



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

Acronis Cyber Backup, in tandem with RDX Removable Storage, provides a solution for small and medium businesses that includes options for Bare Metal Restores.

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.

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: http://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.

Acronis Backup	Backup	plans					?
	Q Search	n					+ Create plan
	🗌 Туре	Name 🕈	Devices	Status (by severity)	Schedule	Destination	import
(T)	6	Backup to NAS	1	_	Monday to Friday at 11:0	\\dps2000vcenter\Pub	
E Pours	- 0	Entire machine to DEMO-Acronis: P\\BMR_Backup\	1		Monday to Friday at 11:0	DEMO-Acronis: F\/BMR	Details
Backup >	6	Files/folders to DEMO-Acronis: F:\Backup\	0	_	Monday to Friday at 11:0	DEMO-Acronis: F:\Back	Run now
Backup replication	6	Files/folders to DEMO-Acronis: F:\Backup_Data\	1	_	Monday to Friday at 11:0	DEMO-Acronis: F:\Back	The second
Validation	6	Juergen's Plan	1	_	Monday to Friday at 11:0	DEMO-Acronis: F:\Back	per cuit
Cleanup							Activities
Conversion to VM							() Alerts
VM replication							
							Clone
A conver							Export
201 serringus							🖉 Disable
							🛞 Delete

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.



Acronis Backup	Backup plans		× Create plan	
OVERVIEW	Q Search		RDX QuikStor Files+Folders	
	□ Type Name ↑	Devices Status (by severity)	WHAT TO BACK UP Files/folders ~	
# PLANS	Backup to NAS	1	DEVICES DEMO-Acronis	
Backup	Files/folders to DEMO-Acronis: F\Backup\		ITEMS TO BACK UP D:\	
Backup replication	Files/folders to DEMO-Acronis: FABackup_Data\	1	WHERE TO BACK UP RDX QuikStor	
Validation	🚱 Juergen's Plan	1	SCHEDULE Monday to Friday	st 11:00 PM
Cleanup	RDX QuikStor Files+Folders	1	HOW LONG TO KEEP Weekly: 4 weeks Daily: 7 days	
VM replication			ENCRYPTION Off	0
				0
Ц ^А ВАСКИРS			Add location	
SETTINGS			CREATE	
Powered by Acronis AnyOsta Engine				

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.

Acronis Backup	Backup plans	0
	Q Search	+ Create plan
	Type Name † Devices Status (by Schedule	Destination Import
II PLANS	Backup to NAS Monday to Priday at 11:0	\\dps2000vcenter\Pub
Backup	Entire machine to DEMO-Acronis: F\BMR_Backup\ Monday to Friday at 11:0	DEMO-Acronis: F\BMR
Backup replication	Files/folders to DEMO-Acronis: FilBackup\ 0 Monday to Filday at 11:0 Files/folders to DEMO-Acronis: FilBackup Data 1 Monday to Filday at 11:0	DEMO-Acronis: FABack
Validation	Juergen's Plan Monday to Friday at 11:0	DEMO-Acronis: P\Back
Cleanup	RDX QuikStor Files+Folders 1 Tuesday, Wednesday, Th	DEMO-Acronis: F\Back
Conversion to VM		() Alerts
VM replication		Clone
Васкирз		
SETTINGS		
		2 Disable
		O Delete
Powered by Acronis AnyData Engine		



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.

Manage this machine locally			
Register media			
Server: not specified		Configure net	work
OHCP host name: localhost	4	Proxy server	
P address: 172.16.236.147		TALL SCORES	
u can turn on MouseKeys to control th	te mouse point	er using the numeric l	veypad.

Click Manage this machine locally.



Recovery Bootable Media - Co	nnected to This Machine (Local Connection) as root	×
Actions 🗸 🕴 Tools 🗸	⊢ Navigation v ⊢ Help v	
Velcome to '192.168	.4.103'	
Recover Recover the data from an serier of	achine. Choose he action is perform or the tool is use.	
Actions		
D Apply Universal Restore	Rowse vaults	
Vavigation		
Tape management	Log	
	E	v-us

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

Recovery Bootable	Media - Connected to This Machine (Local Connection) as root
Contractions -	⊤ Tools∽ ⊤ Navigation∽ ⊤ Help∽
Recover data	
Configure the recovery ope What to recover	ration that will start immediately after you click OK at the bottom of the page.
Select data	Required
Task parameters	
Recovery options	Default
	4
	OK Cancel

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**.



	cronisBackupDat	al					Browse
Show: All arch	ives •						C Refresh
Archive name	Owner	Locates on	Created A	Occu	Back	Back	Comments
🗃 rdxRB-Ac	confi-center\R	rdxRB-Acronis	10/9/18 7:45:42	9.875	0 bytes		
🍞 Backup			10/9/18 7:45:42	10.24	16.14	Full	
Hide Archives Sackup contents	and backups						
Hide Archives Backup contents Volume	and backups Volumes • Type	Сарас	:ity Free sp.	ace F	File syste	m	



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

Recovery Bootable	Media - Connec	ted to This Machine (Local Con	nection) as root		🍡 ×
e 🔿 🛛 Actions 🗸	I Tools∨ I I	Navigation ✓ I Help ✓			
Welcome to '1	92.168.4.	103'			
The console is connected	> 'Recovering	disks/volumes' Details		×	
Recover	View details of act	ivity 'Recovering disks/volumes'			
Recover the da	Details	Log			
	Name:	Recovering disks/volumes			
	Description:	Recovering disks and volumes			
Actions	Start date:	10/9/18 7:54:10 PM			
Apply Univer	End date:	10/10/18 8:40:14 AM			
	Duration:	12 hours 46 minutes			
Navigation	Result	Succeeded			
📷 Tape manag					
				Close	

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 Encrypt Password Protection Password Protection Password Protection Basic Password Protection OK Cancel At the New Password At the New Password OK Cancel At the New Password At the New Password OK Cancel At the New Password OK Cancel At the New Password Confirm New Password See enter the password vou would like to use for this cartridge. New Password Etimated Password Strength: Allow Read Access Allow Read Access Alwor Atdridge Reset and Erse All Encryption OK Confirm New Password Charge Posterion Cantridge Reset and Erse All Encryption Confirm New Password Alwor Access Alwor Access Alwor Access Alwor Access Alwor Actinge Reset and Erse All Encryption Confirm New Password Confirm New Password			
• Full Disk AES 256 XTS Encryption • Basic Password Protection • Basic Password Protection • OK • Cancel • Cancel • At the Protection Type dialog box, select Full 256 XTS Encryption OK • Cancel • At the New Password OK • Cancel • At the New Password GK • At the New Password GK • Cancel • Confirm New Password Symptotic Confirm At the New Password Confirm New Password Strength • At the New Password Strength • Alow Cartridge Reset and All Encryption Confi without a password Click OK. • Cick OK • Cancel • Configuration without a password • Click OK • Cancel • Configuration • Configuration • Cancel • Cancel	Protection Type Selection What type of protection would you like to enable?	×	At the default Encryp Enable Cartridge E Password Protection
OK Cancel New Password Selection X tase enter the password you would like to use for this cartridge. At the New Password dialog, enter and cond password that has an password that has an password strength of the Estimated Password Strength: Confirm New Password Estimated Password Strength: Allow Read Access Allow Write Access Allow Cartridge Reset and Encryption Configuration without a password. Click OK.	 Full Disk AES 256 XTS Encryption Basic Password Protection 		At the Protection Typ dialog box, select Fu 256 XTS Encryption OK.
New Password Selection At the New Password dialog, enter and control dialog. Confirm New Password Confirm New Password Leave the default set of Cartridge Reset and All Encryption Configuration without a password. Sword Name Mer Password More Cartridge Reset and Erase All Encryption Configuration without a password. K Cancel	OK Cancel		
Estimated Password Strength:	New Password Selection ase enter the password you would like to use for this cartridge New Password Confirm New Password	× e.	At the New Passwor dialog, enter and cor password that has a password strength o
Allow Cartridge Reset and Erase All Encryption Configuration without a password. Sword Name ster Password OK Cancel	Estimated Password Strength:		Leave the default se Cartridge Reset and All Encryption Con without a password
	Allow Cartridge Reset and Erase All Encryption Configuration without a password. <u>sword Name</u> ster Password OK Cancel	3	Click OK .
	tus Encryption Test Utility Cartridge Info Vendor: Tandberg Data Modet: QuikStor		dialog box, select eit exFAT, and click OK
atus Encryption Test Utility At the Carthoge Forma dialog box, select either dialog box, select either exFAT, and click OK. Vendor: Tandberg Data Exercise of the carthoge Forma dialog box, select either exFAT, and click OK.	Sensi Numer: 8458005258// Status: AES 256 Encrypted RDX Cartridge is using full disk encryption. Data access is allowed. Disable Access		When returned to the tab, click Advanced and Permissions .
atus Encryption Test Utility Cartridge Info Vendor: Tandberg Data Model: QuikStor Serial Number: 845000625877 Status: AES 256 Encrypted RDX Cartridge is using full disk encryption. Disable Access Disable Access	Aaster Password Properties: Read/Write/Manage Passwords Change Password		
atus Encryption Test Utility Cartridge Info	Remove Encryption		
atus Encryption Test Utility Cartridge Info Wendor: Tandberg Data dialog box, select either exFAT, and click OK. Model: GuidStor GuidStor Serial Number: 84500025877 Status: AES 256 Encrypted GuidStor When returned to the lab, click Advanced P and Permissions. Master Password Properties: ReadWrite/Manage Passwords Disable Access	Advanced Passwords and Permissions		



advanced Options	Х
Add a Password	
View / Modify / Delete Existing Passwords	
Add an Automatic Drive Media Authentication Password	
Delete Automatic Drive Media Authentication from RDX Drive	
Class	
Liose	

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.

Sales and support for Overland-Tandberg products and solutions are available in over 90 countries. Contact us today at salesemea@overlandtandberg.com

IB_v5_jul19_2022

©2022 Overland-Tandberg. All trademarks and registered trademarks are the property of their respective owners. The information contained herein is subject to change without notice and is provided "as is" without warranty of any kind. Overland-Tandberg shall not be liable for technical or editorial errors or omissions contained herein.