

Integrating RDX® QuikStor™ into NetJapan ActiveImage™ Protector

INTEGRATION BRIEF

Backup is the life insurance of a company as it protects its crown jewels. Backup ensures data availability and business continuity after data loss. It is important to know, that data loss could result in loss of business and loss of business might result in closing the business. Backup simply gives a peace of mind.

The 3-2-1 Backup Strategy for full disaster protection

Data loss can be caused by many reasons:

- Employees are pushing the wrong button or delete files by accident
- Software problems might corrupt data
- Hardware failures cause total data loss
- Virus and ransomware attacks destroy data or make them inaccessible
- Fire or natural disasters could damage the IT-equipment
- Sabotage or theft

Because of these different incidents, multiple backup copies should be created and stored at different sites. For full disaster protection, the 3-2-1 backup strategy should be implemented: One media for primary backup and another one as a secondary backup target. If one media fails, the other media is still available for recovery tasks. In addition, a third copy should be stored on a removable media to place this copy off-site. This ensures being capable to accomplish a full data recovery in case of a disaster at the business site. In addition, the off-site copy cannot be affected by a virus or ransomware attack.

RDX® QuikStor™ - ruggedized, removable and simple

Overland-Tandberg's RDX QuikStor is a removable disk system which simply attaches via USB. It consists of a drive and a media. The drive is constantly connected to the Server system. The removable media has a rugged design, it's reliable, fast, easy-to-use, and tough enough to cope in busy and harsh environments. RDX can be implemented as the secondary backup target with the ability to store offsite.

Media Rotation

Especially for smaller environments with single server infrastructure, laptop users or single NAS implementations, media rotation is an ideal method to be fully protected against data loss due to a disaster. In this case, a single backup target with removable media, like RDX, should be implemented. Using multiple media enables you to alternate the media after the backup has finished.

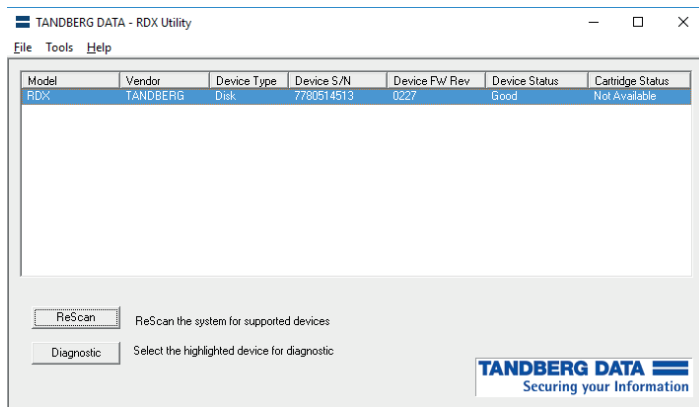


RDX QuikStor combines the benefits of Disk and Tape

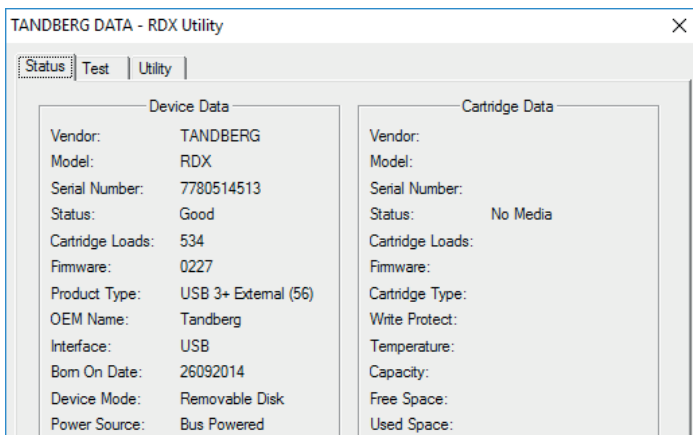
This guide shows a step-by-step instruction of a media rotation scenario with RDX QuikStor as well as the integration of RDX in a 3-2-1 backup scenario including bare metal recovery.

Configure RDX QuikStor in fixed disk mode

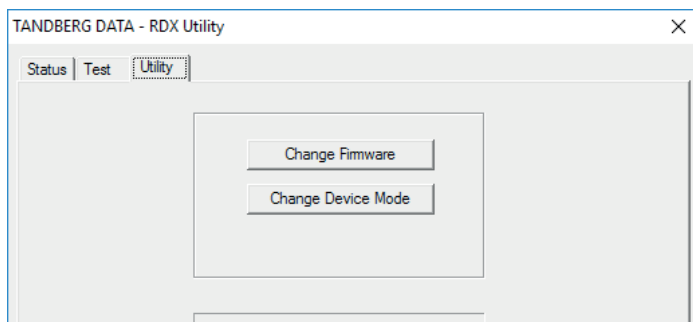
To boot from a RDX cartridge, the RDX drive needs to be switched to fixed disk mode. Use the RDX utility software (version 1.54 or later) to configure RDX QuikStor in fixed disk mode. The software is available on the RDX QuikStor download section of the Tandberg Data website. In addition, the latest firmware should be downloaded and installed. (2.27 or later).



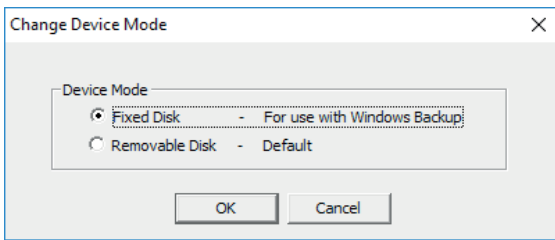
Download the RDX utility from the Tandberg Data website (www.tandbergdata.com). Start the RDX Utility and click on “Diagnostic.” If there is media inside the drive, eject it.



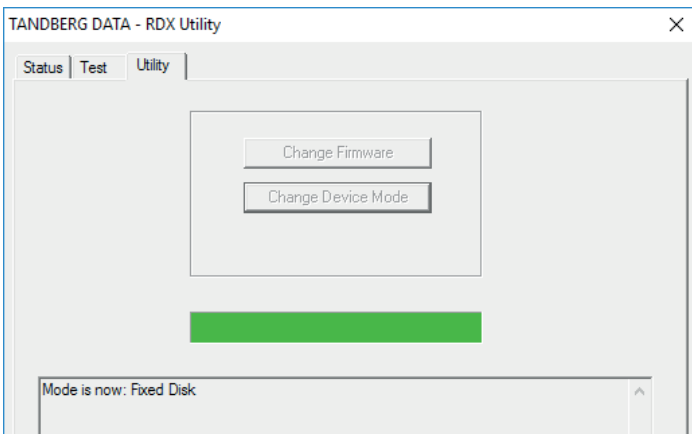
Select the “Utility” tab.



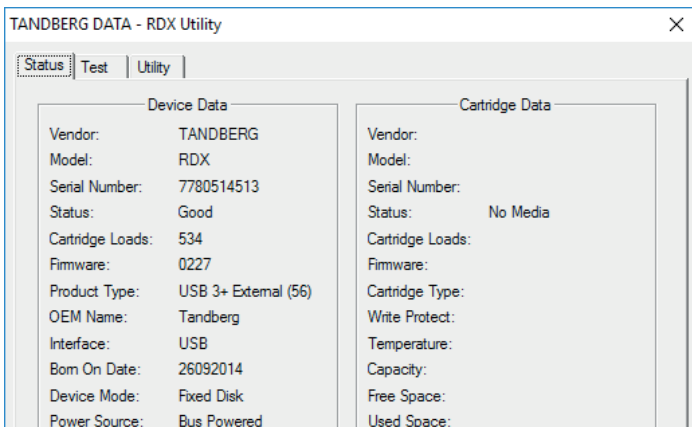
The “Change Firmware” button can be used to update the firmware if necessary. Click on “Change Device Mode.”



▶ Choose “Fixed Disk” and click “OK.”



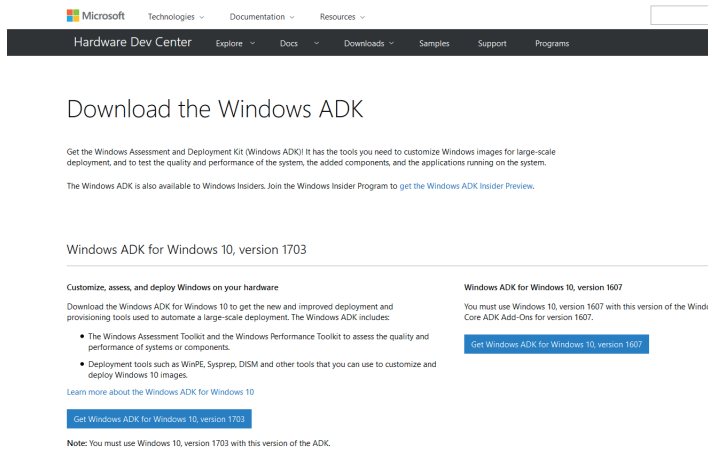
▶ Check the status message in the lower part of the window. Click “Exit” and close the RDX utility window.



▶ RDX is now in Fixed Disk Mode.

Creating a bootable RDX recovery cartridge

In case of a total system crash, the whole operating system needs to be recovered in addition to the application and user files. This could be done by inserting the Windows startup DVD. A more convenient solution is to create a RDX recovery cartridge which includes a bootable Windows Recovery Environment and the backup files.



Download the “Windows Assessment and Deployment” (Windows ADK).

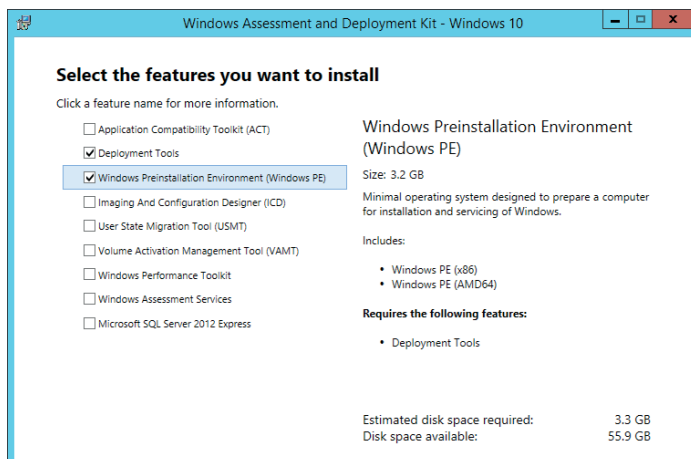
You might use these links:

Windows 8.1:

<https://www.microsoft.com/en-US/download/details.aspx?id=39982>

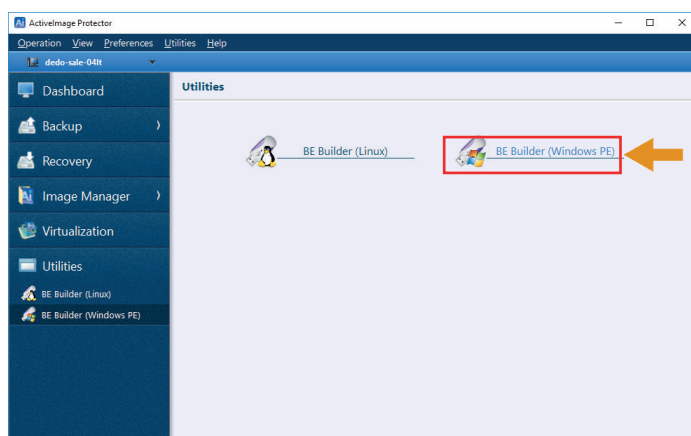
Windows 10 (please use version 1607):

<https://developer.microsoft.com/en-us/windows/hardware/windows-assessment-deployment-kit>



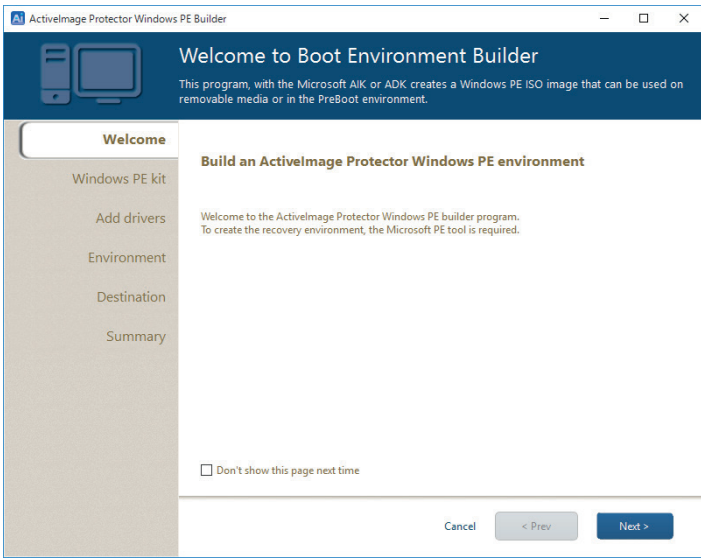
Start “adksetup” to install the Windows ADK. This will create a subdirectory called “Windows Kits”. Open this subdirectory and start “adksetup”.

Please select “Deployment Tools” and “Windows Preinstallation Environment” to install. Deselect all other options.



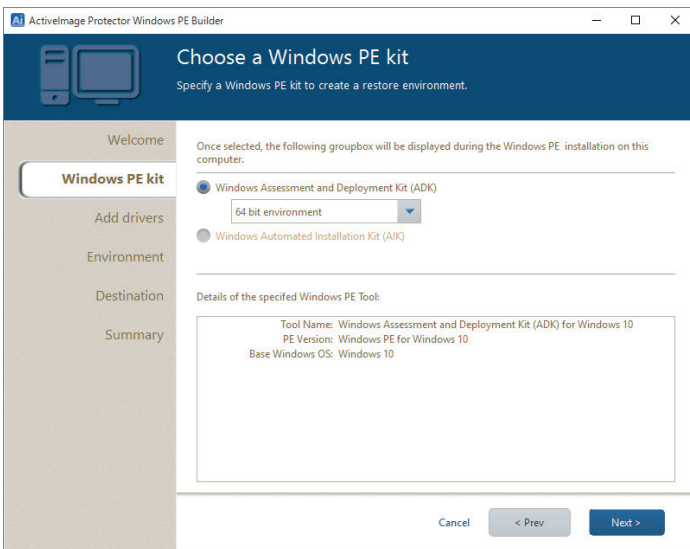
Start the ActiveImage Protector Software.

Choose “Utilities” and select “BE Builder (Windows PE)”.



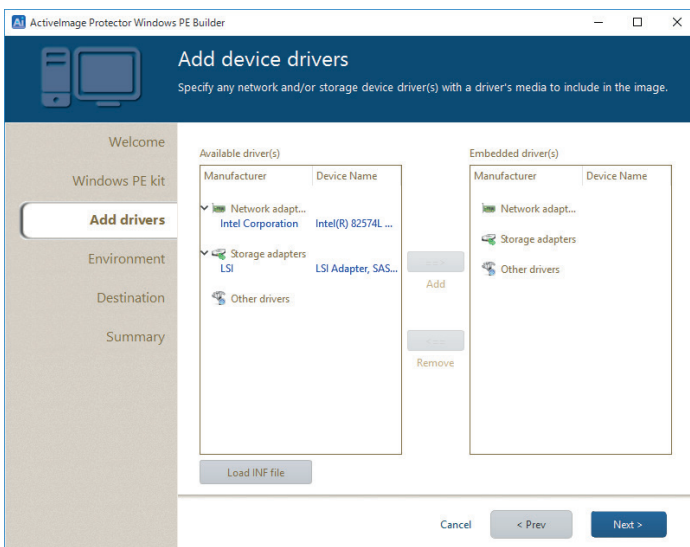
The Boot Environment Builder application is started.

Click "Next".



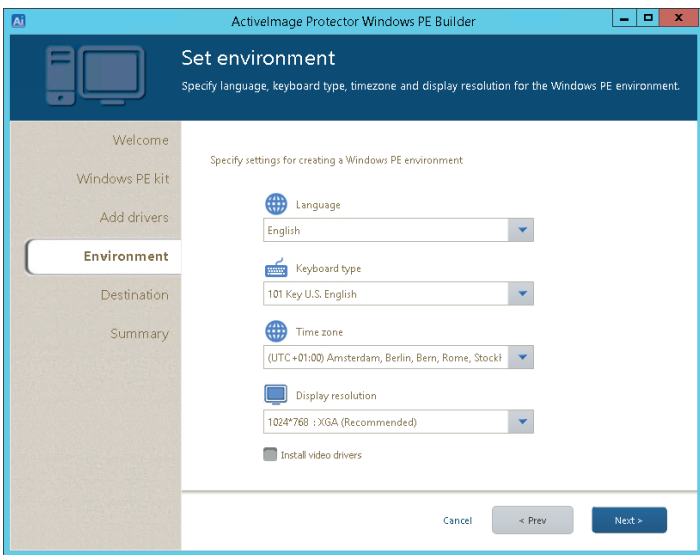
The application recognizes the installed ADK and the operating system version. You might change the version if necessary.

Click "Next".



The Boot Environment Builder allows you to install device drivers needed for your environment. Network and storage device drivers included in the current system are detected and listed on the left pane. Select the driver(s) and click on "=>" to embed them into the boot environment.

To add additional drivers, click on "Load INF file" and browse through your system. Click "Next".

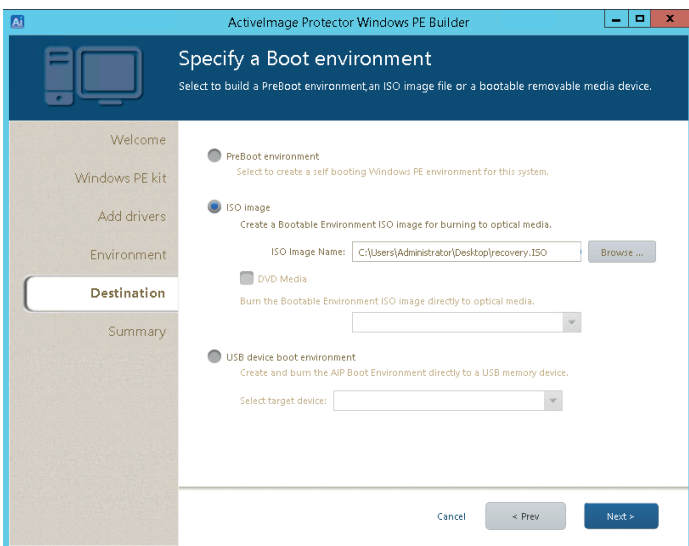


Set your environment.

Hint:

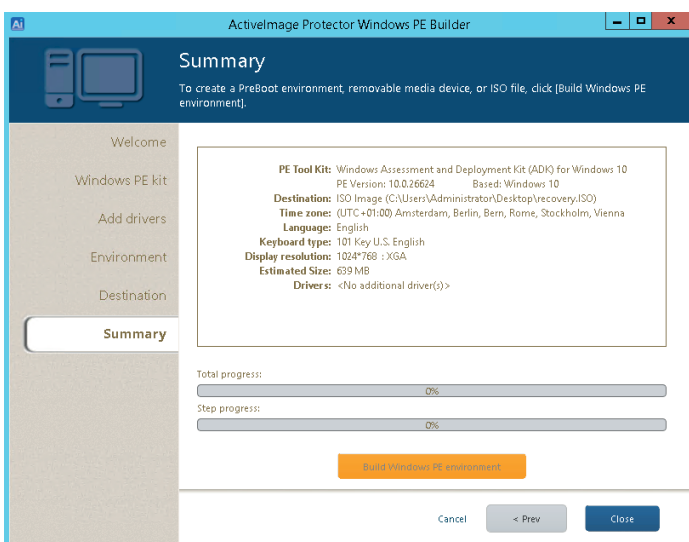
For a higher compatibility, you can skip the video driver installation at this time. You should keep default screen resolution at 1024*768.

Click "Next".



Select "ISO Image" to create an ISO image file in a specified location on your hard disk.

Click "Next".

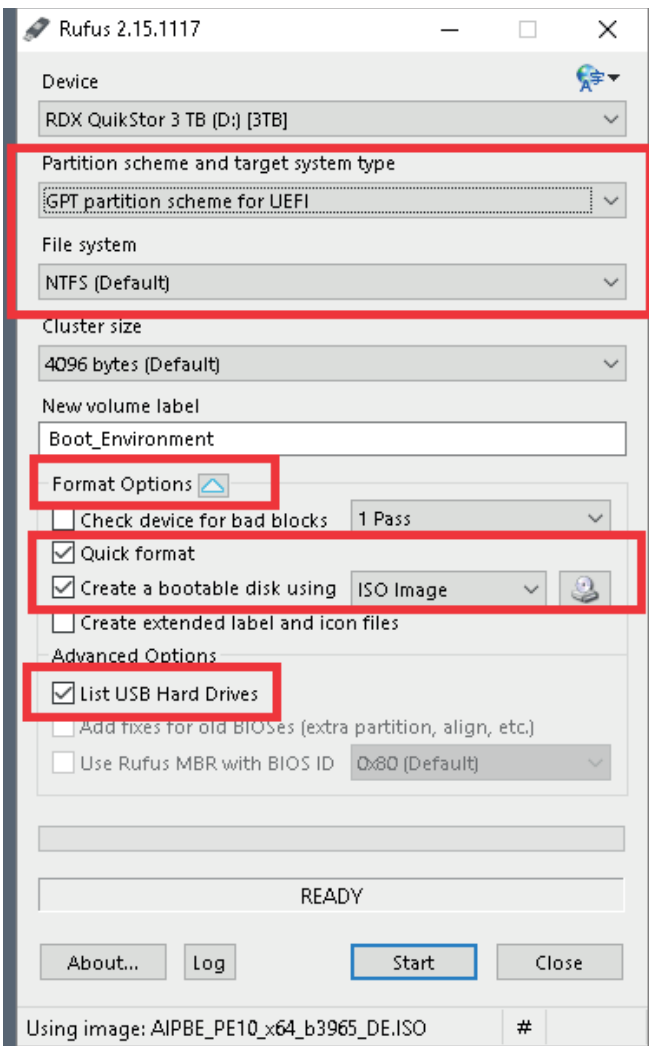


Please check your configuration at the "Summary Screen".

Click on "Build Windows PE environment", if you are satisfied with your settings, otherwise click "< Prev" to make changes.

Click on "OK" to confirm to start building Windows PE environment.

Click "Close" if download has finished.



The ISO file is now stored onto the local disk of the server.

To create a bootable RDX media, we use a third party tool called “Rufus” which is downloadable from

https://rufus.akeo.ie/?locale=en_US.

Please extend the format options and check the “List USB Hard Drives” box is your RDX drive is not listed.

According to your system, choose the right option for MBR or GPT:

RDX media up to 2 TB = MBR partition scheme for BIOS

RDX media over 2 TB = GPT disk partition scheme for UEFI

Check the “Create a bootable disk using” box and select “ISO image” from the listbox. Browse your previous created ISO file.

Please double check your partition scheme and file system settings!!!

Press “Start”.

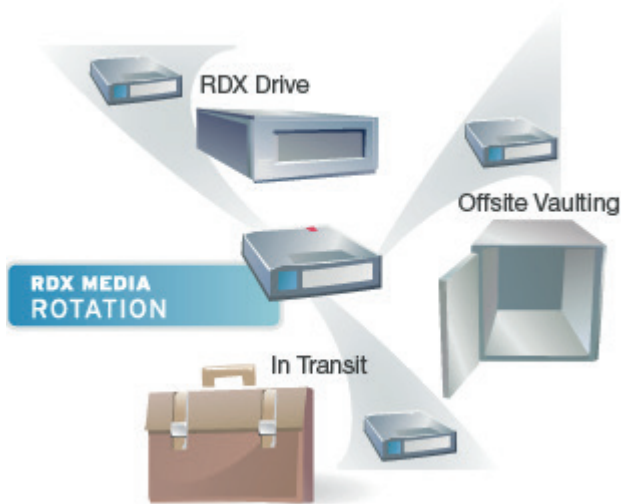
Volume 0		System Rese	NTFS	Partition	500 MB
Volume 1	C		NTFS	Partition	237 GB
Volume 2	D	3TB RDX	NTFS	Partition	1863 GB
Volume 3	E	UEFI_NTFS	FAT	Partition	256 KB

The RDX media is now a bootable media.

As we have chosen to create a GPT partition scheme for UEFI in our example, Rufus added a small FAT32 boot partition.

Scenario I - Backup to RDX QuikStor with Media Rotation

Attach your RDX drive to your computer system. We recommend using at least three RDX media for media rotation implementation. One media is in the office, ready for the next backup job, one media is off-site at a safe location and the third one in in transit to or from the off-site location.

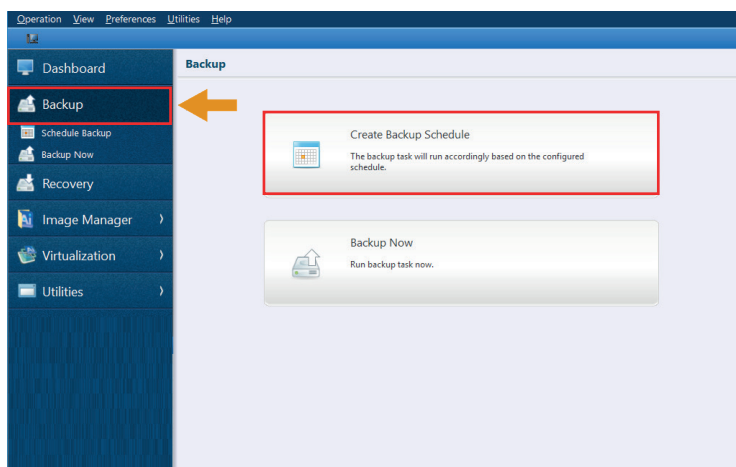


The media rotation scheme:

The first media is in the office, ready for the next backup job

The second media is off-site at a safe location

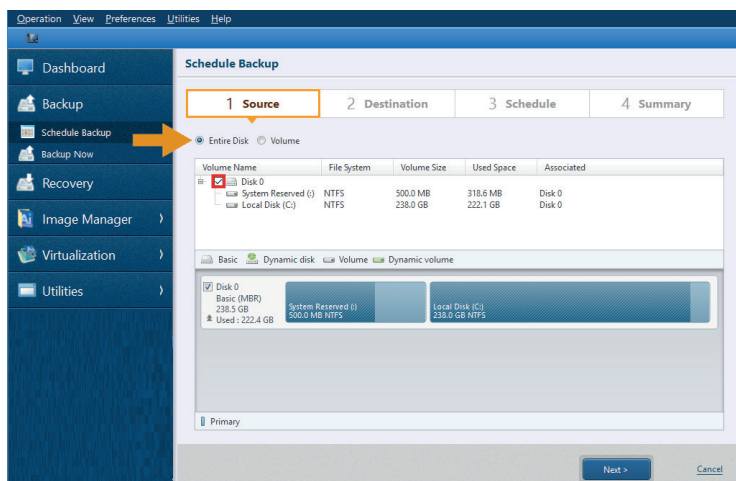
The third Media in in transit to or from the off-site location.



Launch ActiveImage Protector.

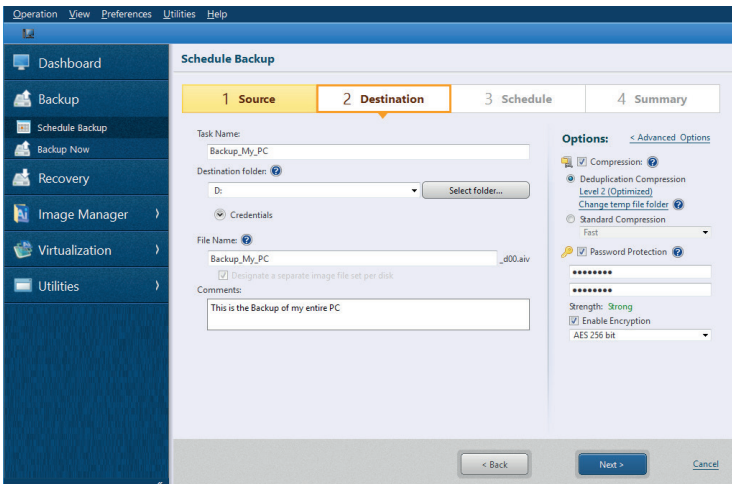
Click on “Backup”.

Choose “Create Backup Schedule”.



Choose the source disk you want to backup. We recommend to choosing “Entire Disk” and selecting all existing volumes.

Click on “Next”.



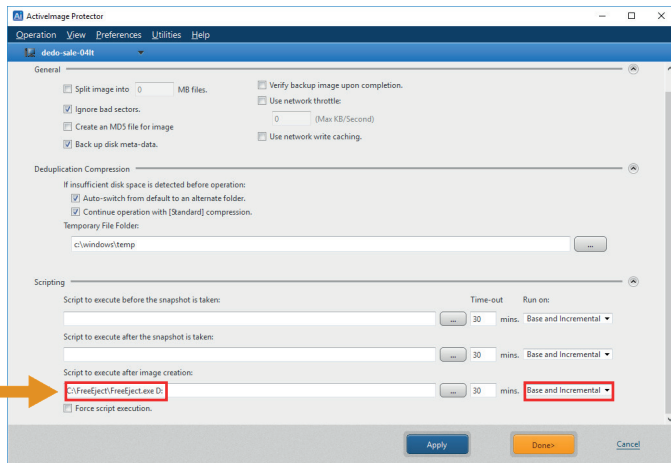
In the "Destination" section, choose a task name to specify your backup job.

Then select the destination you want to store your backup. Here, drive "D:" has been chosen, as this is the connected RDX drive.

The backup filename is automatically created according to date and time. You might overwrite this name with your own suggestion.

On the right side of this window, choose compression / deduplication if applicable and secure your backup file to protect off-site backup against unauthorized use with password and AES 256 bit encryption.

Select "Advanced Options".

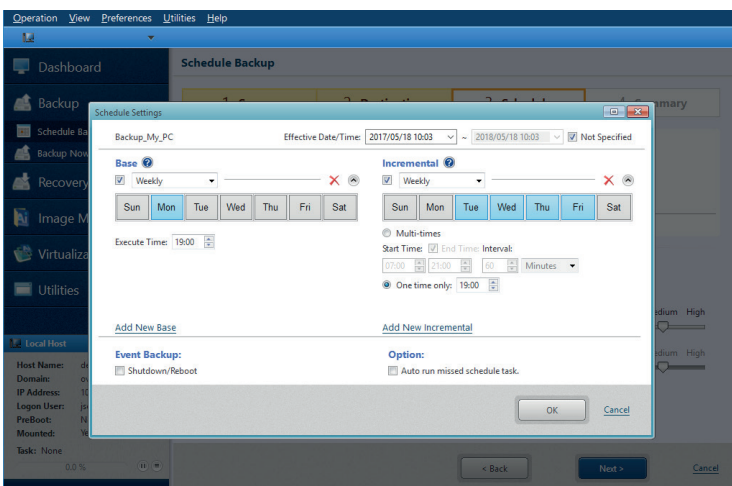


We highly recommend integrating a post processing script to eject the RDX media after each backup as a visual reminder to rotate the media.

A freeware tool is available under <http://www.freeject.com/>

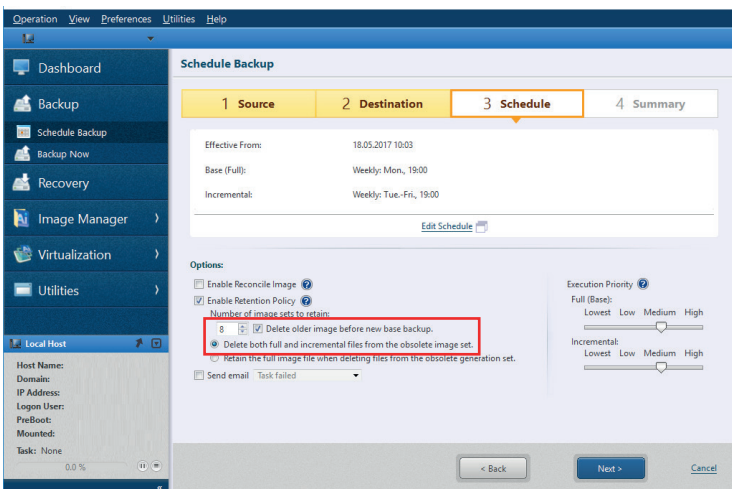
Click on "Done".

Then click "Next".



Define your backup schedule. In this scenario, we define a daily backup on workdays at 7:00 PM, starting with a full backup on Mondays followed by incremental backups from Tuesday through Friday.

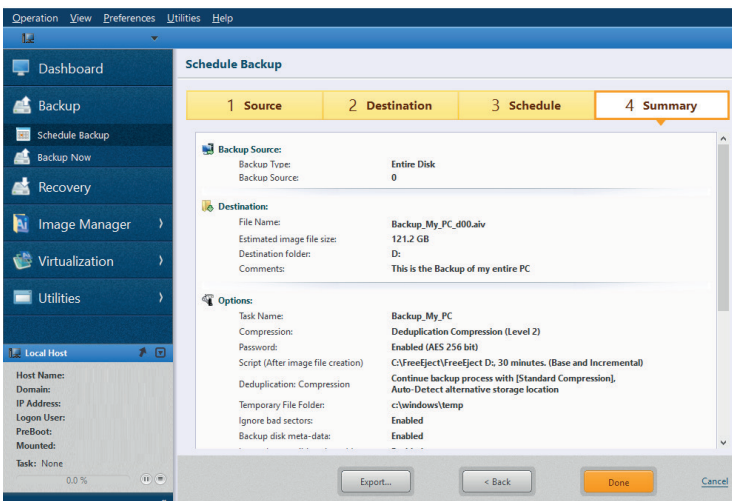
Click "OK".



You might want to set a retention policy to keep a certain number of backup sets (full backups with their corresponding incremental backups).

This will delete older backup sets to free up disk space on your RDX media. The number of sets applies according to your requirements. In this example, we keep 8 weeks (because of a weekly full-backup).

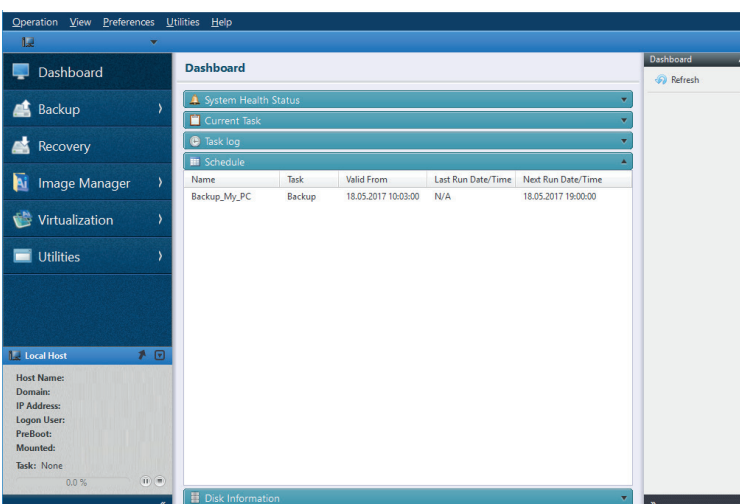
Click "Next".



A summary screen is displayed. Please check your setting.

If you are satisfied with your settings, click "Done", otherwise click on "Back".

After clicking "Done", you can decide whether you want to start your backup right now.



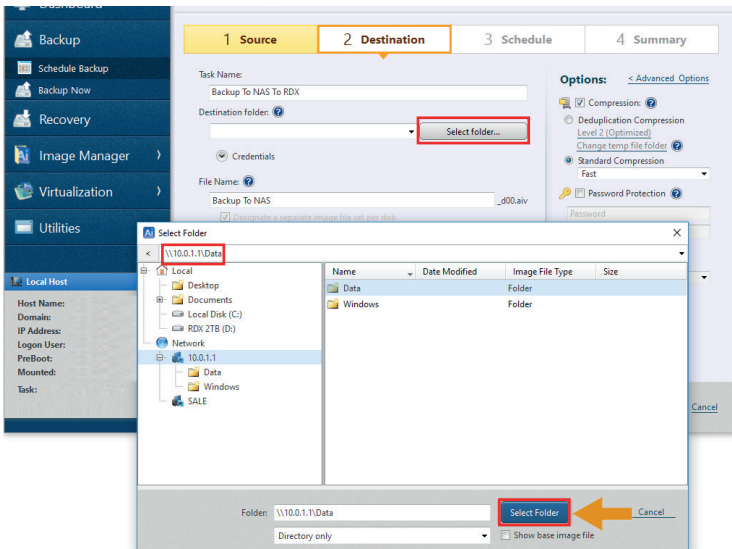
The created backup job is displayed in the dashboard screen and ready to run at the specified time.

Scenario II - Backup to NAS and Replication to RDX QuikStor

Backup to NAS is not sufficient for data protection. As already mentioned at the beginning of this document, a second backup copy to another backup target should be created. Furthermore, one copy should be stored off-site to be protected against local incidents or virus and ransomware attacks.

In conjunction with ImageCenter LE, Active Image Protector is able to perform a primary backup to a NAS System and secondary backup to RDX QuikStor including off-site protection.

Step 1: Backup to NAS

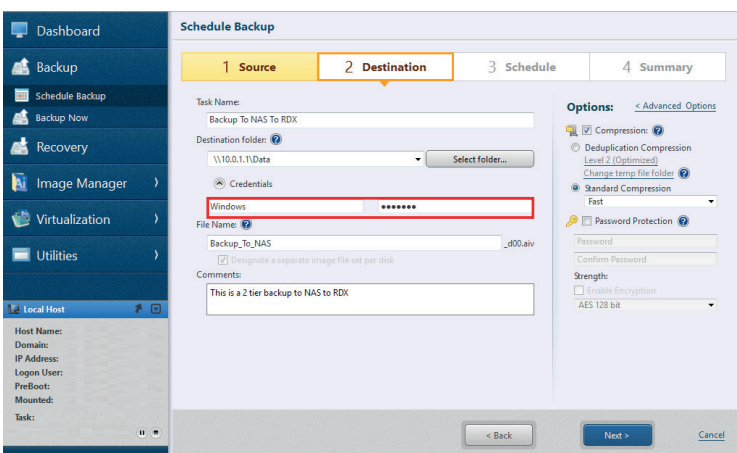


Launch ActiveImage Protector and choose the source disk for backup as described in scenario I.

Click on “Next”.

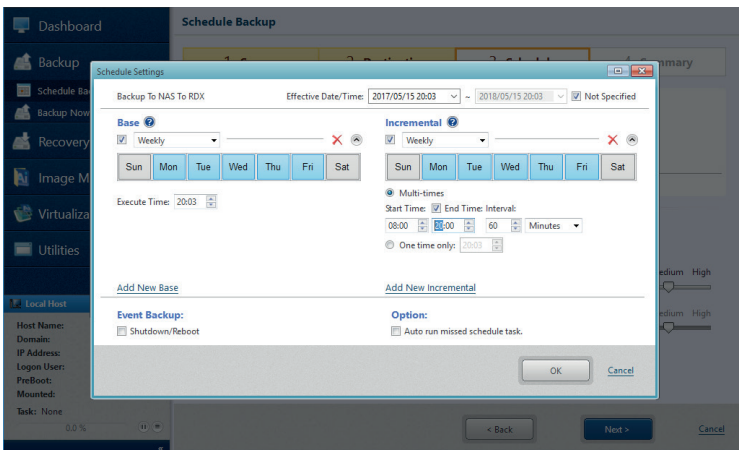
Assign a Task name for the backup job. Then click on “Select Folder” and choose your NAS System. If it does not appear in the selection menu, type in the IP address. If desired, select a subfolder on this NAS as the backup target. In our case, “Data” has been selected.

Click on “Select Folder”.



You might need to provide a username and password for your backup destination.

Click on “Next”.

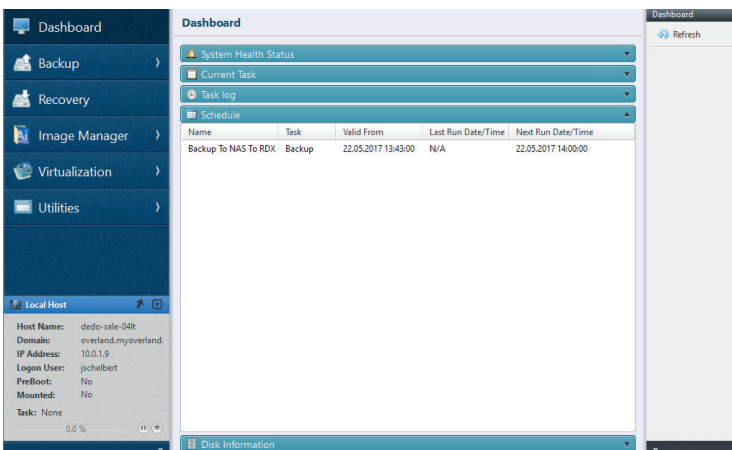


In this example, we perform daily full backups and additional incremental backups on every hour.

These settings might vary according to your business needs.

Click "OK".

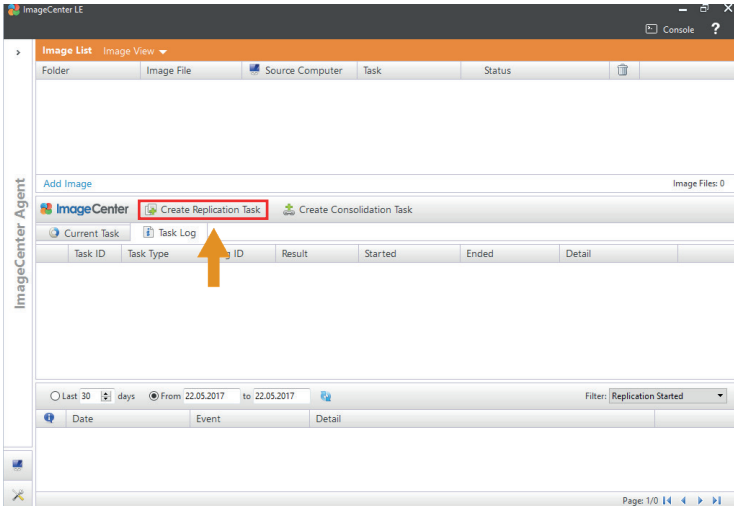
Please refer to scenario I for additional settings.



The created backup job is displayed in the dashboard screen and ready to run at the specified time.

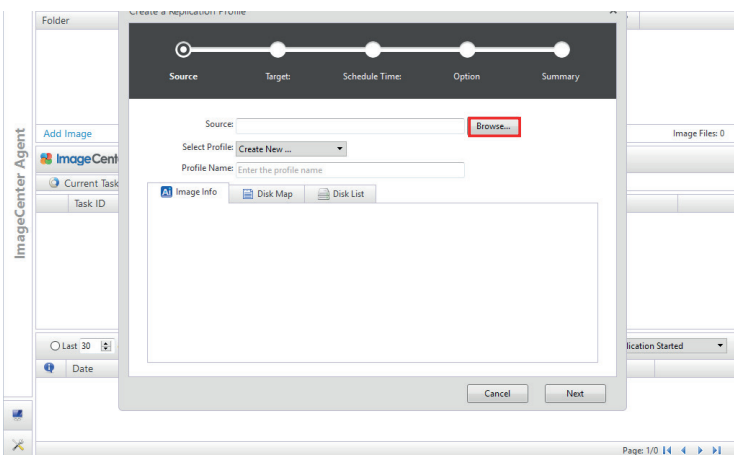
Step 2: Replication to RDX

Replication to RDX can be performed with the ImageCenter LE software, which is part of the backup software package.



Start ImageCenter LE.

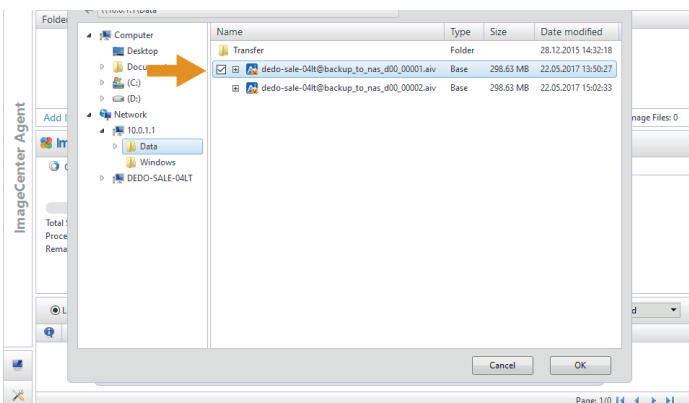
Select "Create Replication Task".



Click on "Browse" to select your primary backup target (the NAS system in our case).

You might need to type in a username and password.

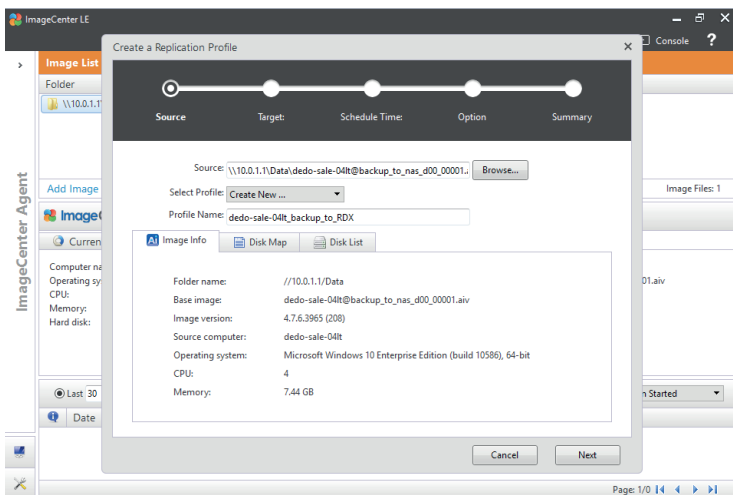
Click on "Next".



Select the image file you want to replicate.

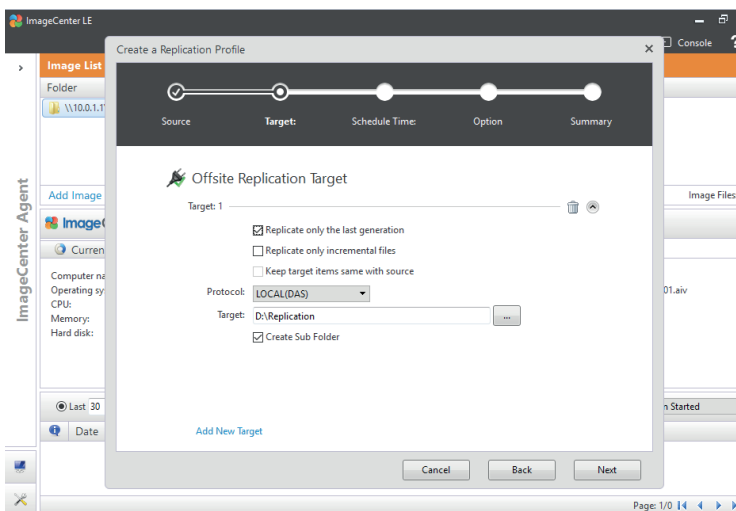
Notice, that only the image file of the initial backup can be selected.

Click "OK".



You might want to change the default profile name.

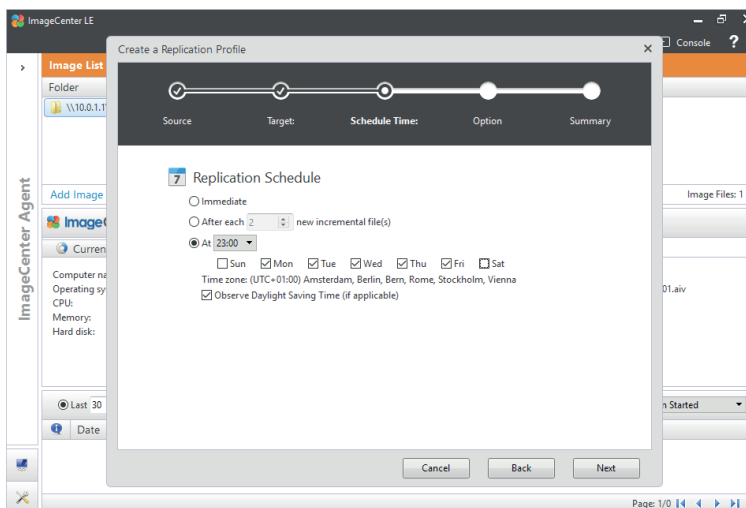
Click "Next".



Select the target for replication. Here, we choose "LOCAL(DAS)" and select drive letter "D:" as this is our RDX drive. In addition, we created a dedicated subfolder for replication.

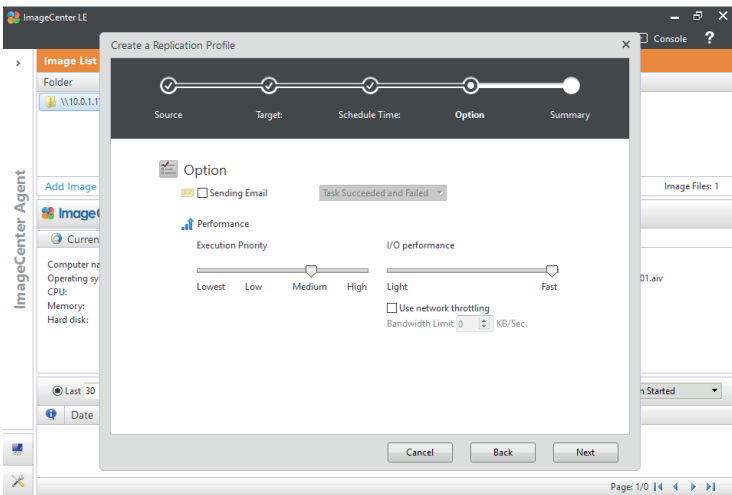
You can choose some replication-options, in this example, we selected "Replicate only the last generation" to replicate the latest backup only.

Click "Next".



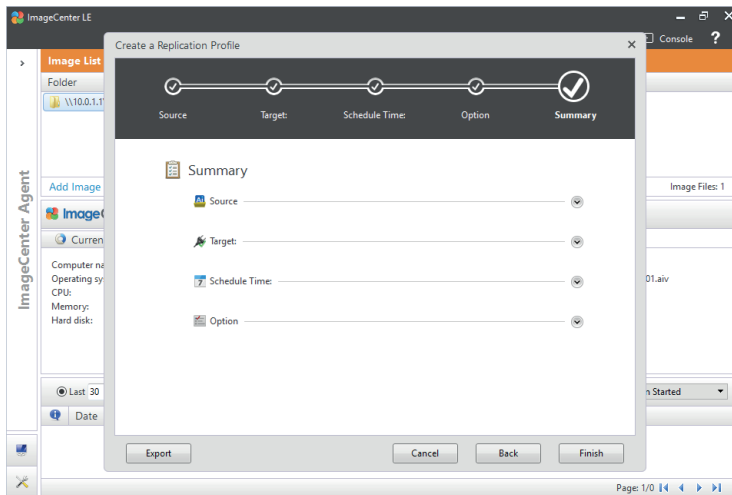
Specify the schedule according to your requirements. In this example, we choose a replication on workdays at 11PM after our full backup.

Click "Next".

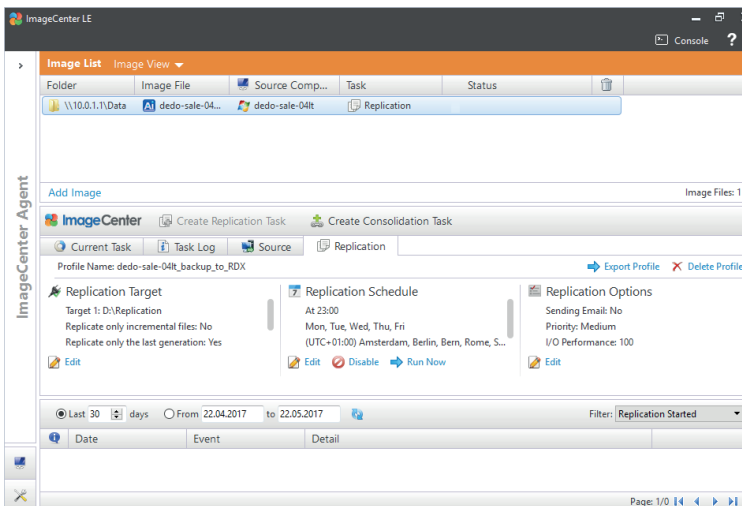


You might want to adjust some performance settings.

Click "Next".



The summary window enables you to review your settings. If you need to change some settings click on "Back", otherwise select "Finish".

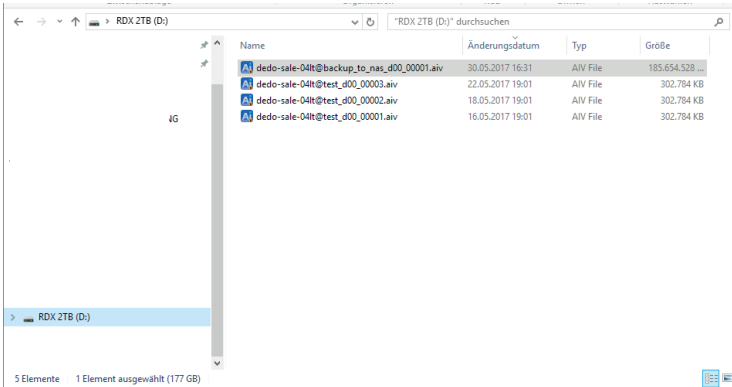


The replication has been created and will start according to the specified schedule.

Performing a restore

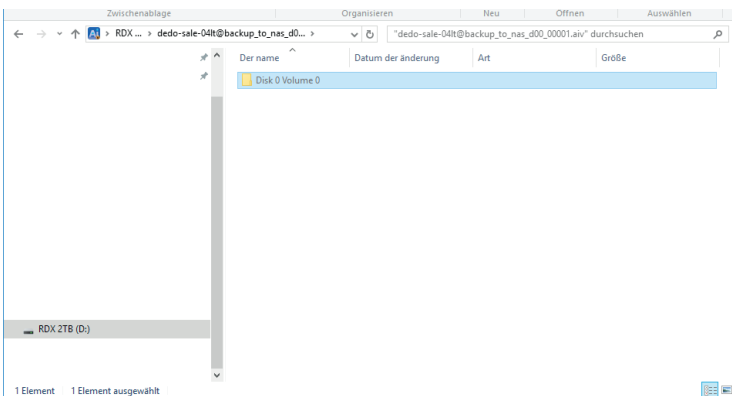
You can perform a single file/directory restore or a full system restore with bare metal recovery.

Single file/directory restore



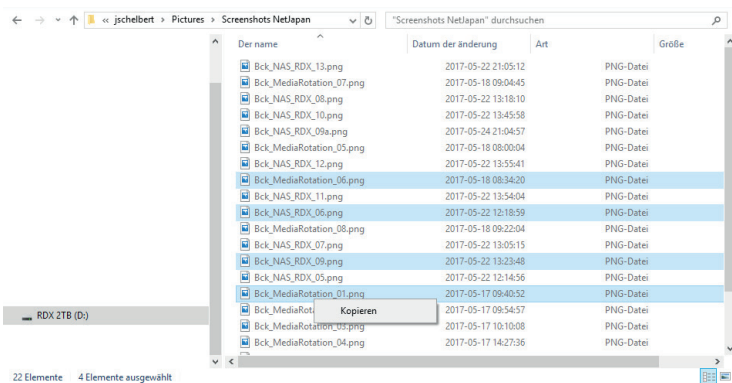
Select your backup target on either your NAS system or RDX media.

Choose the appropriate backup file and double-click on it.

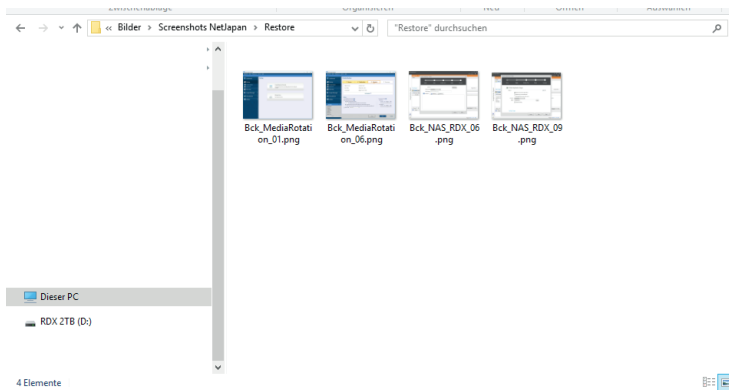


Select the volume you need to restore your files/directories.

Browse your directory structure until you reached the directory/files you need to restore.



Select the appropriate directories/files you need to restore. Right click and select "Copy".



Select the destination folder for restore right click and select "Paste" to restore them.

System Restore using BMR (bare metal recovery)

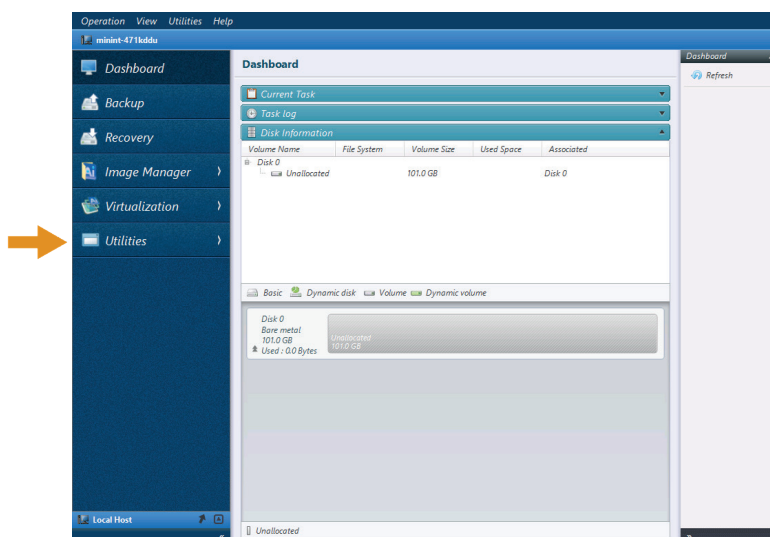
The RDX must be in fixed disk mode for this procedure!

If necessary, you might perform this setting from another computer. Please refer to the section "Configure RDX QuikStor in fixed disk mode" at the beginning of this guide.

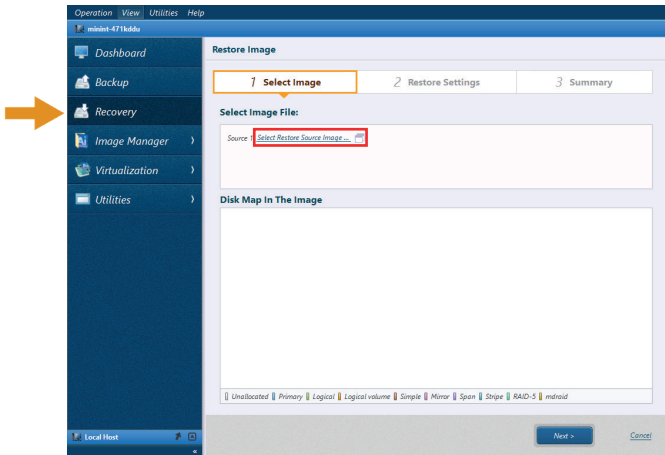
In case, you don't have another system available, you can change the mode directly at the RDX drive by following these steps:

1. Press and hold the eject button for five seconds
2. The LED on the button will now flash alternatively yellow and green
3. Press the eject button once to set the drive into the Fixed-Disk-Mode
4. The LED will now flash continuously yellow, green, green
5. Press the eject twice in rapid succession to confirm

Attach the RDX-drive and load the appropriate cartridge with the system image previously created and the backup files. Power on your system.

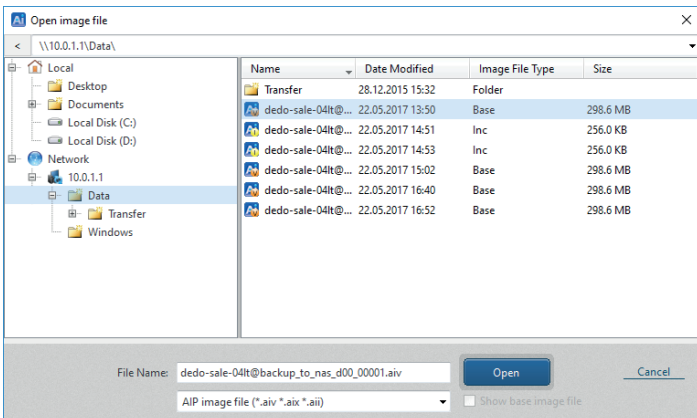


After the recovery environment has booted, the Active Image Protector application is started automatically. You can check the local disks in the overview. If a disk is missing, you can click on "Utilities" and next "Driver loader" to load missing RAID or storage controller driver.



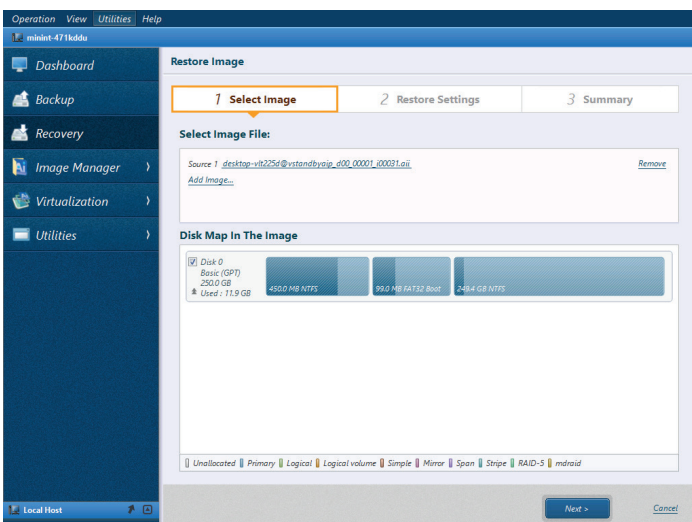
From the menu pane, click “Recovery”.

Click on “Select Restore Source Image”.



Choose a full base backup or an incremental image file for restore.

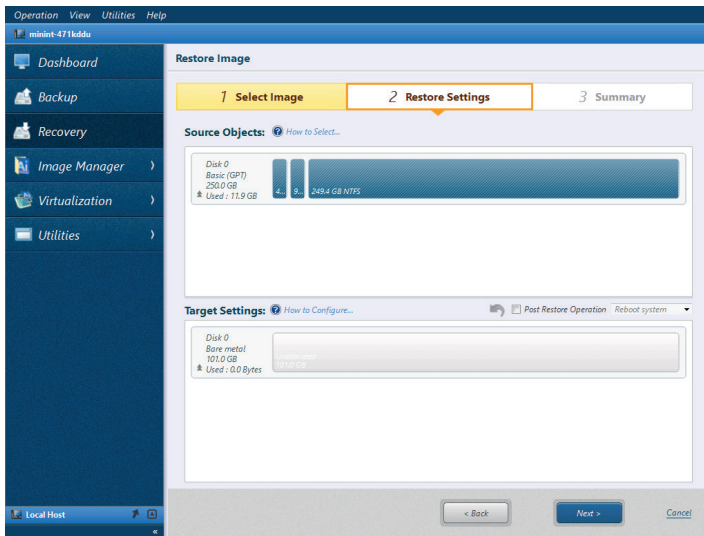
Highlight and click “Open”



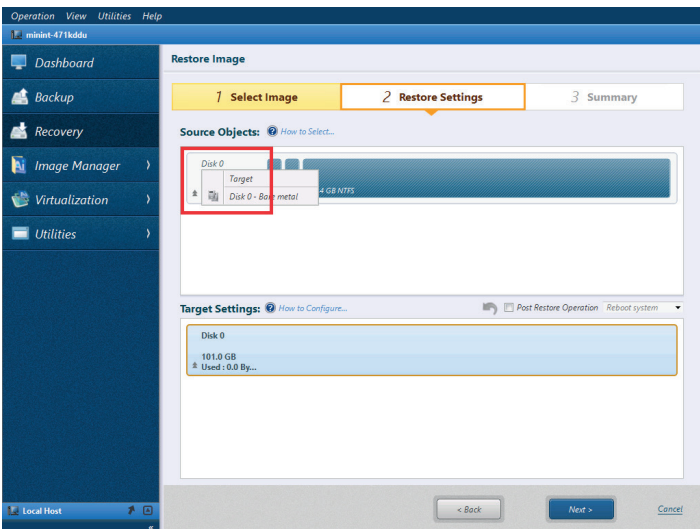
The image has been selected for restore.

Check the box in the Disk Map to select the volume or disk to be restored.

Click “Next”.



The disk selected is now displayed under “Source Objects:”.

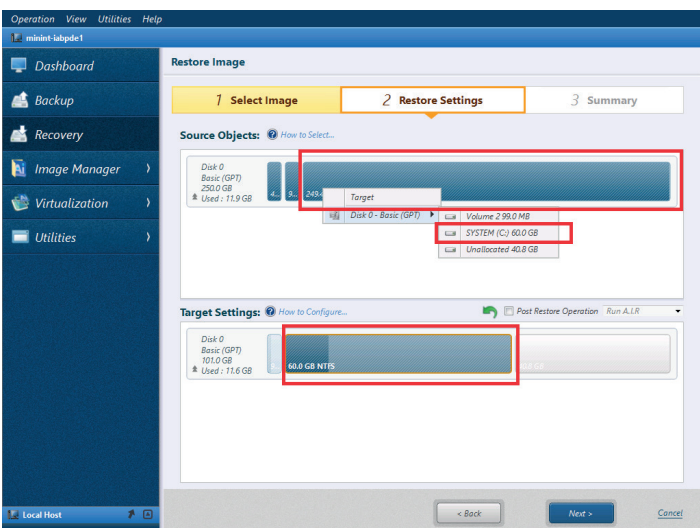


Right-click on the restore source (a disk or a volume).

We have now a few options:

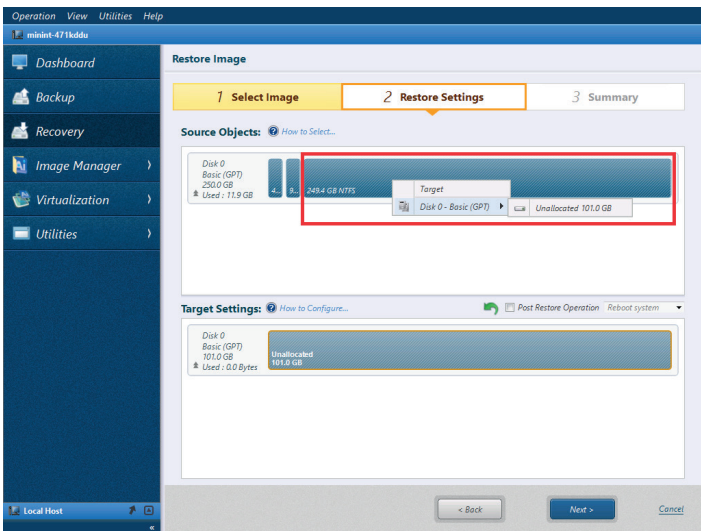
1. We just want to restore the entire disk from the backup to new disk with the same size.

In this case just right click to the disk on top under “Source Objects:” and choose your new target disk and press “ok”.

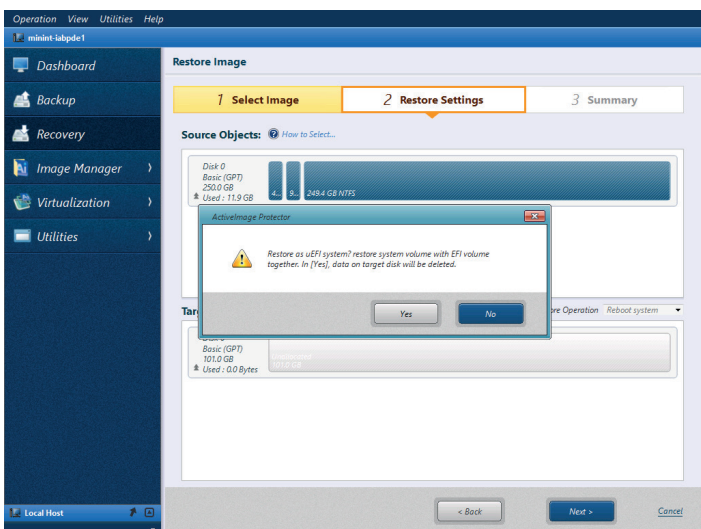


2. You want to restore single volume to an existing disk

Right click on top under “Source Objects:” and choose your target volume and press “ok”.



Right click to the system volume (Windows C: drive) on top under “Source Objects:” and choose your new target disk and press “ok”.



When the restore target destination is specified, the following message is displayed. Click on “Yes”.

If the restore target destination volume or available space is smaller than the source, but the above conditions are satisfied, the volume is added to “Target Settings:”.

If you want to further reduce the volume, right-click on the volume to select “Resize Volume” or place the mouse cursor on the right-end of the volume and drag it to the left.

You can repeat this for the other remaining data volumes, to change the volume size.

Afterwards click on “Next >”. Review the settings and click on “Done” to start the restore task.

After the restart, the system is up and running. Additional tasks may be performed to complete the recovery.

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

IB_v1_aug25_2017

©2019 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.