

| | |
|-------------------------------|---|
| Product Names | DataPort 10 Secure with Internal Key |
| Interface Types & Speeds | SATA: up to 150 Mbps |
| Compatibility | 2.5" SATA Hard Drives 3.5" SATA Hard Drives |
| Data Connectors | One (1) SATA connector |
| Encryption/Decryption | 256-bit AES (Advanced Encryption Standard) |
| Connector Insertion Rating | 25,000+ Carrier-to-Frame |
| Operating System Requirements | <ul style="list-style-type: none"> 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 Weight | 3.00 pounds (includes accessories) |
| Product Dimensions | 5.75" x 7.87" x 1.61" (146mm x 200mm x 41mm) |
| Warranty | 3-year limited warranty. See warranty statement for details and limitations. We don't want anything to go wrong with your CRU-DataPort product. But if it does, Tech Support is standing by and ready to help. Contact us at http://www.cru-dataport.com/technical-support/customer-technical-support.php |

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.



DataPort® 10 Secure with Internal Key Quick Start Guide

Visit <http://www.cru-dataport.com/technical-support/product-manuals.php> to download a copy of the complete User Manual. Additional product information can also be found at <http://www.cru-dataport.com> and <http://www.wiebetech.com>. WiebeTech is a brand of CRU.



Models Covered:

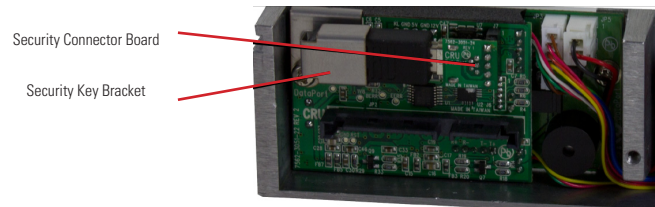
- DataPort 10 Secure with AES 128 (Internal Key Version)
- DataPort 10 Secure with AES 256 (Internal Key Version)

1. Installation Steps

1.1 Security Key Installation

The Security Key Installation steps only need to be followed if you have purchased a version of the DataPort 10 Secure that does not include an internal Security Key.

- a. Remove the DataPort 10 receiving frame from the computer chassis.
- b. Remove the screw holding the Security Key bracket in place from the rear of the receiving frame.
- c. Slide the Security Key connector board off of the rear of the receiving frame.
- d. Insert a Security Key onto the connector board.
- e. Slide the connector board back into place.
- f. Fasten the Security Key bracket in place with the screw removed in Step A above.
- g. Reinstall the DataPort 10 receiving frame into the computer chassis.



The DataPort 10 Secure with Internal Key uses a Security Key that is internally connected to the DataPort 10 encryption engine, 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 10 Secure it will show up as a blank, unallocated drive and you'll need to format the drive before you can use it. **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 of the DataPort 10 Secure with Internal Key User Manual on our website <http://www.cru-dataport.com> for instructions on how to format the drive with Mac or Windows operating systems.

1.2 Receiving Frame Installation

- Slide the receiving frame into an open 5.25" bay.
- Secure the receiving frame to the chassis with the four screws provided.
- Attach the SATA data cable to the rear of the receiving frame and the other end to the corresponding SATA port on the computer's motherboard.
- Attach the SATA power connectors to the rear of the receiving frame. If no SATA power connectors are available, attach the included Molex-to-SATA adapter cable to a Molex power plug. Then plug the SATA end of the adapter cable into the rear of the receiving frame.

1.3 Hard Drive Installation

- If the carrier is bundled with a frame, use the included set of DataPort Keys to unlock the carrier and then remove it from the frame.
- Use a Phillips-head screwdriver to remove the screw securing the carrier cover to the back of the carrier, then slide the cover off.
- Insert a SATA hard drive into the unified power and data connector inside the carrier.
- Secure the hard drive to the carrier by using the mounting screws provided.
- Attach the Temperature Control Cooling Sensor to the top of the hard drive with a piece of tape.
- Replace the cover and secure it with the screw you removed in Step B into the rear of the carrier.
- Reinsert the carrier into the frame.

1.4 Operating your DataPort 10 Secure

- If you have not already done so, slide the DataPort 10 Secure carrier into an open DataPort 10 frame (may be sold separately) on your computer.
- Insert a DataPort Key into the key lock and turn it 90 degrees clockwise to power on the unit.
- The unit is ready to use when both green LEDs are lit, showing that the drive is ready and encryption is activated.

1.5 Safe Carrier Removal

- Turn off the computer or properly dismount the drive from the system. See Section 3 of the DataPort 10 Secure with Internal Key User Manual on our website <http://www.cru-dataport.com> for instructions on how to properly dismount the drive on a Windows system.
- Use the DataPort Key to turn the keylock 90 degrees counter-clockwise to unlock and power off the unit.
- Pull the carrier by the handle towards you to remove the carrier.

2. Encryption

- The DataPort 10 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 DataPort 10 Secure for the data to be decrypted on the drive. If the key is externally connected to the Mini-USB Security Key Port and is not internally installed, then once it has been accepted, it may be removed and stored 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.