

RDX WORM and RDX RansomBlock frequently asked Questions



Q: What is WORM?

A: WORM (Write Once Read Many) is a write-protection for storage-media, which prevents data from changing, overwriting or deletion. WORM media is used in digital archives and meets regulatory compliance requirements, where data must not be changed or deleted.

Q: What is RDX WORM?

A: RDX WORM is a software functionality used with standard RDX Media in conjunction with a license and our rdxLOCK software and works on Windows OS only. Beside RDX WORM, there is a second feature available for Ransomware protection called RDX RansomBlock. Users can choose from either WORM or RansomBlock according to their needs.

Q: What is RDX RansomBlock?

A: RDX RansomBlock is a choosable feature of the rdxLOCK software. The RansomBlock functionality sets all data on the RDX 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. This ensures that virus and ransomware attacks cannot threat backup data. Backup applications are able to use RDX media with RansomBlock like a regular RDX backup target but have to whitelist the backup application.

Q: What are the advantages of RDX with WORM?

A: There is no change in your workflow: RDX WORM is fully transparent for archiving applications. You can continue to work as you used to. After you store your data to RDX WORM, it is automatically unchangeable and undeletable (e.g. virus), but you can read and access your Data without any limitation. Unlike to tape WORM and optical discs (CD, DVD or BluRay), you do not need any additional software to write to the media. With RDX, you benefit from fast and random data-access and high read/write transfer-rates.



Q: Why do I need RDX WORM?

A: RDX WORM supports you in archiving data, which have to meet regulatory compliance requirements like SOX, HIPAA or others.

Q: Can I reuse the rdxLOCK license?

A: Yes this is now possible with the new licenses and the new rdxLOCK software release. This is a new feature compared to our previous software license. Each software license can be reused with the same media only. It allows you to change the WORM mode or change to Ransomblock. However, each time you reuse or change the WORM mode all data will be lost as it has to be repartitioned and formatted.

Q: Are there software only licenses available?

A: Yes, there are. And you can use them with any RDX Media of any size and brand.

Q: Is it possible to have WORM and non-WORM data on one media?

A: Yes, that is possible. There are two different WORM-modes for RDX WORM. There is a "Directory-Level Retention" and a "File Level Retention" mode. The File Level Retention mode controls the WORM function via the read only attribute of a single file. This can be set either manually or via archiving applications.

Q: How do I use a RDX WORM media for the first time, what do I have to consider?

A: You have to install the rdxLOCK software (see manual). Afterwards, you have to start the software to configure the media for the appropriate mode ("WORM" or "RansomBlock"). Then the conversion of the media is performed. For proper rdxLOCK software operation you need to install a VRC-Key (Verified Retention Clock) that can be downloaded from our Website or in rdxLOCK software.

Q: How long does a "Set to WORM" process take?

A: A "Set to WORM" process takes some time, depending on the on the size of existing data in the volume and your hardware. We recommend starting this process before writing first data to the media as the conversion can take several hours or days.



Q: What are the differences to previous license and rdxLOCK 2.3.2.226 software releases?

- A:
- Support of directory level and single file retention
 - rdxLOCK licenses can be reused with same RDX Media
 - support for current Windows OS
 - higher capacity WORM media/licenses
 - new Ransomblock feature

Q: I'm currently using RDX WORM are there any changes or compatibility issues when I perform the software upgrade to the latest rdxLOCK version?

A: No, there are no changes expected. You will be able to continue to use the configured RDX WORM functions with the same license. It is not possible to reuse the license by reformatting the media to benefit of the new rdxLOCK features. However, you benefit of new Windows OS support if you need to migrate your OS.

Q: Can I use the RDX WORM media on different computer systems?

A: Yes, you can. All you need is rdxLOCK software installed; the license is stored on the RDX Media, there is no need to buy additional licenses. If no rdxLOCK software is installed, you will see just three files which show you information about using rdxLOCK. The data is stored in a 2nd hidden and encrypted partition and is not accessible without rdxLOCK software.

Q: How does a license-registration for a WORM media work?

A: The license-registration is performed via rdxLOCK software. Please follow the installation guideline of the manual. Registration could be done over the internet, via e-mail or you can save a file to send the registration file whenever you are online.

Q: What Operating systems are supported?

A: rdxLOCK is a Windows only software solution. When trying to use on other OS you will not be able to access the data. Supported Windows OS versions are listed in our software compatibility guide.

Q: Can I use RDX WORM media with a backup application?

A: Yes, you need to utilize the RansomBlock mode!



Q: Can I use rdxLOCK and RDX WORM / Ransomblock with other RDX vendors RDX drives/docks?

A: Yes, you can. All you need is a RDX WORM Media or rdxLOCK software license. Note: Dell RD1000 will work with 1.0TB and 2.0TB WORM media only.

Q: I was using the 60-Day trial version and don't have access to the data anymore. Can I replace the trial license with a valid rdxLOCK software license and continue to use it for non WORM operations or continue with RDX WORM after a successful trial?

A: Yes, you can. After the trial period is expired, you will not have access to the data stored on your RDX Media. You can then choose to repartition and format your RDX media but that means you will lose all data. If you want to keep your data access you need to apply a license after the trial period for the same or higher capacity.

Q: Does rdxLOCK work with all RDX Drives and RDX QuikStation?

A: Yes it does. Incl. All RDX OEM branded drives for RDX QuikStation it is supported with RDX modes and Disk Autoloader mode only and you can use both RDX WORM and Ransomblock.

Q: What RDX QuikStation operation modes are supported with rdxLOCK?

A: Currently individual RDX targets and Disk-Autoloader modes are supported with rdxLOCK; RDX LVM mode is a roadmap item and any VTL (Tape) modes are not supported.

Q: How do you perform a BMR operation with a RDX RansomBlock volume?

A: This is depending on your backup application and Server environment but for best practice prepare a BMR RDX Media with your backup application and the Windows server incl. backup application and rdxLOCK and store the media at a secure location offline and offsite. the BMR needs to be done in two steps then. 1. Restore the Server with your backup application and rdxLOCK. 2nd restore is required with the RDX media of the desired backup that is needed for recovery. Alternatively, functional VM with rdxLOCK installation and a VM image/snapshot on RDX Media might be sufficient as well.

Sales and support for Overland-Tandberg products and solutions are available in over 90 countries.
Contact us today at sales@overlandstorage.com or sales@tandbergdata.com

©2018 Sphere 3D. 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. Sphere 3D shall not be liable for technical or editorial errors or omissions contained herein.

rdxLock_FAQ_EN_23Oct_2017