase any data on the volume 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 (Windows XP) or by clicking on the Computer button in the Start Menu (Windows Vista, 7, Server 2008, Server 2008 R2).

10.1.3 Mounting and Unmounting Volumes

Mounting Volumes
First ensure that you have established a connection to the RTX Secure using iSCSI initiator software (See Section 9). Then, 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 on the My Computer icon on the desktop (Windows XP) or by clicking the Computer button in the Start Menu (Windows Vista, 7, Server 2008, Server 2008 R2).

Unmounting Volumes
Log off the volume using your iSCSI initiator software. In the Microsoft iSCSI Initiator, you can log off from the "Targets" tab. On Windows XP and Windows Server 2008, select the target and click the Details button. Select the target identifier and then click Log Off.

For Windows Vista, Windows 7, and Windows Server 2008 R2, select the target and then click on the Disconnect button.

10.1 Usage with Mac OS X

10.1.1 Compatibility

The RTX Secure supports 3.5" SATA hard drives.

10.1.2 Formatting a Drive

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

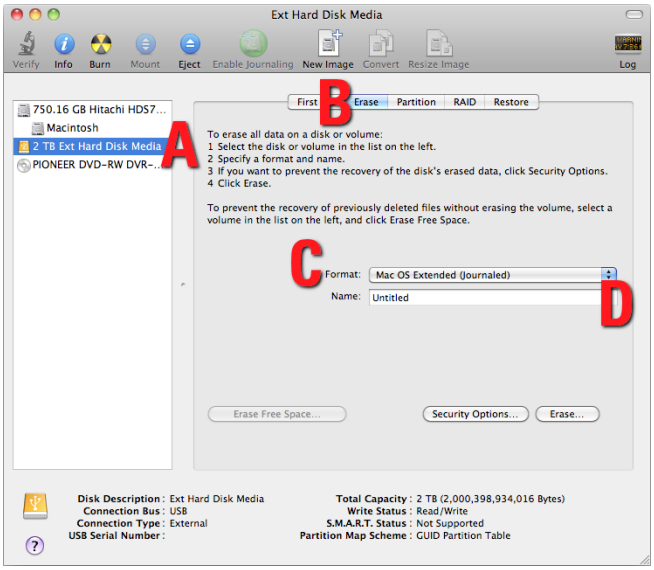
a. Click on the volume in the window to the left.

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 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.



10.1.3 Mounting and Unmounting Volumes

Mounting 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 volume (see section above).

Unmounting Volumes
First, eject the data volume by dragging the volume's icon to the trash bin, or by selecting the icon then pressing Command-E. Next, log off the volume in your iSCSI initiator software. If you are using the GlobalSAN Initiator, select "Log Off" from the "Targets" tab.

Disconnecting in this way allows you to reconnect quickly later. Another way of preventing delays is to keep your iSCSI initiator software open at all times. You can minimize it and allow it to run in the background. Closing the software and then reopening it can cause a lengthy delay before access to the RTX Secure is reestablished.

NOTE: It is strongly suggested that you disable automatic sleep mode on your Mac. You can still put the Mac to sleep manually at any time as long as you follow the above procedures. This will prevent reconnection difficulties.

10.1.4 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 the RTX Secure hard drive only some of the time.

11 RAID Is Not A Backup

Because the 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 complete 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!

12 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.

13 Event Notifications

Physical Disk Events		
Level	**Type**	**Description**
Info	PD inserted	Disk <slot> is inserted into system
Warning	Disk removed	Disk <slot> is removed from system
Error	HDD read error	Disk <slot> read block error
Error	HDD write error	Disk <slot> write block error
Error	HDD error	Disk <slot> is disabled
Error	HDD IO timeout	Disk <slot> gets no response
Info	PD upgrade started	PD [<string>] starts upgrading firmware process
Info	PD upgrade finished	PD [<string>] finished upgrading firmware process
Warning	PD upgrade failed	PD [<string>] upgrade firmware failed

Physical HW Events		
Level	**Type**	**Description**
Warning	ECC single	Single-bit ECC error is detected at <address>
Error	ECC multiple	Multi-bit ECC error is detected at <address>
Info	ECC dimm	ECC Memory is installed
Info	ECC none	Non-ECC Memory is installed
Info	SCSI bus reset	Received SCSI Bus Reset event at the SCSI Bus <number>
Error	SCSI host error	SCSI Host allocation failed

Level	Type	Description
Error	SATA enable device fail	Failed to enable the SATA PCI device
Error	SATA EDMA mem fail	Failed to allocate memory for SATA EDMA
Error	SATA remap mem fail	Failed to remap SATA memory IO space
Error	SATA PRD mem fail	Failed ot initialize SATA PRD memory manager
Error	SATA revision ID fail	Failed to get SATA revision ID
Error	SATA reg fail	Failed to set SATA register
Error	SATA init fail	Core failed to initialize the SATA adapter
Error	SATA diag fail	SATA Adapter diagnostics failed
Error	Mode ID fail	SATA Mode ID failed
Error	SATA chip count error	SATA chip count error
Info	SAS port reply error	SAS HBA port <number> reply terminated abnormally
Info	SAS unknown port reply error	SAS frontend reply terminated abnormally
Info	FC port reply error	FC HBA port <number> reply terminated abnormally
Info	FC unknown port reply error	FC frontend reply terminated abnormally

EMS Events		
Level	**Type**	**Description**
Info	Power install	Power(<string>) is installed
Error	Power absent	Power(<string>) is absent
Info	Power restore	Power(<string>) is restored to work
Error	Power fail	Power(<string>) is not functioning
Warning	Power detect	PSU signal detection(<string>)
Info	Fan restore	Fan(<string>) is restored to work
Error	Fan fail	Fan(<string>) is not functioning
Info	Fan install	Fan(<string>) is installed
Error	Fan not present	Fan(<string>) is not present
Error	Fan over speed	Fan(<string>) is over speed
Warning	Thermal level 1	System temperature(<string>) is higher
Error	Thermal level 2	System overheated(<string>)!!!
Error	Thermal level 2 shutdown	System overheated(<string>)!!! The system will auto-shutdown immediately.
Error	Thermal level 2 CTR shutdown	The controller will auto shutdown immediately, reason [Overheated(<string>)].
Warning	Thermal ignore value	Unable to update thermal value on <string>
Warning	Voltage level 1	System voltage(<string>) is higher/lower.

Level	Type	Description
Error	Voltage level 2	System voltages(<string>) failed!!!
Error	Voltage level 2 shutdown	System voltages(<string>) failed!!! The system will autho shutdown immediately.
Error	Voltage level 2 CTR shutdown	The controller will auto shutdown immediately, reason [Voltage abnormal(<string>)].
Info	UPS OK	Successfully detect UPS
Warning	UPS fail	Failed to detect UPS
Error	UPS AC loss	AC loss for system detected
Error	UPS power low	UPS Power Low!!! The system will auto-shutdown immediately.
Warning	SMART T.E.C.	Disk <slot> S.M.A.R.T. Threshold Exceed Condition occurred for attribute <string>
Warning	SMART fail	Disk <slot>: Failure to get S.M.A.R.T. information
Warning	RedBoot failover	RedBoot failover event occurred
Warning	Watchdog shutdown	Watchdog timeout shutdown occurred
Warning	Watchdog reset	Watchdog timeout reset occurred
Info	Console Login	<username> login from <IP or serial console> via Console UI
Info	Console Logout	<username> logout from <IP or serial console> via Console UI
Info	Web Login	<username> login from <IP> via Web UI
Info	Web Logout	<username logout from <IP> via Web UI
Info	Log clear	All event logs are cleared
Warning	Send mail fail	Failed to send event to <email>

LVM Events		
Level	**Type**	**Description**
Info	RG create OK	RG <name> has been created
Info	RG create fail	Failed to create RG <name>
Info	RG delete	RG <name> has been deleted
Info	RG rename	RG <name> has been renamed as <name>
Info	VD create OK	VD <name> has been created.
Info	VD create fail	Failed to create VD <name>
Info	VD delete	VD <name> has been deleted
Info	VD rename	The name of VD <name> has been renamed to <name>
Info	VD read only	Cache policy of VD <name> has been set as read only
Info	VD write back	Cache policy of VD <name> has been set as write-back

Level	Type	Description
Info	VD write through	Cache policy of VD <name> has been set as write-through
Info	VD extend	Size of VD <name> extends
Info	VD attach LUN OK	VD <name> has been LUN-attached
Info	VD attach LUN fail	Failed to attach LUN to VD <name>
Info	VD detach LUN OK	VD <name> has been detached
Info	VD detach LUN fail	Failed to detach LUN from bus <number> SCSI ID <number>, LUN <number>
Info	VD init started	VD <name> starts initialization
Info	VD init finished	VD <name> completes initialization
Warning	VD init failed	Failed to complete initialization of VD <name>
Info	VD rebuild started	VD <name> starts rebuilding
Info	VD rebuild finished	VD <name> completes rebuilding
Warning	VD rebuild failed	Failed to complete rebuild of VD <name>
Info	VD migrate started	VD <name> starts migration
Info	VD migrate finished	VD <name> completes migration
Error	VD migrate failed	Failed to complete migration of VD <name>
Info	VD scrub started	Parity checking on VD <name> starts
Info	VD scrub finished	Parity checking on VD <name> completes with <address> parity/data inconsistency found
Info	VD scrub aborted	Parity checking on VD <name> stops with <address> parity/data inconsistency found
Info	RG migrate started	RG <name> starts migration
Info	RG migrate finished	RG <name> completes migration
Info	RG move started	RG <name> starts move
Info	RG move finished	RG <name> completes move
Info	VD move started	VD <name> starts move
Info	VD move finished	VD <name> completes move
Error	VD move failed	Failed to complete move of VD <name>
Info	RG activated	RG <name> has been manually activated
Info	RG deactivated	RG <name> has been manually deactivated
Info	VD rewrite started	Rewrite at LBA <address> of VD <name> starts
Info	VD rewrite finished	Rewrite at LBA <address> of VD <name> completes
Warning	VD rewrite failed	Rewrite at LBA <address> of VD <name> failed
Warning	RG degraded	RG <name> is in degraded mode

Level	Type	Description
Warning	VD degraded	VD <name> is in degraded mode
Error	RG failed	RG <name> is failed
Error	VD failed	VD <name> is failed
Error	VD IO fault	I/O failure for stripe number <address> in VD <name>
Warning	Recoverable read error	Recoverable read error occurred at LBA <address> - <address> of VD <name>
Warning	Recoverable write error	Recoverable write error occurred at LBA <address> - <address> of VD <name>
Error	Unrecoverable read error	Unrecoverable read error occurred at LBA <address> - <address> of VD <name>
Error	Unrecoverable write error	Unrecoverable write error occurred at LBA <address> - <address> of VD <name>
Error	Config read rail	Config read failed at LBA <address> - <address> of PD <slot>
Error	Config write fail	Config write failed at LBA <address> - <address> of PD <slot>
Error	CV boot error adjust global	Failed to change size of the global cache
Info	CV boot global	The global cache is OK
Error	CV boot error reate global	Failed to create the global cache
Info	PD dedicated spare	Assign PD <slot> to be dedicated spare disk of RG <name>
Info	PD global spare	Assign PD <slot> to Global Spare Disks
Warning	PD read error	Read error occurred at LBA <address> - <address> of PD <slot>
Warning	PD write error	Write error occurted at LBA <address> - <address> of PD <slot>
Warning	Scrub wrong parity	The parity/data inconsistency is found at LBA <address> - <address> when checking parity on VD <name>
Warning	Scrub data recovered	The data at LBA <address> - <address> is recovered when checking parity on VD <name>
Info	PD freed	PD <slot> has been freed from RG <name>
Info	RG imported	Configuration of RG <name> has been imported
Info	RG restored	Configuration of RG <name> has been restored
Info	VD restored	Configuration of VD <name> has been restored
Info	PD scrub started	PD <slot> starts disk scrubbing process
Info	Disk scrub finished	PD <slot> completed disk scrubbing process
Info	Large RG created	A large RG <name> with <number> disks included is created

Level	Type	Description
Info	Weak RG created	A RG <name> made up disks across <number> chassis is created
Info	RG size shrunk	The total size of RG <name> shrunk
Info	VD erase finished	VD <name> finished erasing process
Warning	VD erase failed	The erasing process of VD <name> failed
Info	VD erase started	VD <name> starts erasing process

iSCSI Events		
Level	**Type**	**Description**
Info	iSCSI login accepted	iSCSI login from <IP> succeeds
Info	iSCSI login rejected	ISCSI login from <IP> was rejected, reason [<string>]
Info	iSCSI logout recvd	iSCSI logout from <IP> was received, reason [<string>]

System Maintenance Events		
Level	**Type**	**Description**
Info	System shutdown	System shutdown
Info	System reboot	System reboot
Info	System console shutdown	System shutdown from <string> via Console UI
Info	System web shutdown	System shutdown from <string> via Web UI
Info	System button shutdown	System shutdown via power button
Info	System LCM shutdown	System shutdown via LCM
Info	FW upgrade start	System firmware upgrade starts
Info	FW upgrade success	System firmware upgrade succeeds
Warning	FW upgrade failure	System firmware upgrade is failed
Error	IPC FW upgrade timeout	System firmware upgrade timeout on another controller
Info	Config imported	<string> config imported

HAC Events		
Level	**Type**	**Description**
Info	RG owner changed	The preferred owner of RG <name> has been changed to controller <number>
Info	Force CTR write through	Controller <number> forced to adopt write-through mode on failover
Info	Restore CTR cache mode	Controller <number> restored to previous caching mode on failback
Info	Failover complete	All volumes in controller <number> completed failover process
Info	Failback complete	All volumes in controller <number> completed failback process
Info	CTR inserted	Controller <number> is inserted into system
Error	CTR removed	Controller <number> is removed from system
Error	CTR timeout	Controller <number> gets no response
Error	CTR lockdown	Controller <number> is locked down
Error	CTR memory NG	Memory size mismatch
Error	CTR firmware NG	Firmware version mismatch
Error	CTR lowspeed NG	Low speed inter link is down
Error	CTR highspeed NG	High speed inter link is down
Error	CTR backend NG	SAS expander is down
Error	CTR frontend NG	FC IO controller is down
Info	CTR reboot FW sync	Controller reboot, reason [Firmware synchronization completed]

14 Working With Volumes Larger Than 2TB in Size

Although the RTX Secure can create data volumes larger than 2TB, some older operating systems cannot access such volumes. This is because they support only 32-bit LBA (Logical Block Addressing).

Newer operating systems (Windows Server 2003, Vista, Windows 7, Mac OS 10.5.x and higher) should be able to use 2TB+ volumes without difficulty. You will simply need to do one of the following two things while creating a Virtual Disk:

- Change the LBA to 64-bit
- Increase the block size to 4096

Windows

Windows XP can only use 2TB+ volumes by increasing the block size to 4096. Neither of the options above will work for operating systems older than Windows XP. You will need to make more than one Virtual Disk, each less than 2TB in size. Each Virtual Disk also needs a different LUN.

Mac OS

Although Mac OS 10.4.x supports only 32-bit LBA, increasing the block size to 4096 will allow you to create a 2TB+ volume that is usable by the OS.

Linux

Versions of Linux vary, but using one of the above methods may allow you to create a 2TB+ volume that your distribution can use.

15 Frequently Asked Questions (FAQ)

Q: I created one volume, but my computer sees two of them. Why?

A: There may be two Logical Unit Numbers (LUN) assigned to that volume. To check this, use the GUI. Navigate to "Volume Configuration" and then "Logical Unit". If there are two Logical Units for the same volume, hover your mouse over the button for one of them in the "Host" column and click on "Detach."

NOTE: You may still see two volumes until you restart your computer.

Q: I've connected the RTX to my DHCP-enabled network through the Config GUI port, but the LCD displays an IP address that is not on my network and I cannot connect to the GUI control panel using that IP address in my web browser.

A: This may occur if you plugged in your cable into the Config GUI port after the RTX Secure has already started up and initialized, or if you previously configured the RTX Secure for a static network or direct connection. The solution is to use the LCD interface to obtain a DHCP address. Press "ENT", then use the ▲(Up) or ▼(Down) arrows to scroll to the option "Change IP Config". Press "ENT". The screen will say "DHCP". Press "ENT", then press the ▲(Up) arrow to select "Yes". Press "ENT". RTX will now attempt to acquire a DHCP address. This new address will be displayed on the main screen of the LCD.

Q: When I try to log on to the RTX Secure using the IP address under the iSCSI configuration menu, nothing happens.

A: Sometimes when you first set up the RTX Secure you'll need to reattach the Logical Unit if it doesn't work the first time.

Q: How many computers can connect to one data volume on the iSCSI unit?

A: The short answer is one computer to one volume. This is the safest and suggested usage of the RTX Secure. If two people are accessing files on the same volume at the same time, there is a very high chance that data corruption will occur. There are a few file systems that can handle different users manipulating the same volume, but they are not supported by Mac OS or Windows. However, if the users connected to the volume have read-only access, then corruption will not be an issue.

Q: When I make more than one volume, I still see all volumes when connecting to the iSCSI IP address. How am I supposed to allow only one person per volume if that's the case?

A: When you attach a Logical Unit to a Virtual Disk you'll probably notice a "Host" field with an asterisk as the default selection. This means that any iSCSI Initiator will be able to connect to that volume through that Virtual Disk. All iSCSI Initiators have a unique name. You can use this name to restrict access to only certain computers. For example, if my initiator is assigned the name iqn.1991-05.com.microsoft:username01.crudataport.local, and if I put that name into the host field when attaching a Logical Unit, then only my specific computer will be able to connect to that volume. You can use this to give one person read access and everyone else write access by attaching two Logical Units to one Virtual Disk.

Q: If I connect one computer to the RTX Secure and then share the files from that computer, can more than one computer access the files? Would the other computers need iSCSI initiators installed on them?

A: One computer at a time can directly access the RTX Secure, but files on the RTX Secure can be shared from that computer to other computers. In such a scenario, the computer attached to the RTX Secure acts as a server. Only the server computer requires an iSCSI initiator. The other computers do not need special software.

Q: What is the difference between iSCSI and NAS (Network Attached Storage)?

A: The difference between iSCSI and NAS is that a NAS does not need a computer to act as a server.

Q: I put my computer to sleep, and now it's having trouble reconnecting to RTX. How can I prevent this?

A: To prevent difficulties such as this, follow the shutdown procedure documented in the LCD menu diagram in Section 7.2.3. CRU-DataPort also suggests that you disable automatic sleep on your computer so it does not go into sleep mode without preparing the RTX Secure for disconnection.

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

A: 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.

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 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.

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 5.3 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 at www.cru-dataport.com/support or call us toll free at (800) 260-9800.

16. Technical Specifications

Product Models	RTX Secure 610-IR and RTX Secure 810-IR
RAID Levels Supported	RAID 0, 1, 3, 5, 6, 0+1, 10, 30, 50, 60, & JBOD
Host Interfaces	Dual Gigabit Ethernet
Data Interface Speeds	Up to 200MB/s (network dependent)
Drive Types Supported	3.5-inch SATA (Serial-ATA) hard disk drives
Online Auto-Rebuild	Yes
TrayFree Technology	Yes
TrayFree Shock Absorbing Bays	Yes
LED Indicators	• Alarm Indicator • Power Indicator • Access Indicator
Security	Separate key lock for each HDD (RTX Secure 610-IR only)
Controller Display	LCD screen with yellow backlight/control panel
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 model), 350 Watts (6-bay and 8-bay models)
Cooling Fan	Two 8cm Ball Bearing Fans
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 610-IR: 28 lbs. without drives, 40 lbs. with drives • RTX Secure 810-IR: 33 lbs. without drives, 45 lbs. 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 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.