DataPort SecureDock™ with Internal Key User Manual

Models Covered:

DataPort SecureDock with Internal Key and AES 128 (USB+SATA)
DataPort SecureDock with Internal Key and AES 256 (USB+SATA)
DataPort SecureDock with Internal Key and AES 128 (FireWire800+USB+SATA)
DataPort SecureDock with Internal Key and AES 256 (FireWire800+USB+SATA)

- Hardware-based AES 128-bit or 256-bit Encryption – Offers affordable military-grade AES 128-bit or 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).

- No Key Management – The encryption key is mounted inside of the dock. Simply remove the carrier and the hard drive is encrypted.

- DataPort 10 Design – A rugged metal design that incorporates a patented temperature controlled cooling system for ultimate data protection.

Table of Contents

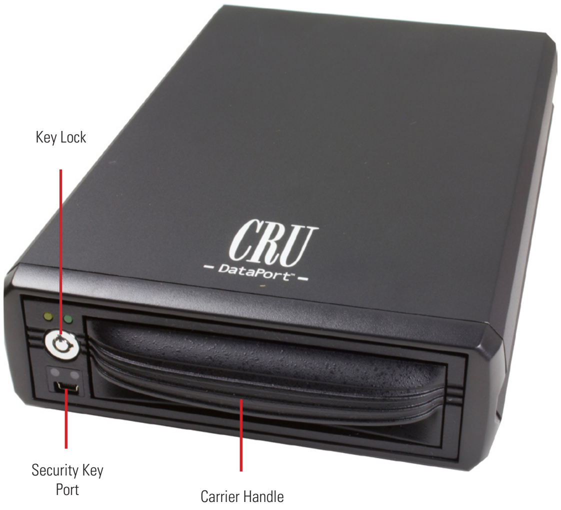
1. Pre-Installation Steps

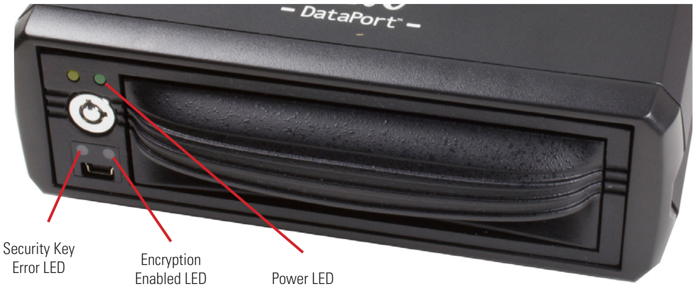
1.1 Box Contents

The following list contains the items that are included in the complete configuration for this device. Depending on which configuration and accessories you purchased, the package may include fewer items than what are listed here. Please contact CRU-DataPort if any items are missing or damaged:

Accessories	Quantity
DataPort Carrier	1
#6-32x1/4 flat-head drive mounting screws	5
AC Adapter	1
DataPort Keys	2
eSATA Cable	1
Security Keys	3
Lanyards for Security Keys	3
Security Key ID Tag	3
Security Key Labels	6

1.2 Identifying Parts of Your DataPort SecureDock with Internal Key





1.3 Warnings and Notices ⚠

Please read the following before beginning installation.

- The main circuit boards of the SecureDock and carrier 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, vibration and percussion.

- Avoid placing the SecureDock and carrier close to magnetic devices, high voltage devices, or near a heat source, including any place where the product will be subject to direct sunlight. Do NOT allow water to make contact with any Security Keys, carrier or SecureDock.

- Though the Security Key port is mechanically identical to a 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 DataPort Secure products.

  Likewise, inserting a Mini-USB cable or other device into the DataPort SecureDock with Internal Key Security Key port on the carrier can cause internal damage and potentially lead to loss of data.

- Any time power is cycled on the DataPort SecureDock with Internal Key, the encryption key will need to be installed in order to access the data on the drive.

2. Installation Steps

2.1 Security Key Installation

The Security Key Installation steps only need to be followed if you have purchased a version of the DataPort SecureDock that does not include an internal Security Key.

a. Slide the two large tabs in on the rear of the SecureDock. Then slide the cover back approximately two inches until it catches and then pull up to remove the cover.

b. Use a Phillips-head screwdriver to remove the screws securing the receiving frame to the SecureDock.

c. Unplug the power (the 4-wired cable) and data connectors (the red SATA cable) from the rear of the receiving frame and remove the receiving frame from the SecureDock.

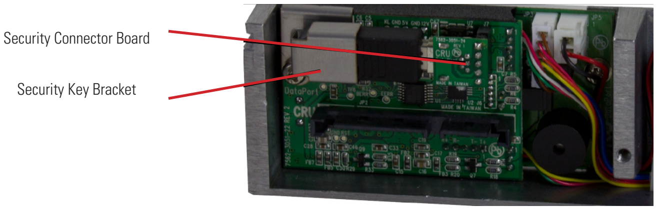
d. Remove the screw holding the Security Key bracket in place to the rear of the receiving frame.

e. Slide the Security Key connector board off the rear of the receiving frame.

f. Insert a Security Key into the connector board.

g. Slide the connector board back into place.

h. Fasten the Security Key bracket in place with the screw removed in Step D above.



i. Reinsert the receiving frame into the SecureDock. Make sure to reconnect all connections and resecure the frame to the SecureDock using the screws you removed in Step B above.

j. Place the cover back onto the SecureDock with the CRU logo facing toward the front of the SecureDock and in the same position that you pulled it off in Step A above. Press down and then slide it forward into place.

h. Slide out the two large tabs on the rear of the SecureDock to secure the cover back in place.

2.2 Hard Drive Installation

a. Remove the carrier from the DataPort SecureDock with Internal Key.

b. Use a Phillips-head screwdriver to remove the screw securing the carrier cover to the back of the carrier, then slide the cover off.

c. Insert a SATA hard drive into the unified power and data connector inside the carrier.

d. Secure the hard drive to the carrier by using the mounting screws provided.

e. Attach the Temperature Control Cooling Sensor to the top of the hard drive with a piece of tape. The Temperature Control Cooling Sensor is the double-wired cord with a sensor thermistor at the end that extends out from the carrier PCB board.

f. Replace the cover and secure it with the screw you removed in Step B into the rear of the carrier.

g. Reinsert the carrier into the dock.

2.3 Operating your DataPort SecureDock with Internal Key

a. Connect the DataPort SecureDock with Internal Key to a computer using either the provided eSATA cable, a USB A-to-B cable, or a FireWire 800 cable (if supported).

b. Connect the DataPort SecureDock with Internal Key to a power outlet with the included AC Adapter.

c. If you have not already done so, slide the DataPort 10 carrier into the DataPort SecureDock with Internal Key.

d. Insert a DataPort Key into the key lock and turn it 90 degrees clockwise to power on the unit.

e. The unit is ready to use when both green LEDs are lit, showing that the drive is ready and encryption is activated.

The DataPort SecureDock with Internal Key uses a Security Key that is internally connected to the DataPort 10, although the internal Security Key can be overridden by a Security Key inserted into the Mini-USB Security Key Port on the face of the receiving frame. When a hard drive is first used with the DataPort SecureDock with Internal Key it will show up as a blank, unallocated drive. In order to encrypt the hard drive it must be initialized and formatted. **Note that formatting a drive will erase all data on the drive, so be sure to back up your data before beginning this operation**. See Section 3 for instructions on how to format the drive with Mac or Windows operating systems.

2.4 Safe Carrier Removal

a. Shut down the computer or properly dismount the drive from the system. See Section 3 for instructions on how to properly dismount the drive from Mac or Windows systems.

b. Use the DataPort Key to turn the keylock 90 degrees counterclockwise to unlock and power off the unit.

c. Pull the carrier by the handle towards you to remove the carrier.

2.5 Other Configuration Options

2.5.1 External Security Key Override

The DataPort 10 Secure supports external key connectivity. A Security Key plugged into the Mini-USB Security Key Port has a higher priority than the internal Security Key and will override the internal Security Key when the unit is powered up.

2.5.2 Changing the Internal Security Key

NOTE: Changing the Security Key will require the hard drive to be reformatted if the new key's encryption code is different than the original key.

Reformatting a drive will erase <u>all</u> data on the drive, so be sure to back up your data before beginning this operation. See Section 3 for instructions on how to format the drive with Mac or Windows operating systems. To replace the Security Key, follow these directions.

a. Remove the Receiving Frame

i. Remove the carrier if it is present and unplug all cables from the rear of the SecureDock chassis.

ii. Push the two tabs inward on each side of the rear of the SecureDock.

iii. Slide the cover backwards off the unit about an inch and a half until it stops. Then tilt it upward and pull it up and off of the SecureDock chassis. Set the cover aside.

iv. Unplug the unified power and data SATA connector from the rear of the receiving frame.

v. Disconnect the green and blue-wired fan alarm connector from the yellow-wired connector.

vi. Use a screwdriver to unscrew the receiving frame and remove it from the chassis.

b. Replace the Security Key

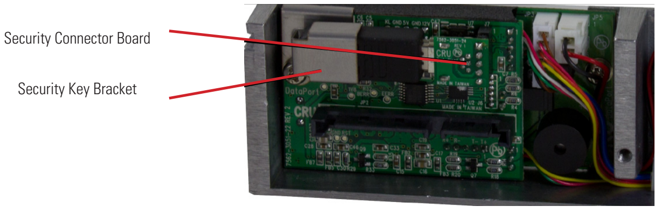
i. Remove the screw holding the Security Key bracket in place from the rear of the receiving frame.

ii. Slide the Security Key connector board off the rear of the receiving frame.

iii. Remove the old Security Key and replace it with the new Security Key.

iv. Slide the Security Key connector board back into place.

v. Fasten the Security Key bracket in place with the screw you removed in the first step of this subsection.



c. Replace the Receiving Frame

i. Reinstall the DataPort 10 receiving frame into the SecureDock chassis using the screws you removed when uninstalling it.

ii. Reconnect the green and blue-wired fan alarm connector to the yellow-wired connector.

iii. Reconnect the unified power and data SATA connector to the rear of the receiving frame.

iv. Replace the cover with the CRU DataPort logo facing towards the front of the chassis. Place the cover onto the chassis so that there is about an inch and a half gap between the logo and the front of the chassis. Then slide the cover closed.

v. Pull the two tabs on each side of the rear of the SecureDock outward to secure the cover.

3. Usage with Mac and Windows Operating Systems

3.1 Usage with Mac OS X

3.1.1 Compatibility

The DataPort SecureDock with Internal Key supports 2.5" and 3.5" SATA hard drives.

3.1.2 Formatting a Drive

To format, use Mac OS X's Disk Utility (found in the applications folder). The DataPort SecureDock with Internal Key must have been powered on with the Security Key present and both the Power and Encryption Ready LEDs must be lit. See Section 2.3 for instructions on how to do so.

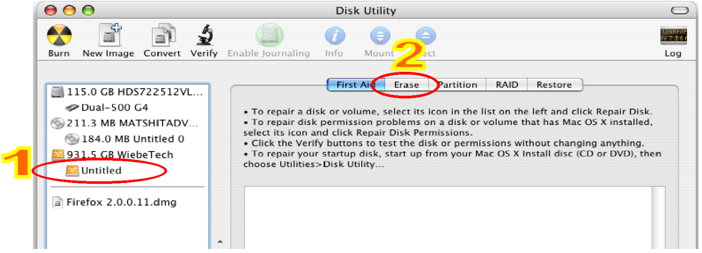
a. Click on the drive in the window to the left (see picture below).

b. Click the Erase tab in the window to the right (see picture below).

c. Select the format type. Most users prefer Mac OS Extended with Journaling (HFS+), which is required for compatibility with Time Machine (OS 10.5 or newer). If you need to use your DataPort SecureDock with Internal Key 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.

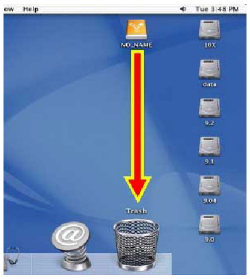
3.1.3 Mounting and Unmounting Volumes



• To repair a disk or volume, select its icon in the list on the left and click Repair Disk.
• To repair disk permission problems on a disk or volume that has Mac OS X installed, select its icon and click Repair Disk Permissions.
• Click the Verify buttons to test the disk or permissions without changing anything.
• To repair your startup disk, start up from your Mac OS X Install disc (CD or DVD), then choose Utilities>Disk Utility...

If the hard drive installed in the DataPort SecureDock with Internal Key was previously formatted with the correct Security Key inserted into the Mini-USB Security Key Port on the face of the receiving frame, then you can begin using the volume right away. If the drive is unformatted, a message will appear on the desktop saying that the disk is unreadable. You can use OS X's Disk Utility to easily format the drive (see section above).

Unmount the volume before powering down the unit by dragging the volume's icon to the trash bin, or by selecting the volume then pressing Command-E. Disconnecting the unit without first unmounting the volume can result in data loss.



3.1.4 Creating a Boot Drive

To activate this feature, you must first install OS X on the hard drive in your carrier. The easiest way to do this is to clone an existing system drive using a utility such as Carbon Copy Cloner or Super Duper. Next, go to System Preferences --> Startup Disk. A window will list the available bootable volumes. Select the volume from which you wish to boot. Another method is to hold down the Option key during boot up. A screen should appear that allows you to select the volume you wish to use. This is useful if you wish to boot from your DataPort SecureDock with Internal Key hard drive only some of the time.

3.2 Usage with Windows Operating Systems

3.2.1 Compatibility

The DataPort SecureDock with Internal Key supports 2.5" and 3.5" SATA hard drives.

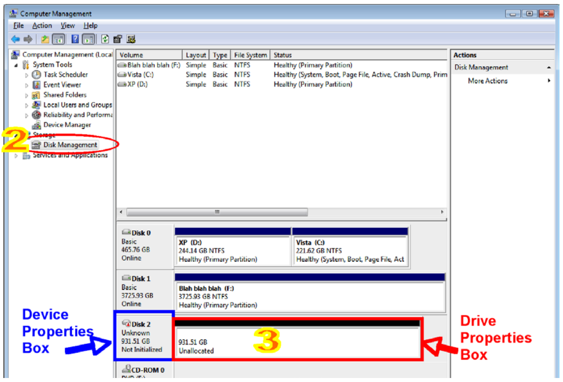
3.2.2 Formatting a Drive

To format, use the Disk Management utility. The DataPort SecureDock with Internal Key must have been powered on with the Security Key present and both the Power and Encryption Ready LEDs must be lit. See Section 2.3 for instructions on how to do so.

a. Right-click on My Computer, then select Manage. The Computer Management window will open.

b. In the left pane of this window, left-click on Disk Management.

c. The drive should appear in the list of Disks in the lower middle/right pane (see picture below). You may need to scroll down to see it. If the drive is already formatted, you can identify it easily by its volume name. If it's unformatted, the Drive Properties Box will say "Unallocated" and you'll need to initialize the disk before formatting it. Initialize the disk by right-clicking the Device Properties Box and selecting Initialize Disk.



Volume	Layout	Type	File System	Status
Blah blah blah (F:)	Simple	Basic	NTFS	Healthy (Primary Partition)
Vista (C:)	Simple	Basic	NTFS	Healthy (System, Boot, Page File, Active, Crash Dump, Prim
XP (D:)	Simple	Basic	NTFS	Healthy (Primary Partition)

Disk 0
Basic
465.76 GB
Online

XP (D:)
244.14 GB NTFS
Healthy (Primary Partition)

Vista (C:)
221.62 GB NTFS
Healthy (System, Boot, Page File, Act

Disk 1
Basic
3725.93 GB
Online

Blah blah blah (F:)
3725.93 GB NTFS
Healthy (Primary Partition)

Disk 2
Unknown
931.51 GB
Not Initialized

931.51 GB
Unallocated

CD-ROM 0

d. To format the drive, right-click the Drive Properties Box and select Format.

e. If you are prompted to select a partition type, select MBR for volumes 2TB or smaller, or GPT for volumes larger than 2TB.

NOTE: Windows XP does not support GPT or volumes larger than 2TB.

f. Click through several more windows, leaving the default settings, until you see a window that allows selection of a file system. Choose NTFS and enter a name for the new volume. Be sure to check the box labeled "Perform a quick format" unless you want to completely erase any data on the drive and have time to wait. A quick format should take less than a minute, while standard formatting may take several hours.

g. Click "Next" and then "Finish" to start the format process. When the format is complete, the Drive Properties Box will update to show the new volume name. The new volume can now be found by double-clicking on the "My Computer" icon on the desktop.

3.2.3 Mounting and Unmounting Volumes

If the hard drive installed in the DataPort SecureDock with Internal Key was previously formatted with the correct Security Key in place, then when the DataPort SecureDock with Internal Key is properly connected and turned on, a window may open to allow you access to the volume. If no window appears, you can find the volume by double-clicking the "My Computer" icon.

Unmount the DataPort SecureDock with Internal Key before powering it down by single-clicking the green arrow icon on the task bar (in Windows XP) or the USB plug icon with the green checkmark on the taskbar (Windows Vista and Windows 7), then selecting "Safely remove…." Windows will indicate when it is safe to disconnect the DataPort SecureDock with Internal Key. Disconnecting the unit without first ejecting it can result in data loss.

4. Encryption

- The DataPort SecureDock with Internal Key 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 DataPort SecureDock with Internal Key for the data to be decrypted on the drive. If the key is externally connected to the Mini-USB Security Key Port and is not internally installed, then once it has been accepted, it may be removed and stored 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.

5. Frequently Asked Questions (FAQ)

Q: What do the LED lights indicate?

A:

#	LED Name	Color	State	Description
1	Drive Activity	Amber	Intermittent	Flashes when the drive is being accessed.
2	Power	Green	Solid	Unit is powered on.
			Flashing	Fan Failure.
3	Key Error	Red	Solid	Encryption engine error. Contact Technical Support.
			Flashing	The Security Key is not present or is not functioning.
4	Encryption	Green	Solid	The Security Key is present and encryption is enabled.

Q: Why can't I access my data when I turn on my unit?

A: If you have data on the drive, don't panic! Barring the failure of the hard drive your data is still intact, but is not reachable because the correct Security Key is not installed, or the drive was not formatted within this unit using the unit's internal Security Key.

If you are using an external Security Key, make sure you are using a drive that was formatted while that particular Security Key was installed in the mini-USB Security Key port on the front of the carrier. If the unit is on, power it off and then insert the correct Security Key into the Security Key port. Then turn your unit back on. When both green LEDs are lit, showing that the drive is ready and encrypted, you should then be able to access your data. You can then remove the Security Key and store it in a safe location.

If you do not have an external Security Key installed, make sure you are using a hard drive that has been formatted within this unit. If it has, please contact Technical Support. If the drive was not formatted within this unit, determine if the drive was formatted with a separate Security Key or was formatted without a Security Key. If it was formatted with a separate Security Key, refer to the previous paragraph. If it was formatted without a Security Key, you will need to make a backup copy of your data and format the drive using the correct Security Key. See Section 3 for instructions on how to format the drive with Mac or Windows operating systems.

Q: I turned my unit off and back on and now I cannot access my data. Why?

A: You should only have this problem if you are using an external Security Key to override the internal Security Key. If you are not using an external Security Key and are experiencing this issue, please contact Technical Support.

Cycling power on the unit will require you to reinsert the external Security Key into the Mini-USB Security Key port before turning the unit back on, even if you have not turned your computer off. If the unit is on, power it off and insert the correct Security Key into the Mini-USB Security Key port on the front of the carrier. Then turn your unit back on. When both green LEDs are lit, showing that the drive is ready and encrypted, you should then be able to access your data. You can then remove the Security Key and store it in a safe location.

Q: Why can't I use another device through the Mini-USB port on the front of the DataPort SecureDock carrier?

A: This port is used by an external Security Key only. Inserting an external Security Key into the mini-USB port will override the encryption of the internal key and the unit will use the external encryption key to access the data on your hard drive. It does not pass data to the drive itself.

Under no circumstances should you insert anything other than a Security Key into the Mini-USB Security Key Port. Though it is mechanically identical to the standard Mini-USB port, inserting a Mini-USB cable or other device into the Mini-USB Security Key Port on the carrier can cause internal damage and potentially lead to loss of data.

Likewise, inserting the Security Keys into any other Mini-USB port will damage the keys and render them useless. Please only use the Security Keys in DataPort Secure products.

If you have already tried to use another device through this port or have inserted the Security Key into another device's Mini-USB port, first check to see if your Security Key still works in your unit. If it does not, please contact Technical Support.

Contacting Technical Support

Still need help? Please contact our Technical Support team through CRU-DataPort.com. Or call us toll free at (800) 260-9800, or directly at (360) 816-1772.

6. Technical Specifications

Product Name	DataPort SecureDock with Internal Key
Interface Types & Speeds	• eSATA: up to 150 Mbps • USB 2.0: up to 480 Mbps • FireWire 800: up to 786 Mbps
Compatibility	• 2.5" SATA Hard Drives • 3.5" SATA Hard Drives
Data Connectors	One (1) eSATA connector One (1) USB 2.0 connector One (1) FireWire 800 connector (Optional)
Encryption/ Decryption	128-bit AES (Advanced Encryption Standard) 256-bit AES (Advanced Encryption Standard)
Connector Insertion Rating	25,000+ Carrier-to-Frame
Operating System Requirements	• Windows 7, Vista, or XP • Mac OS X • Linux distributions that support SATA, USB, or FireWire 800
Compliance	EMI Standard: FCC Part 15 Class B, CE EMC Standard: EN55022, EN55024 FIPS: FIPS 140-2, FIPS PUB 197
Shipping Weights	3.00 pounds (includes accessories)
Dimensions	5.75" x 7.87" x 1.61" (146mm x 200mm x 41mm)
Warranty	We don't expect anything to go wrong with your CRU product. But if it does, Tech Support is standing by and ready to help. Contact us at http://www.cru-dataport.com/support. We also offer phone support at (800) 260-9800.

Product Warranty
CRU-DataPort (CRU) warrants this product to be free of significant defects in material and workmanship for a period of three years from the original date of purchase. CRU's warranty is nontransferable and is limited to the original purchaser.

Limitation of Liability
The warranties set forth in this agreement replace all other warranties. CRU expressly disclaims all other warranties, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose and non-infringement of third-party rights with respect to the documentation and hardware. No CRU dealer, agent, or employee is authorized to make any modification, extension, or addition to this warranty. In no event will CRU or its suppliers be liable for any costs of procurement of substitute products or services, lost profits, loss of information or data, computer malfunction, or any other special, indirect, consequential, or incidental damages arising in any way out of the sale of, use of, or inability to use any CRU product or service, even if CRU has been advised of the possibility of such damages. In no case shall CRU's liability exceed the actual money paid for the products at issue. CRU reserves the right to make modifications and additions to this product without notice or taking on additional liability.

FCC Compliance Statement: "This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation."

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a home or commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

In the event that you experience Radio Frequency Interference, you should take the following steps to resolve the problem:

1) Ensure that the case of your attached drive is grounded.
2) Use a data cable with RFI reducing ferrites on each end.
3) Use a power supply with an RFI reducing ferrite approximately 5 inches from the DC plug.
4) Reorient or relocate the receiving antenna.

FC Tested to comply with FCC standards

FOR HOME OR OFFICE USE