Using RDX QuikStation® and QuikStor® with Acronis® Cyber Backup

INTEGRATION BRIEF

Acronis Cyber Backup, in tandem with RDX Removable Storage, provides a solution for small and medium businesses that includes options for Bare Metal Restores. In addition, the inclusion of rdxLOCK RansomBlock software helps shield your data from Ransomware attacks.

Overland-Tandberg and Acronis have combined hardware and software to provide small and medium businesses with the best of class data backup scenarios. This guide explains how to:

* Configure your RDX to work with Acronis Cyber Backup.
* Perform a Bare Metal Restore (BMR) including how to boot from RDX for a BMR.
* Use RDX PowerEncrypt and RDX drive Auto-Authentication for a BMR.
* Use rdxLOCK RansomBlock software to configure your RDX volume to block Ransomware attacks.

Overland-Tandberg RDX QuikStor drives and QuikStation appliances

Overland-Tandberg's RDX QuikStor removable disk storage system offers rugged, reliable and convenient storage for backup, archive, data interchange and disaster recovery. RDX QuikStor is available as an external device with USB 3.0 interface and, attached to a desktop, laptop or server, is ready for immediate use. RDX QuikStor also comes as an internal drive with either a USB 3.0 or SATA III interface.

The RDX QuikStation iSCSI network-attached removable disk appliance is designed to provide a flexible platform for data protection and off-site disaster recovery for either physical or virtual SMB and SME environments. The RDX QuikStation family offers two models with either four or eight integrated RDX drives to fit varying capacity and feature requirements.

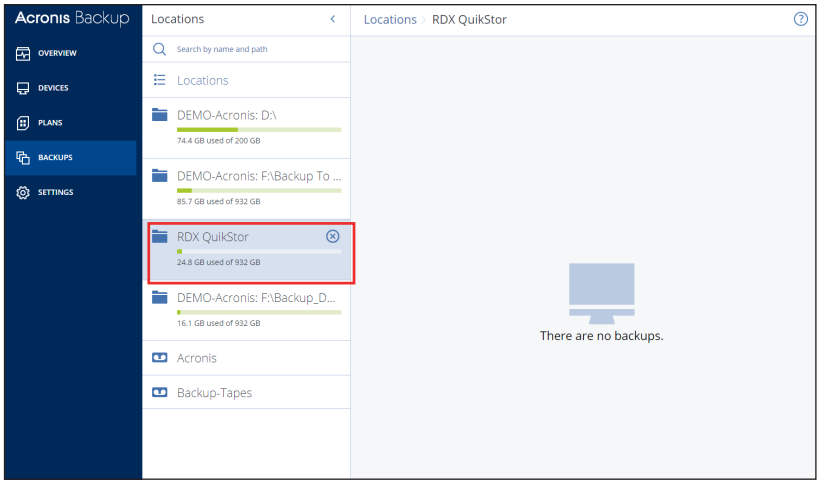
Acronis Cyber Backup Software

Acronis Cyber Backup keeps your business operations running by ensuring your data is always available. It reliably protects any data source on 21 platforms–virtual, physical, cloud and mobile–regardless of the size or location of the data. As your data needs grow or your infrastructure evolves, keeping your company data secured is easy with flexible, scalable storage and simple backup administration.

Using RDX with Acronis Cyber Backup

With Acronis Cyber Backup installed, you can make an RDX QuikStation or RDX QuikStor the backup target for an easy backup solution.

NOTE: For best results, install RDX Manager before continuing. The file is available at: (ftp://ftp1.overlandtandberg.com/rdx/RDX Manager/Windows/).*



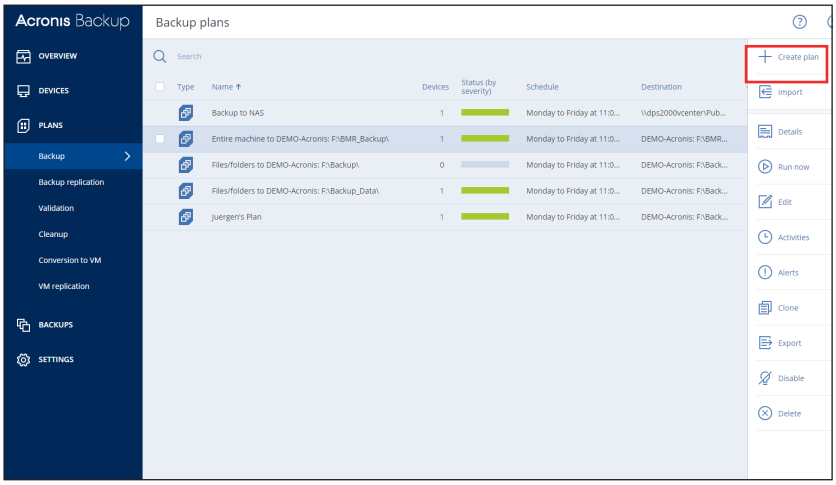
At the Acronis Cyber Backup Management Console:

On the left, click the **DEVICES** option in the left menu bar.

Under **All devices**, check the RDX.

On the left, click **BACKUPS**.

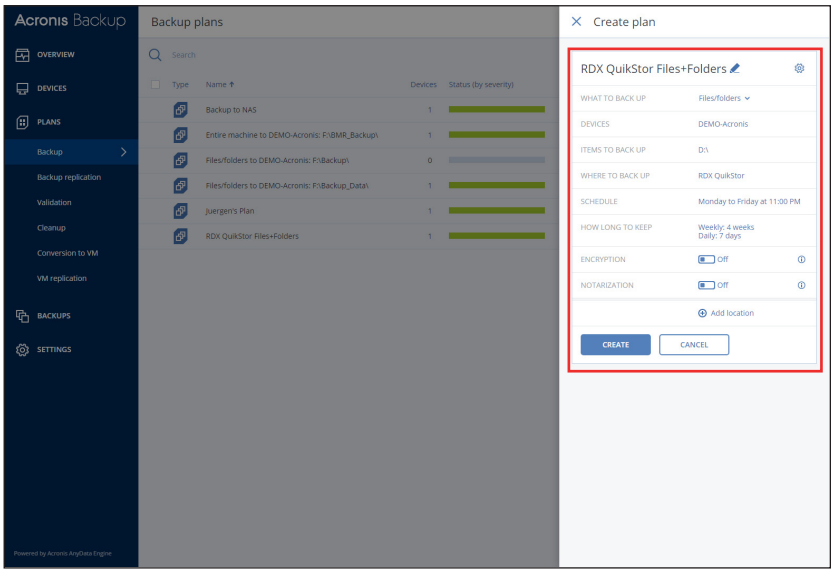
Select the RDX from **Locations** as your backup target device.



On the left, click **PLANS > Backup**.

On the right, click **+Create plan**.

* Safari browsers might not be able to start this site. Please try an alternative browser.

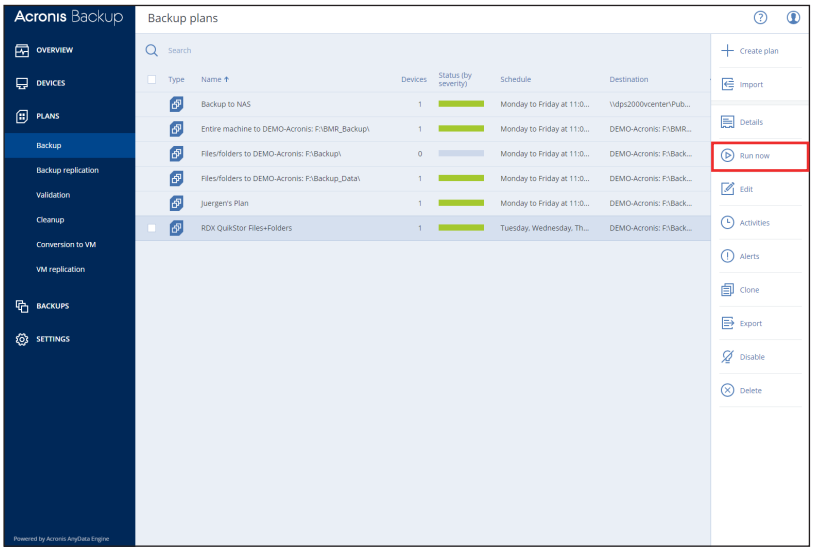


Configure the Backup plan:

1. Enter a unique plan name.
2. Select **WHAT TO BACK UP** from the drop-down list.

   Select **Entire machine** for a BMR.
3. Click DEVICES, click **+Add**, check the computer, and click **ADD**.
4. At the **Devices** list, select the computer being backed up and click **DONE**.
5. Select the **ITEMS TO BACK UP**.

   Double-click the drive label to select specific files and folders.
6. For **WHERE TO BACK UP**, select the RDX.
7. As needed, configure any of the remaining options.
8. When done, click **CREATE**.

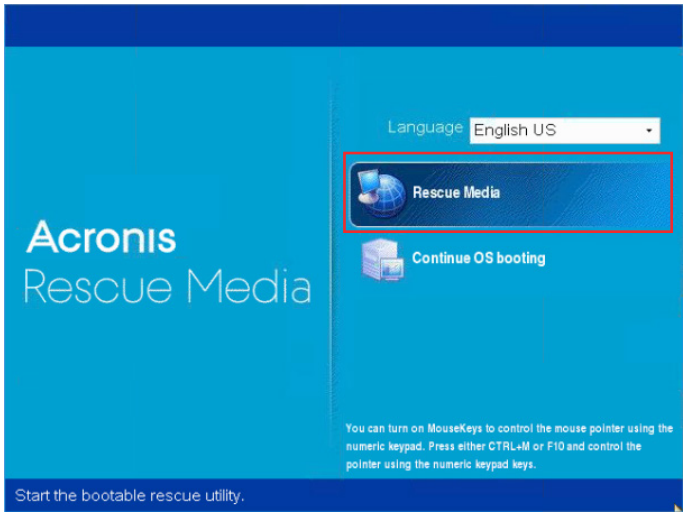


To manually run a backup right now, select the plan and click **Run now** on the right.

Boot from RDX for Bare Metal Restore

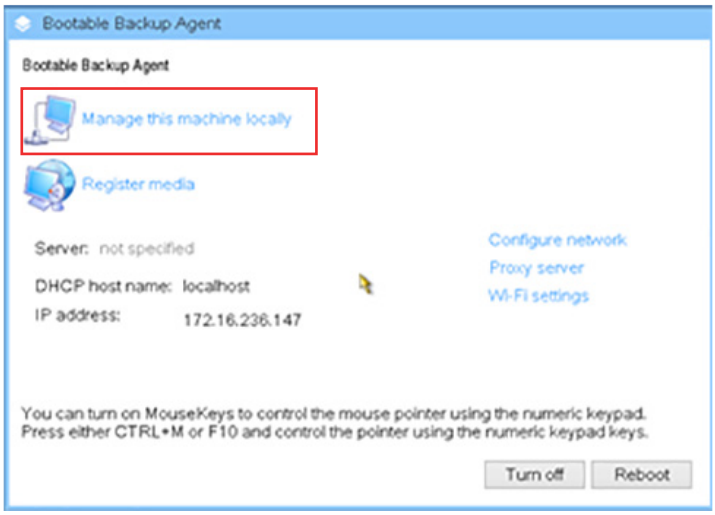
NOTE: Depending on your backup application and BMR environment, Acronis can mount an iSCSI target (such as a QuikStation 8) for a full BMR.

To restore an entire machine or move to new computer:

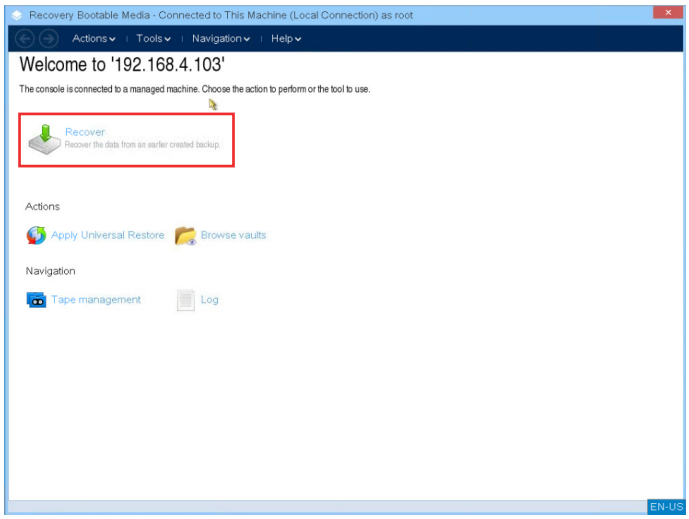


With the RDX attached and media with the **Entire machine** backup inserted, use the USB with the Acronis Emergency Recovery files to boot the machine.

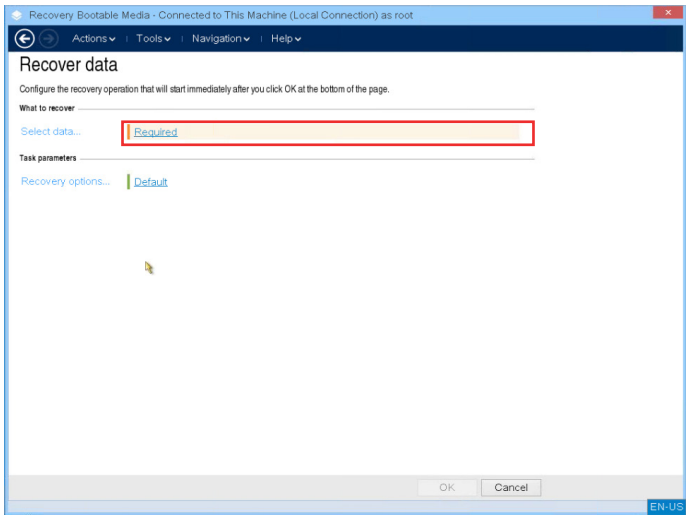
Double-click **Rescue Media**.



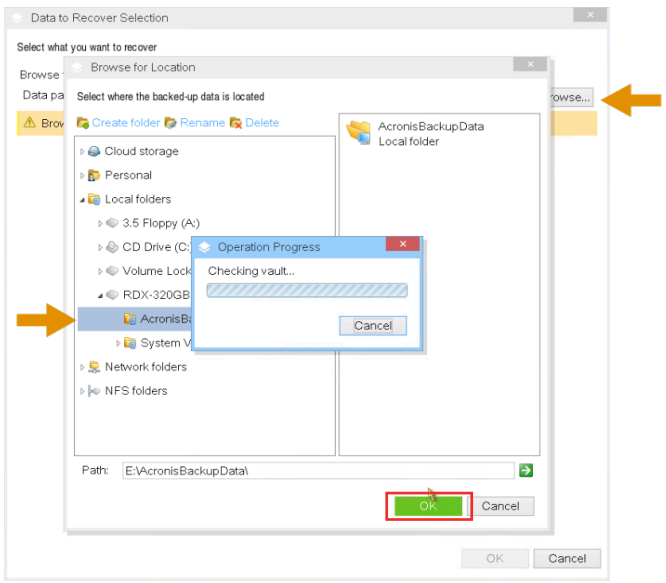
Click **Manage this machine locally**.



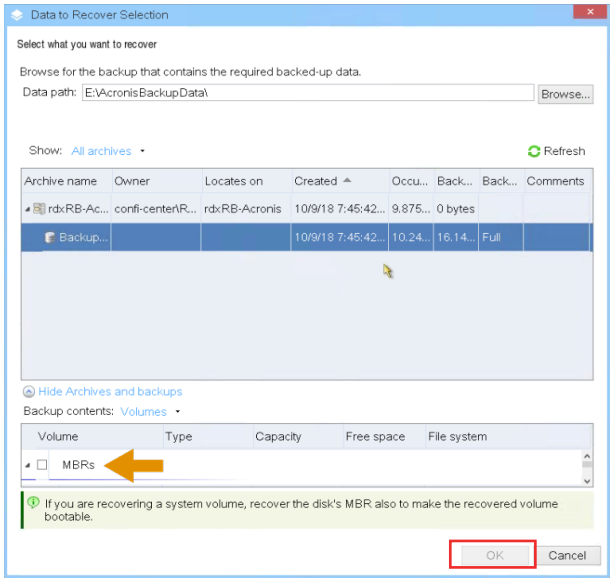
At the Welcome screen, click **Recover**.



At the **Recover data** screen, to the right of **Select data**, click **Required**.

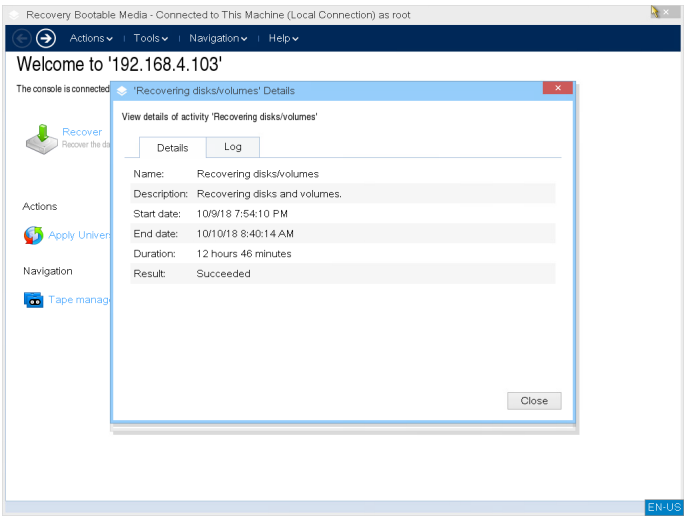


At the **Data to Recover Selection** pop-up, click **Browse**, select the backup on the RDX media, and click **OK**.



Select all the volumes of the backup and click **OK**.

At the **Recover data** screen, click **OK** to start the recovery.



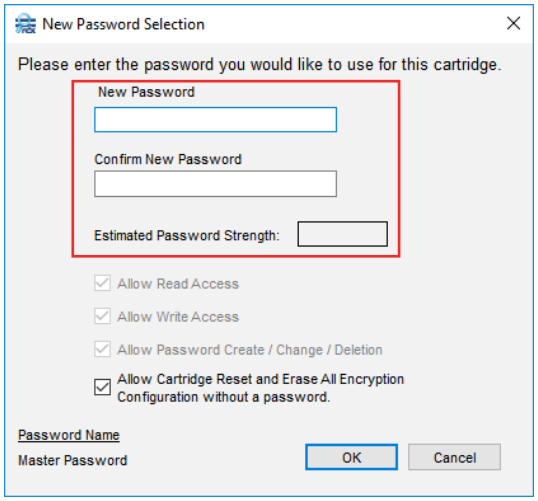
The recovery **Details** screen shows the recovery process.

Use RDX Drive PowerEncrypt and Auto-Authentication for BMR

We provide hardware encryption through RDX PowerEncrypt, currently available in the internal RDX QuikStor drive with a SATA III interface running firmware 0253 or later. RDX Manager software offers full management and control of this feature. Please refer to our PowerEncrypt web page for more information on this feature.

At the default Encryption tab, click **Enable Cartridge Encryption/ Password Protection**.

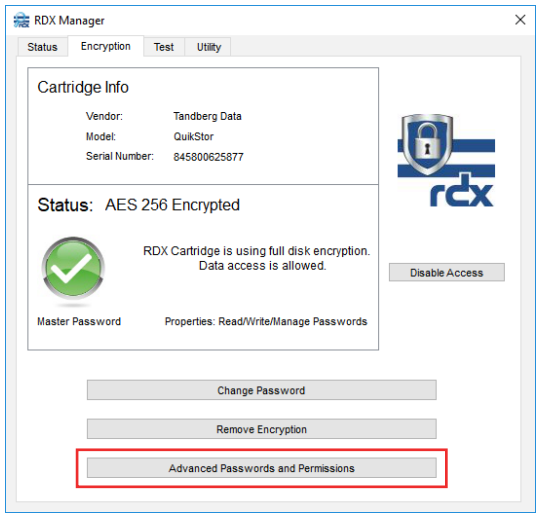
At the Protection Type Selection dialog box, select **Full Disk AES 256 XTS Encryption** and click **OK**.



At the New Password Selection dialog, enter and confirm a strong password that has an estimated password strength of **Very Good**.

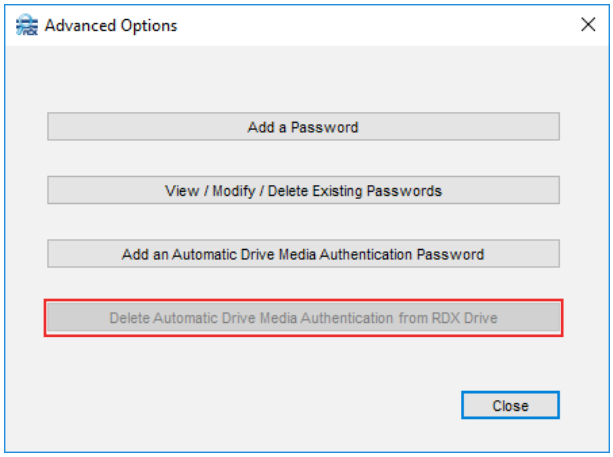
Leave the default setting of **Allow Cartridge Reset and Erase All Encryption Configuration without a password** checked.

Click **OK**.



At the Cartridge Format Selection dialog box, select either **NFTS** or **exFAT**, and click **OK**.

When returned to the Encryption tab, click **Advanced Passwords and Permissions**.



At the Advanced Options dialog, click **Add Drive's Automatic Authentication Password** for the cartridge and click **OK**.

At the auto-authentication confirmation dialog click **OK**.

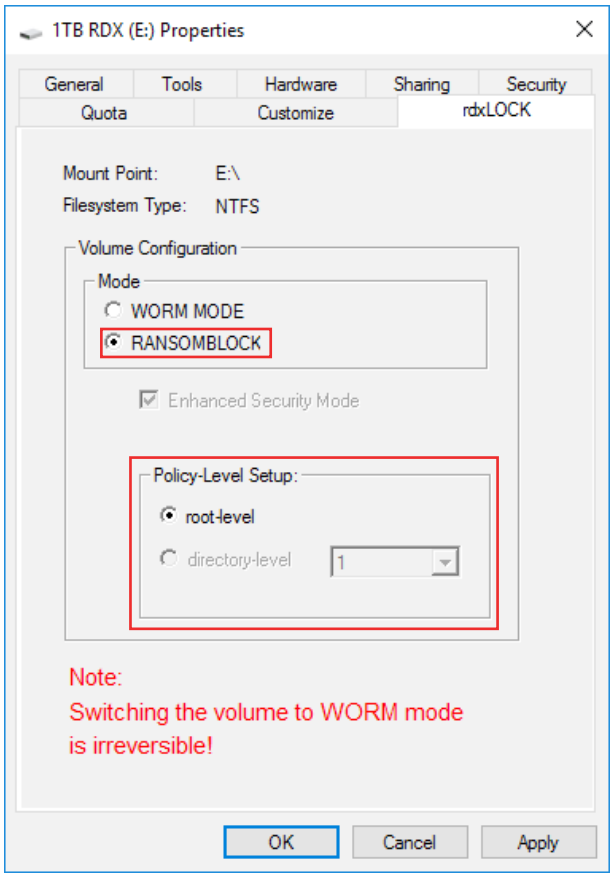
Click **Close** to activate the configuration.

Block Ransomware with rdxLOCK RansomBlock

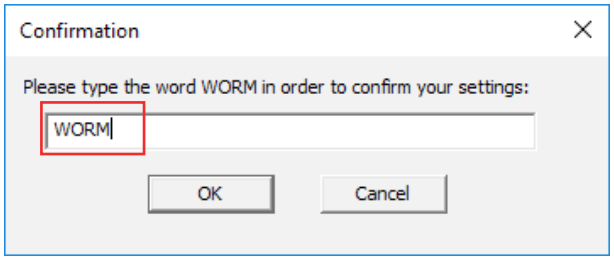
The rdxLOCK RansomBlock functionality sets all data on the RDX WORM media into a read-only mode. In addition, it allows write operations to RDX media for granted applications and processes similar to a personal Firewall. Therefore, backup applications are able to use RDX WORM media like a regular RDX backup target.

RansomBlock performs a validation check each time a write operation tries to access the RDX media. In case of a virus, ransomware attack, or unauthorised access, RansomBlock denies this operation and protects the data stored on RDX media from being infected.

To set up rdxLOCK RansomBlock:



1. Run the rdxLOCK Manager program as an administrator.
2. Right-click the appropriate volume and select **Properties**.
3. At the Properties dialog, select the **rdxLOCK** tab.
4. Select **RANSOMBLOCK** Volume Configuration mode.
5. Click **OK**.



At the Confirmation screen, type “WORM” (in all capital letters) and click **OK**.

NOTE: After confirming, the whole volume is ready for monitoring and controlling file system access using RansomBlock.

RDX PowerEncrypt with rdxLOCK RansomBlock

If you plan to use RDX PowerEncrypt with RansomBlock, you need to configure the hardware encryption first before you configure and use RansomBlock (2-Stage BMR).

First, using non-RansomBlock protected RDX media with rdxLOCK installed that has been stored at a secure location, do an initial restore. Then, do a second restore with the RansomBlock-protected RDX Media.