CRU

Protecting
Your Digital
Assets™

Product Name	DataHarbor with DataPort 10 Secure Bay
Interface Types and Speeds	• Ethernet: up to 1 Gbps • eSATA: up to 3 Gbps • USB 3.0: up to 5 Gbps • USB 2.0: up to 480 Mbps • Serial RS-232: up to 11520 bit/s
Drive Types Supported	3.5" SATA* Hard Drives *SATA III Drives must be jumpered to run at 3.0 Gbps transfer speed
Connectors	Two (2) Gigabit Ethernet connectors Two (2) eSATA connectors Two (2) USB 3.0 connectors Four (4) USB 2.0 connectors (3 rear, 1 front) One (1) Serial connector One (1) PS/2 connector One (1) VGA connector One (1) Speaker connector One (1) Line In connector One (1) Microphone connector
Server Operating System	Windows Storage Server 2008 R2 Essentials
Supported Client Operating Systems	Windows XP SP3, Vista SP2, 7, or 8.1 Mac OS 10.5 Leopard or Mac OS 10.6 Snow Leopard* *Client Backups must be manually configured
Compliance	EMI Standard: FCC Part 15 Class B, CE EMC Standard: EN55022, EN55024
Shipping Weight	24 pounds (includes accessories)
Product Dimensions	16.14" x 1.72" x 14.17" (410mm x 44mm x 360mm)
Technical Support	Please contact your IT administrator if you have questions about Microsoft Windows Storage Server 2008 R2 Essentials, or visit http://technet.microsoft.com/en-us/library/ff953176.aspx Contact us at www..com/support for support related to your DataHarbor hardware. We also offer phone support at (800) 260-9800 or (360)-816-1800.

Product Warranty
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 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 OFFICE OR COMMERCIAL USE

CRU

Protecting
Your Digital
Assets™

CRU® DataHarbor®
with DataPort 10 Secure Bay
Daily Operations Guide

NOTE: DataHarbor Setup and other tasks normally performed by the IT Administrator are addressed in the DataHarbor IT Administrator's System Manual, which can be found on www.cru-inc.com/support. These include:

- Managing the backup schedule
- Managing Windows updates
- Remote Web Access
- Adding user accounts
- Restoring client computers
- Restoring the server

1 Managing the Daily Backup

CRU strongly recommends you maintain an offsite daily backup by performing these steps at the beginning or end of each business day, depending on your situation.

a. While leaving the DataHarbor on, power off the removable DataPort 10 by turning its latch 90 degrees counterclockwise.

b. The RAID alarm will sound. Press the **Enter** button to mute it.

c. Pull the removable drive from the unit and replace it with a different removable drive. This will serve as your offsite backup drive.

d. Turn the latch 90 degrees clockwise to power the new drive.

e. Wait a few seconds and the LCD will ask if you would like to add a new drive. Press the **Enter** button. The RAID will now automatically begin rebuilding.

f. Take the offsite backup drive and store it in a **separate geographic location** from the DataHarbor and any Security Keys. This will protect the data in case of fire or other catastrophe at the site of the DataHarbor.

NOTE: Since a Security Key is needed to access the data on the offsite backup drive, storing the drive separately from the keys ensures that in the event the offsite backup drive is lost or stolen, the data inside will remain inaccessible to the thief.

2 Using the Launchpad

To access the Launchpad, open the **Start Menu** and navigate to **All Programs → Windows Storage Server 2008 R2** and click on **Windows Storage Server 2011 R2 Launchpad**. Sign in with your user name and password and then click on the → icon.

2.1 Backup

The Backup button opens the Backup Properties window. Backups happen automatically at the time of day set by your server administrator, so manual backups are only necessary in special circumstances.

2.1.1 Backup Status

a. Click on the **Start backup** button to manually begin a backup.

b. Name the backup and click **OK**.

The computer will begin backing up to the server. To stop the backup, click on the **Stop backup** button.

2.1.2 Power Management

Click on the check box next to "Automatically wake this computer up from sleep or hibernation to run a scheduled backup" in order to enable this feature. It is useful to ensure that laptops or computers that are set to go to sleep are successfully backed up. Uncheck the check box in order to disable it.

2.2 Remote Web Access

The following instructions require your administrator to have enabled Remote Web Access for your user account. Remote Web Access allows you to use a web browser to easily access the Dashboard, shared files, and other computers on your network when you are away from the office. When you connect to computers on your network, you can access their desktops as if you were sitting in front of them.

a. Click on the **Remote Web Access** button in the Launchpad.

b. Your browser will open a window to a login and password page. Enter your username and password and click on the → icon.

A page will open where all the shared data and computers your user account has permissions to use will be available to access.

2.2.1 Connecting to a Remote Computer

If you have the appropriate permissions, you can remotely connect to other computers on the server network. This feature requires Internet Explorer.

c. Use **Remote Web Access** to open your user account's Remote Web Access home page (see Section 2.2).

d. In the listing of computers to the left, click on the **Connect** button on the computer you wish to connect to.

e. If this is the first time you are remotely connecting to a computer, a RemoteApp prompt will open asking you to allow remote connections from the server. Click on the **Connect** button to do so.

f. A Windows Security window will open. Enter the computer's username and password to connect to it and click **OK**.

g. A Remote Desktop Connection window will open with the remote computer's login screen showing. Enter the appropriate login credentials and click **Enter.**

You have now accessed the remote computer's desktop.

2.3 Shared Folders

The Shared Folders button opens an Explorer window that allows you to access all the shared data on the server that your user account has permissions to use.

2.4 Dashboard

The Dashboard button opens the Dashboard application where you can manage the DataHarbor's operating system: Windows Storage Server 2008 R2 Essentials. You will be able to add or remove user accounts, add or remove shared folders, set shared folder access, among other features. **Use of this application requires the server's local administrator account password. Dashboard is not available for Mac OS.**