rdxLOCK Administration Guide

August 2022
10400876-005

The names of companies and individuals used in examples are fictitious and intended to illustrate the use of the software. Any resemblance to actual companies or individuals, whether past or present, is coincidental.

PROPRIETARY NOTICE

The information contained in this document is subject to change without notice.

All information contained in or disclosed by this document is considered proprietary by Overland-Tandberg. By accepting this material the recipient agrees that this material and the information contained therein are held in confidence and in trust and will not be used, reproduced in whole or in part, nor its contents revealed to others, except to meet the purpose for which it was delivered. It is understood that no right is conveyed to reproduce or have reproduced any item herein disclosed without express permission from Overland-Tandberg.

Overland-Tandberg provides this manual as is, without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Overland-Tandberg may make improvements or changes in the product(s) or programs described in this manual at any time. These changes will be incorporated in new editions of this publication.

Overland-Tandberg assumes no responsibility for the accuracy, completeness, sufficiency, or usefulness of this manual, nor for any problem that might arise from the use of the information in this manual.

FW 2.3.2 (GD)

Overland-Tandberg
4542 Ruffner Street, Suite 250
San Diego, CA 92111 USA

TEL 1.800.729.8725 (toll free)
1.858.571.5555
FAX 1.858.571.3664

Tandberg Data GmbH
Nikolaus-Groß-Straße 13
44329 Dortmund, Germany

TEL +49 231 5436 0
FAX +49 231 5436 111

OVERLAND TANDBERG

www.overlandtandberg.com

Contents

Chapter 1: Product Information

Chapter 2: Installation

Chapter 3: Configuration

Chapter 4: Best Practices

Appendix A: Troubleshooting

Appendix B: QuikStation Volume Licensing

Index

1

Product Information

rdxLOCK is a software solution that enables RDX cartridges to be used as a storage device for regulatory compliance archiving, when data must not be deleted or overwritten.

Topics in Product Information:

- Overview
- Key rdxLOCK Features
- rdxLOCK Restrictions
- rdxLOCK GUI

Overview

Applications can write data directly to a rdxLOCK protected RDX system, but are not allowed to make any modification after the data has been locked. The locking mechanism is completely controlled by rdxLOCK on a directory- or file-level basis and ensures that a file object is changed to be WORM-based on the selected protection policy. A special API is not necessary for this change.

The rdxLOCK's protection policies ensure that files can't be modified, renamed, moved, or overwritten in any way, preserving data in a non-rewritable, non-erasable manner for an infinite period of time. Additionally, rdxLOCK prevents the alteration of file attributes.

As rdxLOCK is able to use the existing server and disk storage infrastructure, an audit-compliant archive can be implemented in a cost-effective manner.

Key rdxLOCK Features

Enhanced Security Mode (ESM)

Enhanced Security Mode encrypts rdxLOCK volumes on the block level in a way that no content of the real volume is visible unless rdxLOCK is running. Instead of the real content of the NTFS volume, you see a small FAT volume as a placeholder with warning information. This also inhibits the deletion of files on rdxLOCK-protected volumes in the following cases:

- There is no rdxLOCK software installed at all.
- The rdxLOCK WORM volume has been moved to a server system which does not have rdxLOCK installed.
- The rdxLOCK file system filter has been stopped.
- The rdxLOCK software has been uninstalled from the system.

Since rdxLOCK 2.3.1, ESM is mandatory in ESM versions 6 or 7. Volumes with ESM version 5 and below are still supported but have to be migrated to ESM version 6.

Migration has to be performed using the rdxLOCK GUI. New volumes can only be created with ESM version 7 to differentiate between migrated volumes (version 6) and new created volumes (version 7). The internal ESM number is increased to prevent an older rdxLOCK version from mounting this volume.

NOTE: Run a backup of the WORM volume before changing the encryption or migrating to current ESM versions.

Verified Retention Clock (VRC)

A compliant data storage system needs a secure tamper-proof time base to measure retention periods and ensure WORM integrity.

The rdxLOCK software provides a secure and compliant retention time management process called Verified Retention Clock (VRC). This facility has to be synchronized directly after setting up the software by entering a special TimeSync key. (See TimeSync Key on page 15.)

This key contains a trusted time stamp for verifying that the system clock is in a certain range compared to UTC (Coordinated Universal Time). Only when the verification succeeds, can WORM volumes be initialized, configured, and controlled. As long as the verification has not been implemented, the system can not be used for managing WORM volumes.

All WORM volumes created by a rdxLOCK application with a non-verified system clock are marked as “TEST WORM VOLUMES” and can only be converted to valid, productive WORM volumes on systems with both a verified system clock and a valid temporary license.

After a successful system clock verification, VRC closely monitors the system clock and ensures that system clock manipulations cannot be used to delete files.

Small changes in the system clock are manageable, but when the clock is adjusted over large ranges or the system is switched off or rebooted for any reason, the result is a prolongation of retention periods. To mitigate such artificially extended retention time periods, VRC allows a drifting of the retention time offset (RTT-Offset) of up to a week per year to make up for downtimes due to system maintenance and other housekeeping events. Any longer periods of downtime beyond an acceptable value (out of bounds) need to be handled via a TimeSync key. In most cases, a new TimeSync key will need to be installed.

rdxLOCK Restrictions

- The rdxLOCK software can not be installed on systems which have any version of TrueCrypt installed.
- The rdxLOCK software supports certified removable cartridges and devices, such as RDX cartridges and devices.
- File systems other than NTFS are not supported.
- System volumes and cluster quorum disks are excluded by the configuration procedure.
- Appending data to rdxLOCK-protected files is not supported.
- Files having Extended Attributes or reparse points attached can’t be set to WORM.

- The Recycle Bin functionality can not be used on WORM volumes, since **rdxLOCK** denies the move operation to the recycle bin when an expired WORM file is selected for deletion. Therefore it is recommended to deactivate the Recycle Bin for the individual WORM volumes to make the deletion of expired WORM files possible.

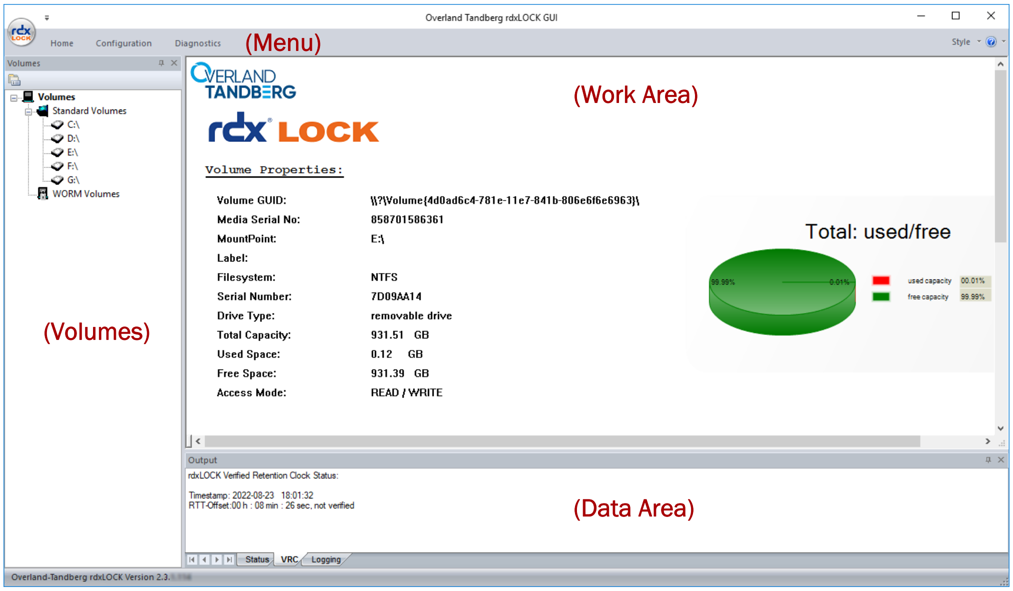
  Please note that Microsoft has redesigned the Recycle Bin behavior in Windows VISTA, Windows 2008 Server, and Windows 7. The properties of the Recycle Bin are now tied to user profiles rather than the actual disk. Therefore each user must explicitly switch off the Recycle Bin of the corresponding WORM volumes when accessing them locally for deleting expired WORM files.
- Upgrades are only supported from **rdxLOCK** version 2.1.0 Build 29 and higher.

  Previous versions need special support, so please contact your service provider.
- Read-only volumes are not supported.
- Volumes mounted inside a WORM volume are not WORM protected.
- Shrinking an ESM protected volume is not supported.
- Adding a mirror to an ESM protected volume is not supported.
- Volumes marked as “active” can not be used in ESM mode.
- Backing up an image of a single, ESM-encrypted partition on a GPT disk is not supported.

  In this case an image backup of the entire GPT disk must be created including the backup of unused sectors.

rdxLOCK **GUI**

Management of **rdxLOCK** is handled primarily through the **rdxLOCK** GUI.



Volume Properties:

Volume GUID: \\?\Volume{4d0ad6c4-781e-11e7-841b-806e6f6e6963}\
Media Serial No: 858701586361
MountPoint: E:\
Label:
Filesystem: NTFS
Serial Number: 7D09AA14
Drive Type: removable drive
Total Capacity: 931.51 GB
Used Space: 0.12 GB
Free Space: 931.39 GB
Access Mode: READ / WRITE

```
rdxLOCK Verified Retention Clock Status:

Timestamp: 2022-08-23   18:01:32
RTT-Offset:00 h : 08 min : 26 sec, not verified
```

The GUI consists of three menu items (Home, Configuration, and Diagnostics), a visual hierarchy of the volumes, a main work area, and a secondary data area.

2

Installation

This section covers the installation of the rdxLOCK software.

NOTE: Administrative rights are required to install, configure, license, update, and set policies and retention times for **rdxLOCK**. When installing **rdxLOCK**, you need to be logged in as Administrator or run the installation program using the **Run as administrator** context menu option.

Topics in Installation:

- Install rdxLOCK
- Post-Installation Actions
- Uninstall rdxLOCK

Install rdxLOCK

When installing rdxLOCK, you can use either a “silent” mode or the normal Windows process.

Installation Preparation

1. Close **all applications** running on the system.
2. Copy the rdxLOCK executable program (`rdxLOCKSetup_<version#>.zip`) to your Windows system and note its location.
3. Go to the file location and unzip the **downloaded file**.

Silent Mode

You can run rdxLOCK setup executable in a “silent” mode. This applies to new installations and updates. In “silent” mode the rdxLOCK setup runs automatically with default settings (with installing ESM) automatically and, if wanted, in the background. If it is not deselected, a reboot is performed after setup.

The “silent” setup is started in CMD with following parameters:

/SILENT	automatically, status dialogs are still displayed, reboot needs to be acknowledged
/VERYSILENT	automatically, completely in the background, reboot if not disabled.
/NORESTART	the reboot is deselected (only with a “silent” mode)

Example:

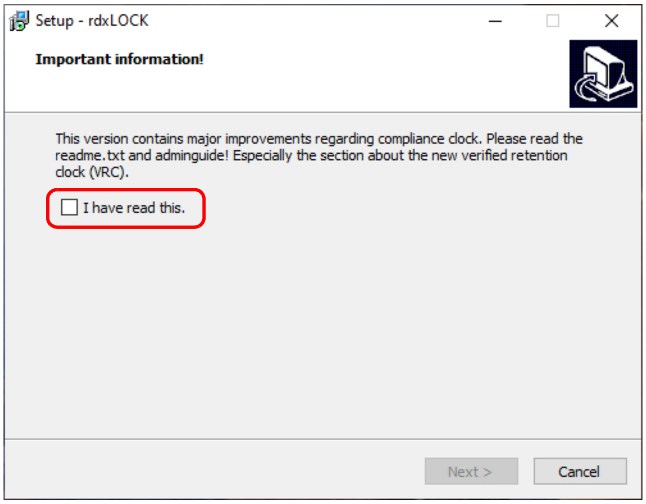
```
rdxLOCKSetup_<version#>.exe /SILENT /NORESTART
```

Install rdxLOCK Procedure

To install rdxLOCK using the wizard:

1. Run the **rdxLOCK** program to start the installation wizard.
2. At the Important Information screen, check the **I have read this** box and click **Next.**

   You must confirm you have read the information to continue.



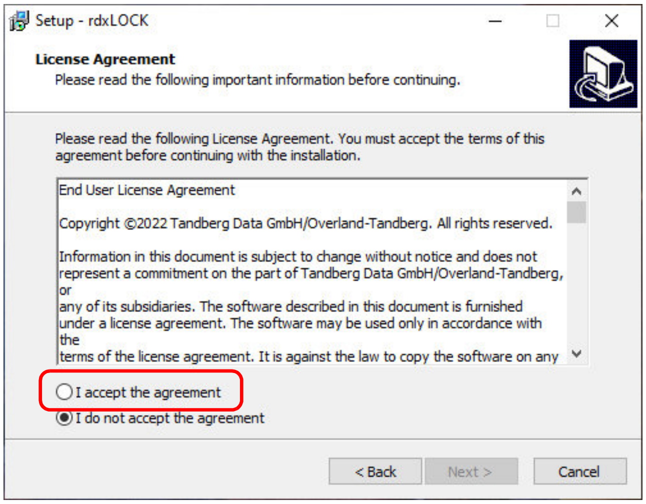
Important information!

This version contains major improvements regarding compliance clock. Please read the readme.txt and adminguide! Especially the section about the new verified retention clock (VRC).

□ I have read this.

3. At the License Agreement, if you agree with the terms, select **I accept the agreement** and click **Next**.

   You must accept the license agreement to continue.



License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

End User License Agreement

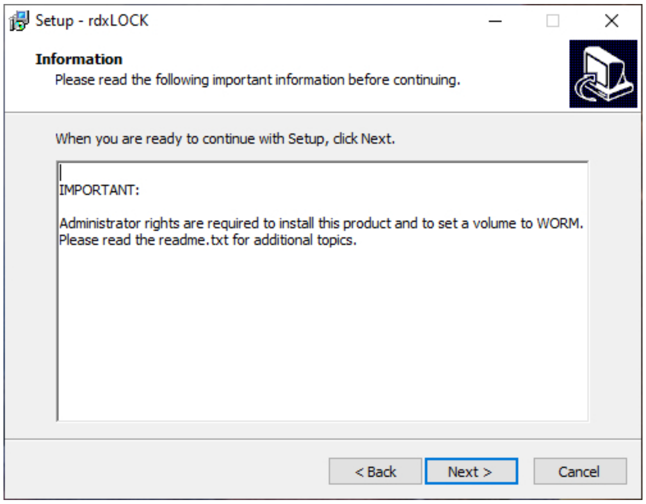
Copyright ©2022 Tandberg Data GmbH/Overland-Tandberg. All rights reserved.

Information in this document is subject to change without notice and does not represent a commitment on the part of Tandberg Data GmbH/Overland-Tandberg, or
any of its subsidiaries. The software described in this document is furnished under a license agreement. The software may be used only in accordance with the
terms of the license agreement. It is against the law to copy the software on any

○ I accept the agreement

● I do not accept the agreement

4. At the information regarding administrator rights, after reading, click **Next**.



Information

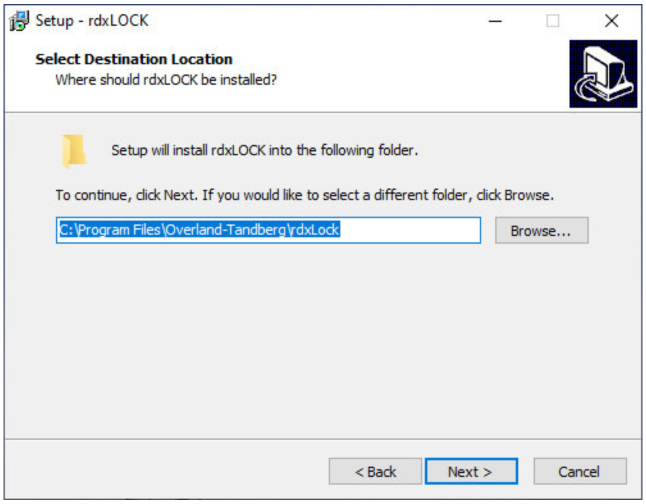
Please read the following important information before continuing.

When you are ready to continue with Setup, click Next.

IMPORTANT:

Administrator rights are required to install this product and to set a volume to WORM.
Please read the readme.txt for additional topics.

5. At the **Select Destination Location** screen, either accept the default location or, using the **Browse** button, select the folder where you want to install **rdxLOCK**, and then click **Next**.



Select Destination Location

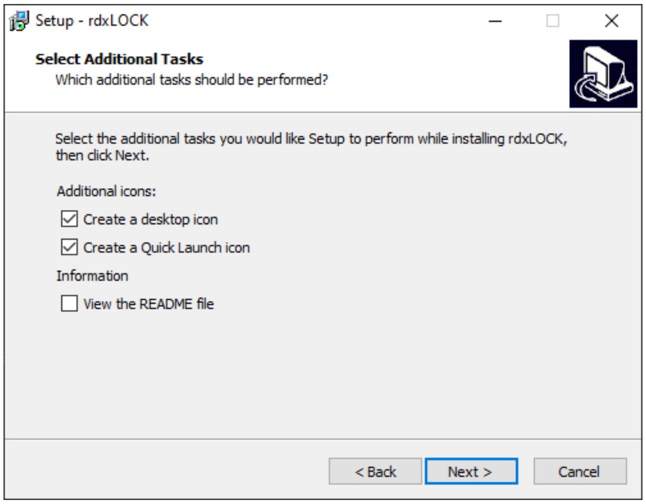
Where should rdxLOCK be installed?

Setup will install rdxLOCK into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files\Overland-Tandberg\rdxLock

6. At the **Select Additional Tasks** window, choose the tasks you want and click **Next**.



Select Additional Tasks

Which additional tasks should be performed?

Select the additional tasks you would like Setup to perform while installing rdxLOCK, then click Next.

Additional icons:

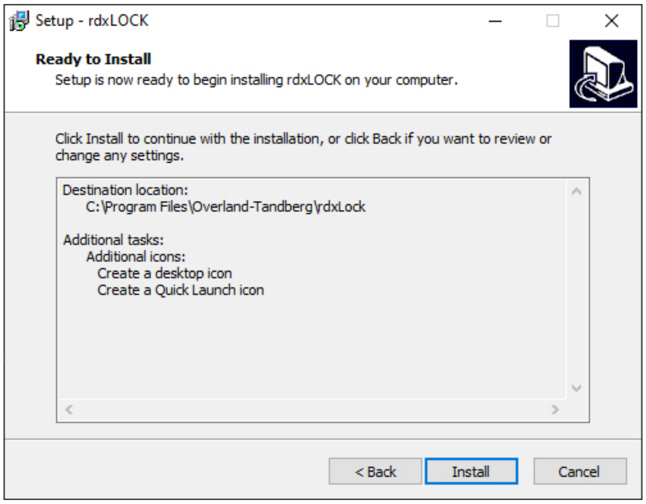
☑ Create a desktop icon

☑ Create a Quick Launch icon

Information

☐ View the README file

7. At the **Ready to Install** screen, verify the settings and click **Install**.



Setup - rdxLOCK

Ready to Install

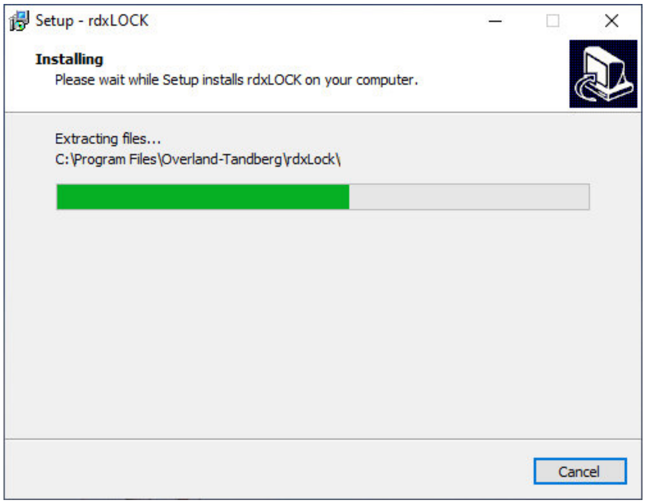
Setup is now ready to begin installing rdxLOCK on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

```
Destination location:
    C:\Program Files\Overland-Tandberg\rdxLock

Additional tasks:
    Additional icons:
      Create a desktop icon
      Create a Quick Launch icon
```

The **rdxLOCK** software is installed in the selected destination folder.



Setup - rdxLOCK

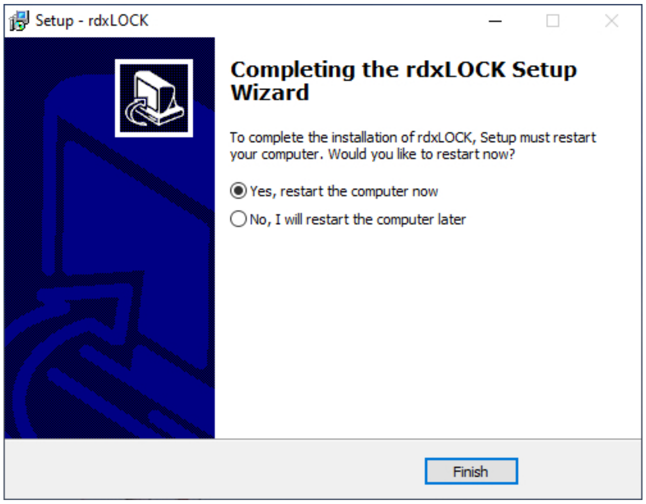
Installing

Please wait while Setup installs rdxLOCK on your computer.

Extracting files...
C:\Program Files\Overland-Tandberg\rdxLock\

8. At the final Wizard screen, choose to restart the computer now or later and click **Finish** to complete the installation.

   The computer must be restarted for **rdxLOCK** to function.



Setup - rdxLOCK

Completing the rdxLOCK Setup Wizard

To complete the installation of rdxLOCK, Setup must restart your computer. Would you like to restart now?

● Yes, restart the computer now

○ No, I will restart the computer later

Post-Installation Actions

Once the **rdxLOCK** is up and running, perform the following actions as required.

System Clock Verification

After a new installation or an upgrade from versions prior to 2.2.6, the system clock needs to be verified by a TimeSync key (see TimeSync Key on page 15).

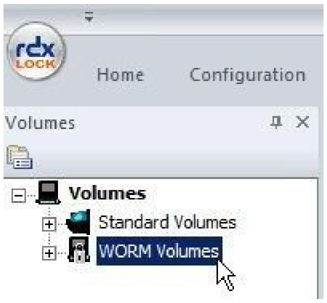
Until the system clock is verified by TimeSync, the following restrictions exist:

- New Volumes are created as WORM test volumes that cannot be converted to regular volumes and become read-only after 60 days.
- WORM volumes created by **rdxLOCK** versions prior to 2.2.6 or previous are put into READ- ONLY mode and are not switched to the regular WORM mode until the TimeSync verification has succeeded.

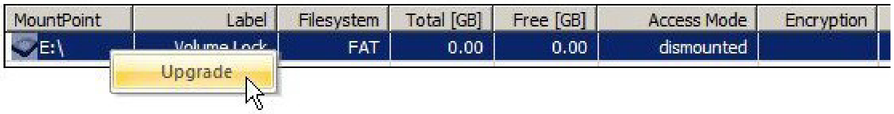
Existing WORM Volumes Upgrade

After an upgrade from **rdxLOCK** versions prior to 2.3.1, all your WORM volumes need to be upgraded.

1. Start the **rdxLOCK** and select **WORM Volumes**.



2. Right-click a WORM volume and click **Upgrade**.



MountPoint	Label	Filesystem	Total [GB]	Free [GB]	Access Mode	Encryption
E:\	Volume Lock	FAT	0.00	0.00	dismounted	

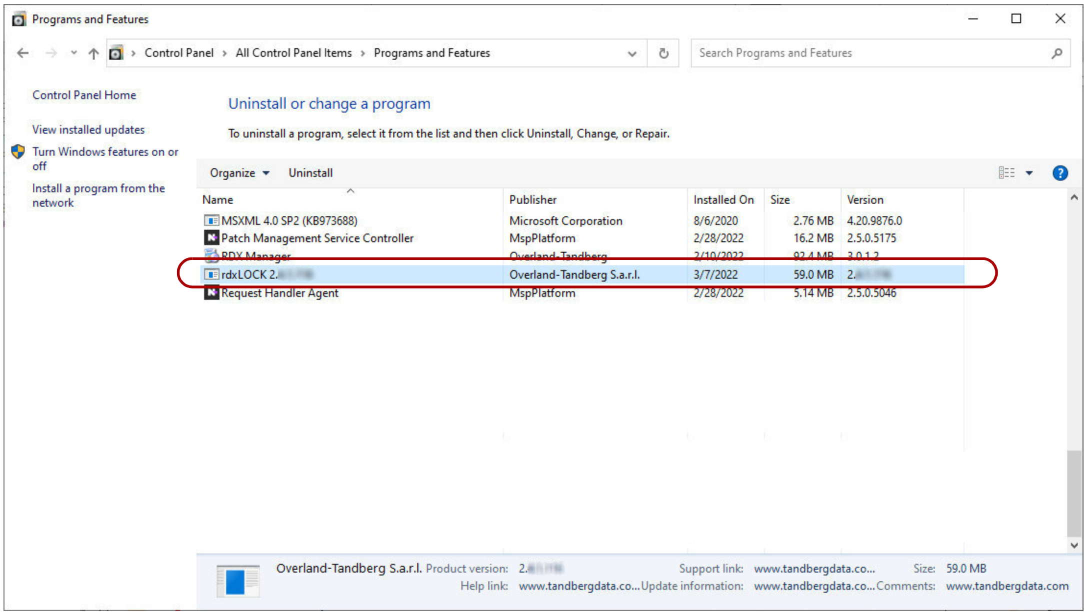
NOTE: Upgraded Volumes can no longer be read by prior versions.

Uninstall rdxLOCK

NOTE: You must exit **rdxLOCK** before it can be uninstalled.

You can uninstall **rdxLOCK** using the Windows Software Manager:

1. Click **Start > Control Panel > Programs and Features**.
2. From the list of programs, select the **rdxLOCK** software and click **Uninstall** (or **Remove**).



Programs and Features
Control Panel > All Control Panel Items > Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Install a program from the network
Organize
Uninstall

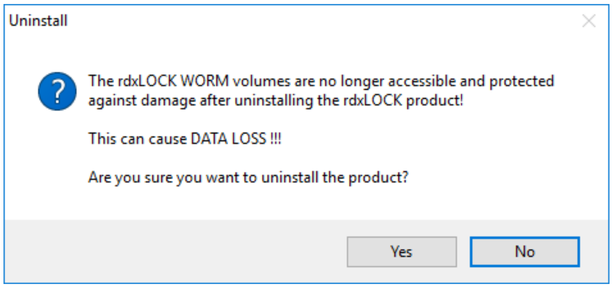
Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed On	Size	Version
MSXML 4.0 SP2 (KB973688)	Microsoft Corporation	8/6/2020	2.76 MB	4.20.9876.0
Patch Management Service Controller	MspPlatform	2/28/2022	16.2 MB	2.5.0.5175
RDX Manager	Overland-Tandberg	2/10/2022	92.4 MB	3.0.1.2
rdxLOCK 2.[redacted]	Overland-Tandberg S.a.r.l.	3/7/2022	59.0 MB	2.[redacted]
Request Handler Agent	MspPlatform	2/28/2022	5.14 MB	2.5.0.5046

Overland-Tandberg S.a.r.l. Product version: 2.[redacted] Support link: www.tandbergdata.co... Size: 59.0 MB
Help link: www.tandbergdata.co... Update information: www.tandbergdata.co... Comments: www.tandbergdata.com

3. At the first conformation screen, click **Yes**.

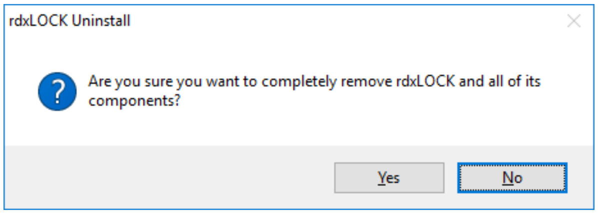


The rdxLOCK WORM volumes are no longer accessible and protected against damage after uninstalling the rdxLOCK product!

This can cause DATA LOSS !!!

Are you sure you want to uninstall the product?

4. At the second conformation screen, click **Yes** again.

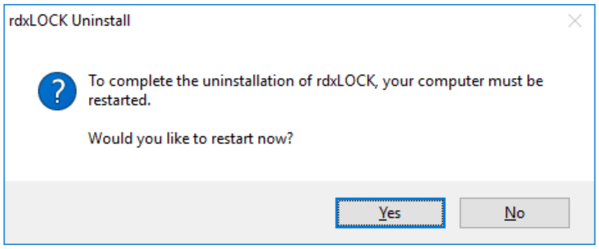


rdxLOCK Uninstall

Are you sure you want to completely remove rdxLOCK and all of its components?

During uninstall, a status screen shows the progress.

5. Due to the Enhanced Security Mode, a reboot is required to completely remove **rdxLOCK** from your system; click **YES**.



rdxLOCK Uninstall

To complete the uninstallation of rdxLOCK, your computer must be restarted.

Would you like to restart now?

⚠ CAUTION: If you remove the **rdxLOCK** product from your system, you will not be able to access WORM-committed files anymore.

In addition, due to the Enhanced Security Mode applied to a WORM volume, the WORM NTFS file system is hidden and inaccessible after uninstalling the **rdxLOCK** product.

3 Configuration

This section focuses on the setup and configuration of newly installed rdxLOCK software.

Topics in Configuration:

- TimeSync Key
- WORM Volume Setup
- Protection Policies and Retention Periods
- License Keys

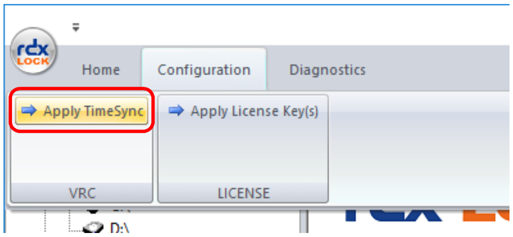
TimeSync Key

A TimeSync key is used to verify that the system clock is in a certain range compared to UTC and therefore ensures that file retention times are managed in a safe and secure fashion.

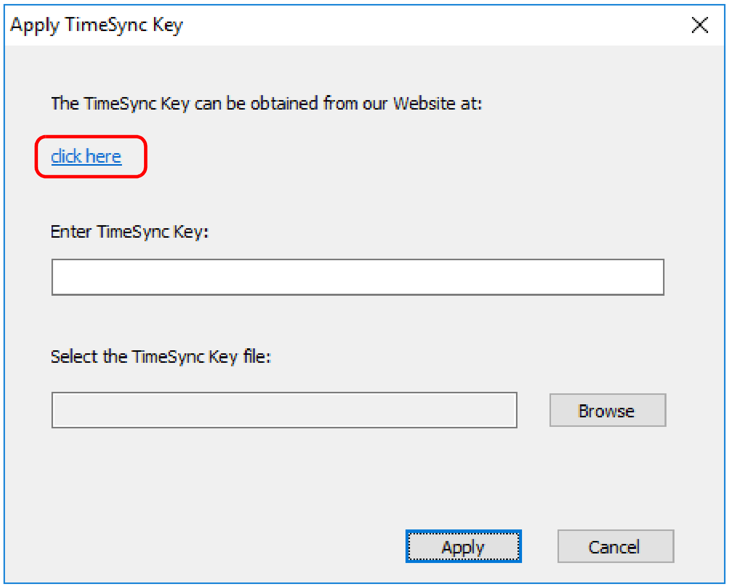
Once the TimeSync key verification process succeeds, the system is ready for handling WORM volumes. Every additional TimeSync operation resets the internal "corrective retention time offset" parameter (RTT-Offset). rdxLOCK maintains this RTT-Offset to manage the time offset between the system clock and the Verified Retention Clock (VRC). These offsets occur due to normal situations like the system being powered down or potentially abnormal situations where the system clock is changed or potentially rolled back.

To apply a TimeSync key:

1. Start the rdxLOCK GUI application.
2. Select the menu item **Configuration > Apply TimeSync**.



3. Click the **click here** link.



Apply TimeSync Key

The TimeSync Key can be obtained from our Website at:

click here

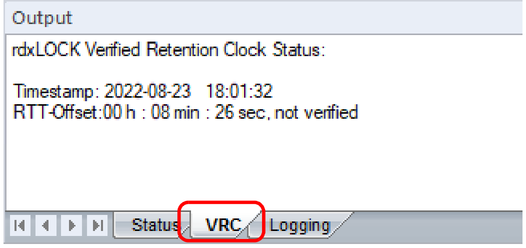
Enter TimeSync Key:

Select the TimeSync Key file:

4. Copy the **TimeSync key string** from the webpage directly to the corresponding dialog's input field and press **Apply**.

   Alternatively, you can save the key to a file first and then select that file for applying the TimeSync key using **Browse**.

NOTE: This can take up to 2 minutes (until the system clock gets verified). VRC information is displayed in the output panel view called "VRC" of the rdxLOCK GUI application.



Output

```
rdxLOCK Verified Retention Clock Status:

Timestamp: 2022-08-23   18:01:32
RTT-Offset:00 h : 08 min : 26 sec, not verified
```

WORM Volume Setup

For converting an NTFS volume to a WORM volume, use the rdxLOCK GUI to open the **Properties** page of the appropriate volume. Alternatively, you can use Windows Explorer or Disk Management.

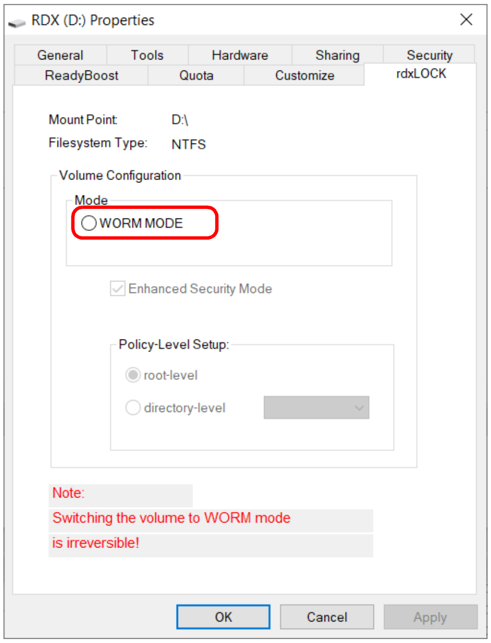
NOTE: This approach can only be used if you are logged in as the local administrator or as a domain administrator with special security options.

1. Run the rdxLOCK program, right-click the appropriate volume in the table, and select **Configure**.

   If you are logged in as a standard user, who is not a member of the local administrator group, you will get an UAC prompt for entering the administrator's password to run the program with full elevated rights and privileges as an administrator.

2. Select the rdxLOCK tab.

3. Click **WORM MODE** to select it.



Mount Point: D:\
Filesystem Type: NTFS

Volume Configuration

Mode

○ WORM MODE

☑ Enhanced Security Mode

Policy-Level Setup:

● root-level

○ directory-level

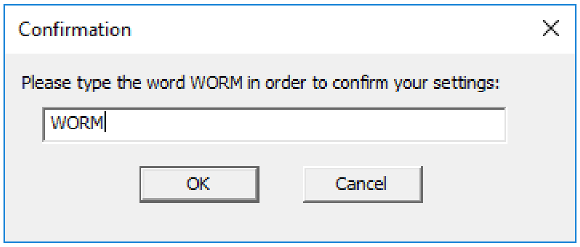
Note:
Switching the volume to WORM mode
is irreversible!

CAUTION: Switching the volume to WORM mode is irreversible! While the cartridge can be reformatted on a system without **rdxLOCK**, all data will be lost.

The **Policy Level Setup** is automatically set to **root level** and **Enhanced Security Mode** (ESM) is activated.

IMPORTANT: Under Enhanced Security Mode, data on the volume will be encrypted after confirmation. The RDX cartridge volume must be almost empty for it to be converted and used with WORM. Too much data on it causes an error.

4. Click **OK** to save the settings.
5. At the Confirmation screen, type **`WORM`** (all caps) and click **OK**.

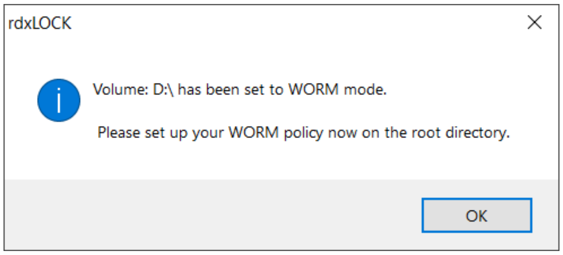


Please type the word WORM in order to confirm your settings:

WORM

NOTE: Enhanced Security Mode encryption can be activated on a WORM volume at any time, but cannot be switched off after its activation.

6. At the screen indicating that the WORM mode is set, click OK.

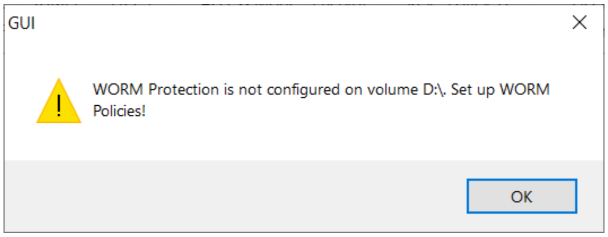


rdxLOCK

Volume: D:\ has been set to WORM mode.

Please set up your WORM policy now on the root directory.

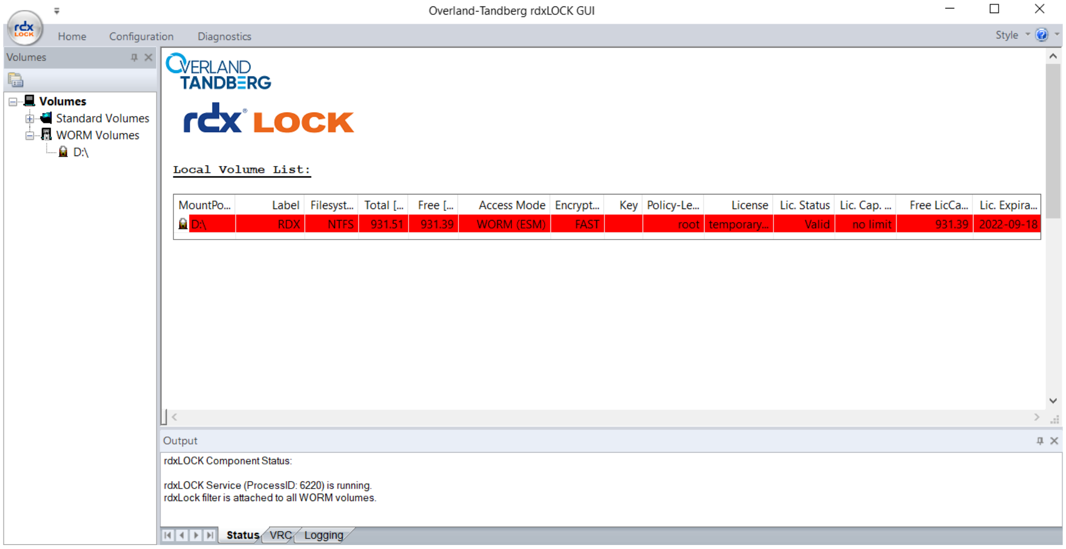
7. At the WORM Protection not configured message, click OK.



GUI

WORM Protection is not configured on volume D:\. Set up WORM Policies!

The drive is moved to the WORM Volumes list on the left and is highlighted in red.



Local Volume List:

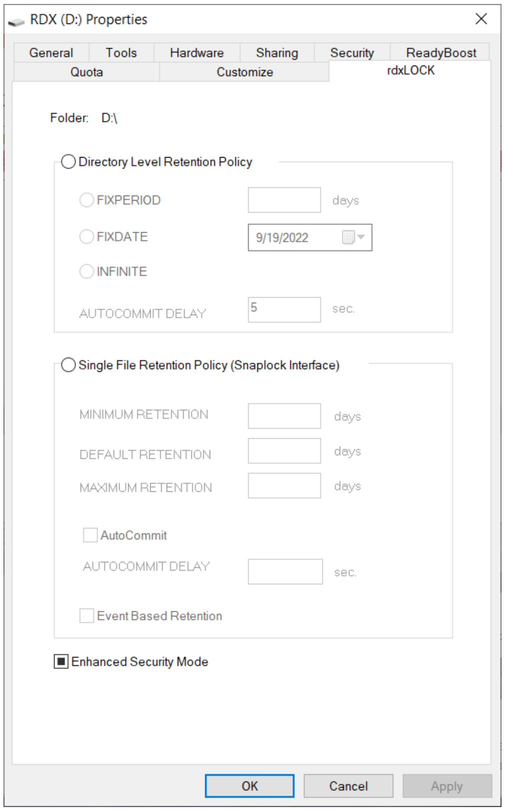
MountPo...	Label	Filesyst...	Total [...	Free [...	Access Mode	Encrypt...	Key	Policy-Le...	License	Lic. Status	Lic. Cap. ...	Free LicCa...	Lic. Expira...
D:\	RDX	NTFS	931.51	931.39	WORM (ESM)	FAST		root	temporary...	Valid	no limit	931.39	2022-09-18

Output

```
rdxLOCK Component Status:

rdxLOCK Service (ProcessID: 6220) is running.
rdxLock filter is attached to all WORM volumes.
```

If you right-click the drive and select **Configure**, the rdxLOCK tab information changes to show unconfigured options.



Folder: D:\

○ Directory Level Retention Policy

○ FIXPERIOD days

○ FIXDATE 9/19/2022

○ INFINITE

AUTOCOMMIT DELAY 5 sec.

○ Single File Retention Policy (Snaplock Interface)

MINIMUM RETENTION days

DEFAULT RETENTION days

MAXIMUM RETENTION days

□ AutoCommit

AUTOCOMMIT DELAY sec.

□ Event Based Retention

■ Enhanced Security Mode

Protection Policies and Retention Periods

After a volume has been configured for WORM, protection policies should then be defined on the root directory. WORM policies must be configured as they are required for WORM to function. All subdirectories created under the configured root directory inherit the same configured policies.

Definition of key terms:

- **Directory-Level Retention** (DLR) – Retention periods are related to directories, not to single files. All files in a certain directory and all sub-directories are treated the same way.
- **Single File Retention** (SFR) – Retention periods are related to individual files.
  - **Auto-Commit Mode** – Files written into a certain location are committed to be WORM after a defined period of time (AUTOCOMMIT DELAY) by the rdxLOCK software. (No application activity is needed.)
  - **Application-Commit Mode** – Files written into a certain location are NOT committed to be WORM without application activities. To set files to WORM status, the application has to follow the SnapLock procedure and set the read-only flag for the file or directory.

Directory-Level Retention (DLR)

The DLR policy always uses the Auto-commit mode which means all files are set to WORM after the Auto-commit delay period. No file stays as a non-WORM status in such folders.

Single File Retention (SFR)

By setting the read-only attribute of the file, the WORM-commit operation is either triggered automatically by **rdxLOCK** (Auto-commit mode) or a third-party application (Application-commit mode).

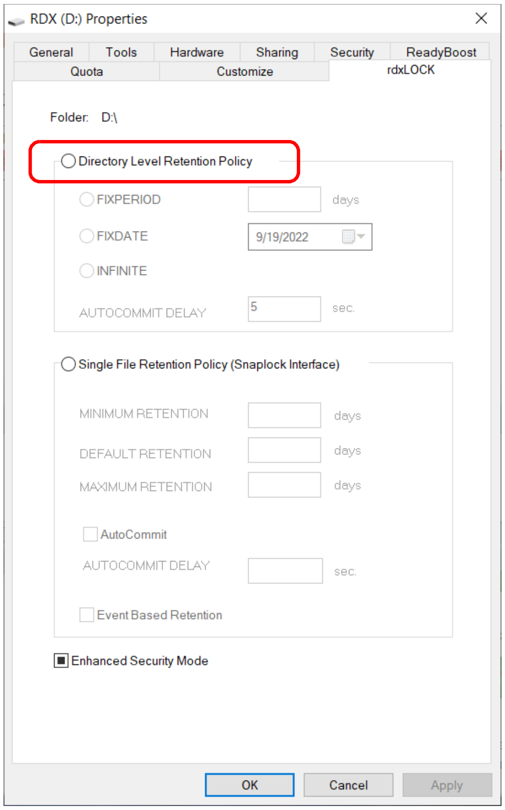
When the Application-Commit Mode is active, files MUST be set to read-only either manually or by an application to activate the WORM protection. If the file's read-only attribute is not set, the file remains unprotected.

NOTE: The retention period for an RDX WORM volume is set to **Infinite** for both DLR and SFR.

rdxLOCK Directory-Level Retention Policy

The **rdxLOCK** DLR policy automatically commits files to WORM after their creation, however the WORM trigger can be delayed by a value that is configured for the "AUTOCOMMIT DELAY" parameter. This value can be set between 0 and 3,000,000 seconds (~ 34.7 days). The value can be modified at any time (increase/decrease) to fit to your needs.

To configure the DLR policy, right-click the appropriate WORM drive in the **rdxLOCK** GUI and select **Configure**.



Folder: D:\

○ Directory Level Retention Policy

○ FIXPERIOD days

○ FIXDATE 9/19/2022

○ INFINITE

AUTOCOMMIT DELAY 5 sec.

○ Single File Retention Policy (Snaplock Interface)

MINIMUM RETENTION days

DEFAULT RETENTION days

MAXIMUM RETENTION days

□ AutoCommit

AUTOCOMMIT DELAY sec.

□ Event Based Retention

■ Enhanced Security Mode

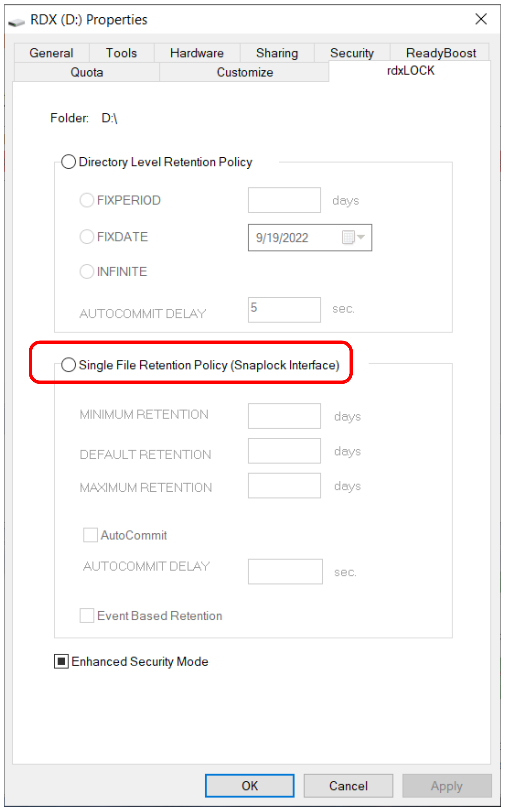
These rules apply to WORM files covered by a **rdxLOCK** DLR policy:

- WORM files cannot be modified, overwritten, renamed, or deleted.
- WORM files cannot be changed back to non-WORM files.

- Security settings (ACL) on WORM files can not be changed any more. Therefore, we recommend to always using security groups in order to be able to change security for single users by adding or removing them from the assigned group.

rdxLOCK **Single File Retention Policy**

The rdxLOCK SFR policy provides compatibility with applications using the SnapLock interface to write data to a NetApp filer or similar systems.



Folder: D:\

○ Directory Level Retention Policy

○ FIXPERIOD days

○ FIXDATE 9/19/2022

○ INFINITE

AUTOCOMMIT DELAY 5 sec.

○ Single File Retention Policy (Snaplock Interface)

MINIMUM RETENTION days

DEFAULT RETENTION days

MAXIMUM RETENTION days

□ AutoCommit

AUTOCOMMIT DELAY sec.

□ Event Based Retention

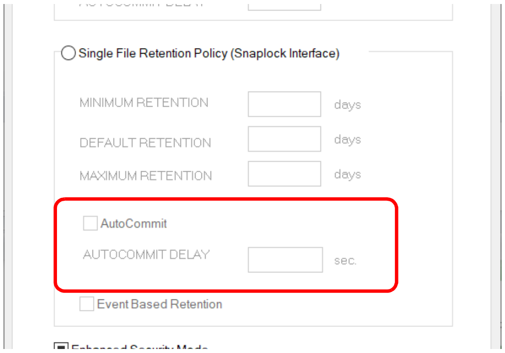
■ Enhanced Security Mode

All retention options are automatically set to **INFINITE**.

The following steps are necessary to convert a file to WORM when using the rdxLOCK SFR policy without the **AutoCommit** feature enabled.

1. Copy a writable file to a directory which is covered by the SFR policy.
2. Setting the read-only attribute of the file.
   This triggers the WORM commit operation.

If the **AutoCommit** feature is enabled, after files have not been modified for a specified period of time (**AUTOCOMMIT DELAY**), the files are automatically converted to WORM state.



○ Single File Retention Policy (Snaplock Interface)

MINIMUM RETENTION		days
DEFAULT RETENTION		days
MAXIMUM RETENTION		days

□ AutoCommit

AUTOCOMMIT DELAY sec.

□ Event Based Retention

These rules apply to WORM files covered by a rdxLOCK SFR policy:

- WORM files can not be modified, overwritten, renamed or deleted.
- WORM files can not be changed back to non-WORM files.
- The retention period for an RDX WORM volume is set to Infinite.
- Since the expiration date of a WORM file is stored in its last-access time stamp attributes, the last-access time stamp is not updated on a read access as on a standard NTFS file system.
- Security settings (ACL) on WORM files can not be changed any more.

  We recommend to always using security groups in order to be able to change security for single users by adding or removing them from the assigned group.

The following rules apply to both RDX WORM policies:

- RDX WORM policies are configured on the root level.
- When configuring protection policies on the directory level, it is not mandatory to assign a WORM policy to each folder in this hierarchy.
- Directories containing WORM files cannot be renamed.
- New created directories can be renamed within the “AUTOCOMMIT-DELAY” time period after their creation (or within 60 seconds if the Auto-commit feature is disabled).

License Keys

NOTE: A permanent license key can only be requested on an system with a Verified Retention Clock installed. See Verified Retention Clock (VRC) on page 6.

The rdxLOCK software includes a trial license that allows each volume to be used for 60 days after they are configured as WORM. While the trial license does not have a capacity limit and is not limited to a specific number of volumes, you must register those volumes to obtain a permanent license if you want to use them past the 60-day trial period.

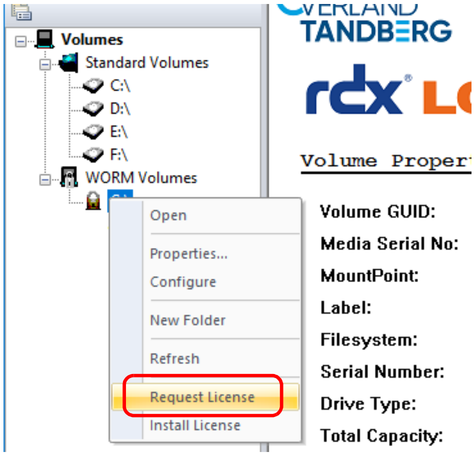
NOTE: Access to all WORM volumes on a system with an expired trial license will be denied.

To obtain a permanent license key, each WORM volume must be registered separately using both the Capacity ID provided with the RDX cartridge and the cartridge’s serial number. The license key you receive is then used to generate the permanent license for that specific cartridge’s capacity and is linked to that cartridge’s serial number.

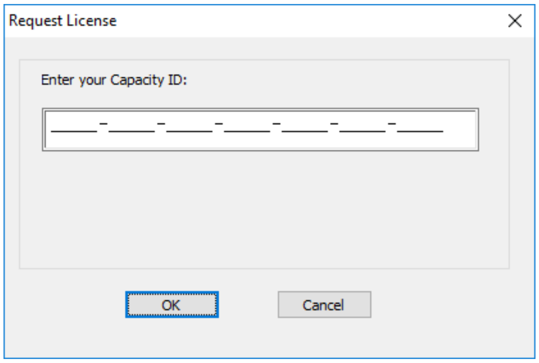
IMPORTANT: To use rdxLOCK with the RDX Logical Volumes feature on a QuikStation system, a special multiple-media license must be obtained from Overland-Tandberg Technical Support. See Appendix B, "QuikStation Volume Licensing," for details.

To obtain and install a permanent license:

1. In the Windows Start menu, select **Programs > rdxLOCK > rdxLOCK GUI**.
2. From the **WORM Volumes** list, right-click the **specific WORM volume drive letter** for which you want to request a permanent license.
3. From the volume's context menu, select **Request License**.



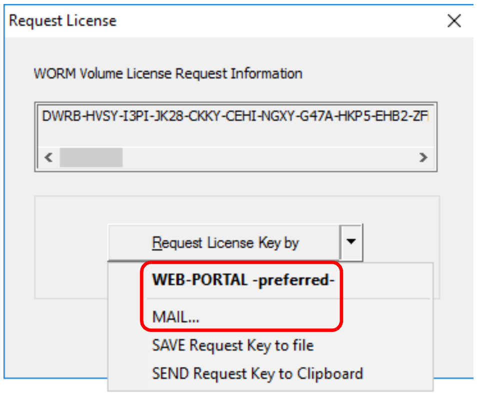
4. At the **Request License** screen, enter the **Capacity ID** which was provided with your RDX cartridge or rdxLOCK license.



Characters are automatically converted to uppercase letters if lowercase letters are entered.

5. Click **OK** to generate the WORM Volume License Request Information.

6. Send the **request** to the licensing service using either the online WEB-PORTAL option (recommended) or via email.


Request License
WORM Volume License Request Information
DWRB-HVSY-I3PI-JK28-CKKY-CEHI-NGXY-G47A-HKP5-EHB2-ZF
Request License Key by
WEB-PORTAL -preferred-
MAIL...
SAVE Request Key to file
SEND Request Key to Clipboard

- **WEB-PORTAL Option**:

  NOTE: When using the WEB- PORTAL option, your server MUST be connected to the internet.

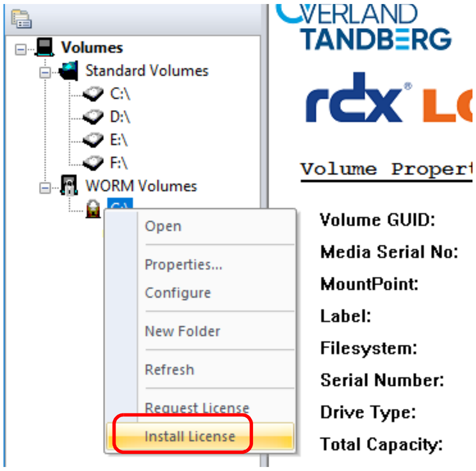
  Use the drop-down menu item WEB-PORTAL to launch your browser and access the WEB-PORTAL. Log into the WEB-PORTAL and follow the steps online to acquire the license key file. If you do not yet have login access, you need to register and provide a valid email address. The licensing service then responds back to you using that email address.

- **Email Option:**

  Use the drop-down menu item MAIL to launch your email client and automatically generate an email with the necessary information. Copy the WORM Volume License Request Information to a text file and send it as an email attachment to supportEMEA@tandbergdata.com.

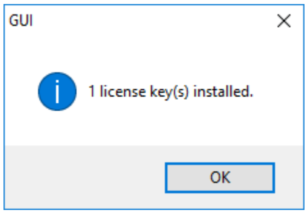
7. After receiving the email with the permanent license key file, save the file to an easy-to-access location.

8. In the rdxLOCK GUI, right-click the **volume letter** and select **Install License** from the context menu.



9. Browse to the **permanent license key file** and click **Open** to activate the license.

10. At the successful installation message, click **OK**.

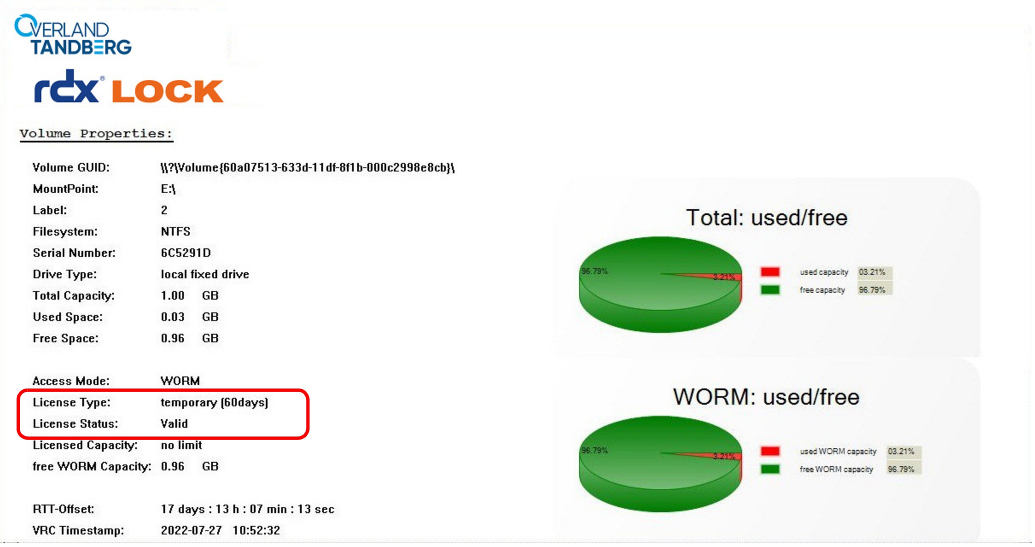


GUI

1 license key(s) installed.

11. Check the license type and status on the right-side pane of the **rdxLOCK** GUI.

It can take up to four (4) minutes before the license status is updated.



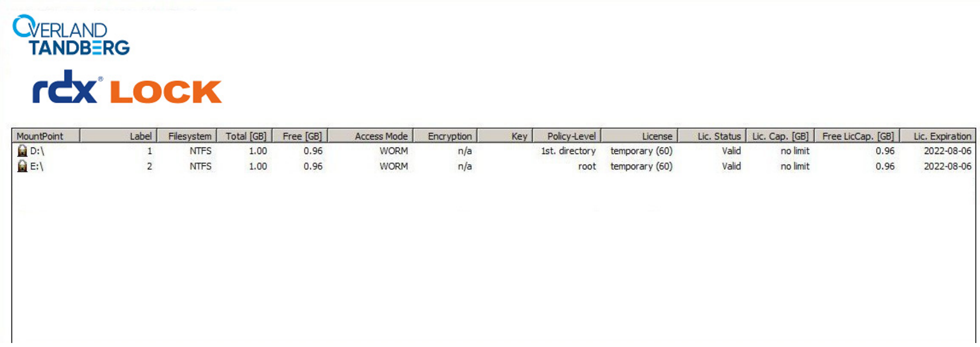
Volume Properties:

Volume GUID:	\\?\Volume{60a07513-633d-11df-8f1b-000c2998e8cb}\
MountPoint:	E:\
Label:	2
Filesystem:	NTFS
Serial Number:	6C5291D
Drive Type:	local fixed drive
Total Capacity:	1.00 GB
Used Space:	0.03 GB
Free Space:	0.96 GB
Access Mode:	WORM
License Type:	temporary (60days)
License Status:	Valid
Licensed Capacity:	no limit
free WORM Capacity:	0.96 GB
RTT-Offset:	17 days : 13 h : 07 min : 13 sec
VRC Timestamp:	2022-07-27 10:52:32

After you have installed a permanent license, you can still add additional WORM capacity to a WORM volume with add-on licenses. Add-on license keys are also installed using the **Install License** option in volume's context menu.

The **rdxLOCK** software monitors the capacity on each WORM volume and displays a warning message in the **rdxLOCK** event log when a WORM volume nears its capacity limit. If the capacity limit is exceeded, write operations on the volume are denied until additional WORM capacity is licensed for the volume.

Volume Properties in the **rdxLOCK** GUI provides an overview of the installed license types, statuses, and used/free WORM capacities.



MountPoint	Label	Filesystem	Total [GB]	Free [GB]	Access Mode	Encryption	Key	Policy-Level	License	Lic. Status	Lic. Cap. [GB]	Free LicCap. [GB]	Lic. Expiration
D:\	1	NTFS	1.00	0.96	WORM	n/a		1st. directory	temporary (60)	Valid	no limit	0.96	2022-08-06
E:\	2	NTFS	1.00	0.96	WORM	n/a		root	temporary (60)	Valid	no limit	0.96	2022-08-06

Permanent License Reuse

Once you obtain a permanent WORM license to use on a specific RDX cartridge, that license is stored on the RDX cartridge itself. If you delete the license by either erasing, reformatting, repartitioning, or, in any other way, changing the cartridge and its metadata, the license is deleted. However, the license can be regenerated and reused on that same cartridge by just re-registering the RDX cartridge using the same Capacity ID and serial number to get a new key.

To reuse your existing license:

1. On a system that does NOT have rdxLOCK installed, **reformat** the RDX cartridge using Windows.

   You can use your existing system only if rdxLOCK has been completely uninstalled including the removal of the Enhance Security Module (ESM). When you are done reformatting the cartridge, reinstall the rdxLOCK software.

2. On an rdxLOCK system, use the **normal licensing procedure** to request a permanent license key for the cartridge.

   Use the same Capacity ID and serial number to generate the WORM Volume License Request Information. Refer to License Keys on page 22.

3. Send the **request** via WEB-PORTAL or email.

4. Install the **new permanent license key** you receive.

The cartridge is now ready to reuse on your rdxLOCK system.

4

Best Practices

RDX WORM cartridge includes a 60-day trial rdxLOCK software license linked to the RDX cartridge and its capacity.

RDX WORM cartridge should be used with Enterprise Content Management (ECM) systems, Document Management Systems (DMS), Finance Data, Data Logging, Patient Files (such as PACS), Documentation, and Video and Voice recordings since it helps you meet compliance requirements for electronically stored data.

Topics in Product Information:

- Filter Compatibility
- Data Protection Strategies

Filter Compatibility

IMPORTANT: It is strongly recommended to exclude all rdxLOCK WORM volumes from automatic antivirus scans. Any attempt to quarantine WORM-committed files may lead to unexpected behavior.

The rdxLOCK software was successfully tested in combination with the following third-party applications:

- Symantec Antivirus Version
- McAfee VirusScan Enterprise
- TrendMicro ServerProtect
- Microsoft Defender

NOTE: Compatibility of rdxLOCK with any antivirus solution named above is subject to change. rdxLOCK may not work with recent versions.

For last-minute information regarding any limitations and known problems, read the `ReadMe.txt` file.

Data Protection Strategies

The following data protection strategy is available for rdxLOCK WORM volumes.

Backup / Restore

In order to meet regulatory compliance rules and preserve the WORM aspects of the original files, you must use Full Image Backup for protecting your WORM volumes.

In case of a WORM volume recovery, you also have to use a Full Image Restore to preserve the WORM functionality and meet the regulatory compliance rules.

File-based restores are not WORM compliant.

A suitable image backup and restore solution should provide the following features:

- Reliability
- Online image backup
- Creating a consistent image backup of a WORM volume while the volume is available to other system applications is mandatory.
- Differential or incremental online image backup
- Differential or incremental image backup speeds up the image backup process and saves disk space, since only files which have been changed since the last (full) backup need to be backed up.
- Network support
- Image files can be saved directly to internal and network drives.
- Configurable image file sizes
- The solution should allow specifying a maximum size for the disk image files.
- Support of volumes larger than 2 TB (GPT disk)
- Command line support
- This functionality is needed for automating backup and restore procedures.
- Optional Compression mode
- Optional Data Encryption

A

Troubleshooting

This appendix provides information on rdxLOCK error codes and some troubleshooting steps.

Topics in Troubleshooting:

Reporting a Problem

For technical assistance with a registered version of rdxLOCK, email your inquiries to supportEMEA@tandbergdata.com.

Include the following information in your email when you report a rdxLOCK issue:

- Issue description.
  - Provide symptoms of the issue.
  - When did the issue occur?
  - Which activities have caused the issue?
  - Which file objects are affected by the issue?
- A copy of the rdxLOCK Service Report.

  The rdxLOCK automatically generates a Service Report by selecting **Diagnostics > Generate Service Report.** All service information is stored in the file `rL_Diag.zip`, which is located in the directory:

  ```
  <rdxLOCK_install_dir_name>\Diagnostics
  ```
- A list of third-party-applications installed on your system, including antivirus scanners and backup management applications.

rdxLOCK Tab Not Available on Explorer's Property Page

The rdxLOCK tab on the Windows Explorer's property page is only available for local or domain administrators.

For rdxLOCK running on Windows 2012 R2 Server Standard & Enterprise Edition, 64-bit, Microsoft Failover Cluster Support, Windows 2016 Server (Microsoft Failover Cluster currently not supported), and Windows 2019 Server (Microsoft Failover Cluster currently not supported), set up the User Account Control accordingly:

- If the built-in domain administrator account is used for configuring rdxLOCK, the local security policy **User Account Control: Admin Approval Mode for the Built-in Administrator Account** must be disabled.

- If another domain administrator account other than the built-in domain administrator is used for configuration, the local security policy **User Account Control: Run all administrators in Admin Approval Mode** must be disabled.

Application Event Log Message: "Invalid license"

An invalid license may result from the following conditions:

- Temporary license has expired.
- License information can't be read on the WORM volume. Check if the **rdxLOCK** service is running.
- WORM volume has been restored. In this case, a new, permanent license must be requested.

TimeSync Out Of Bounds

An RTT-Offset (retention time offset) of up to a week per year between the system clock and the Verified Retention Clock (VRC) are allowed to make up for downtimes due to system maintenance and other housekeeping events.

However, when the clock is adjusted over large ranges or the system is switched off or rebooted for any reason, the result is a prolongation of retention periods. Also, the deletion of files before they expire can result in a prolongation of retention periods when the system clock is changed.

Any longer periods of downtime beyond an acceptable value (out of bounds) need to be handled via a TimeSync key. In most cases, a new TimeSync key will need to be installed.

B

QuikStation Volume Licensing

Single Licensing

Normal rdxLOCK licensing only supports the RDX Removable Disk mode at the single cartridge level. If you want to use logical volumes and expand the capacity over several RDX cartridges such as with QuikStation, you need a special multiple-media license.

Logical Volume Multiple-Media Licensing

The RDX Logical Volume configuration combines up to either 4 RDX cartridges (for the QuikStation 4) or 8 RDX cartridges (for the QuikStation 8) into a single logical volume target.

The Removable Disk RDX Logical Volume configuration causes the host computer to view the RDX as a single removable disk allowing it to be ejected. When the RDX Logical Volume is ejected, all RDX cartridges in the Logical Volume are ejected together.

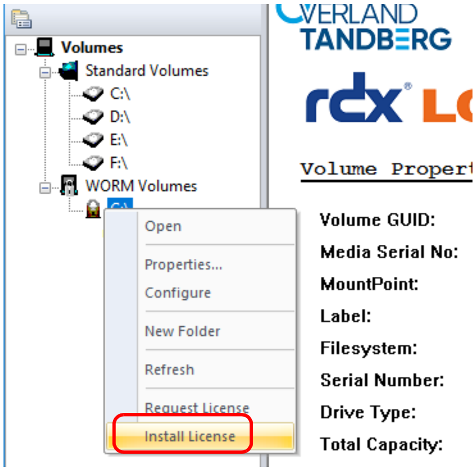
Convert Single Licenses into a Multiple-Media License

To use rdxLOCK with the RDX Logical Volumes feature on a QuikStation system where multiple RDX cartridges are presented as a single disk target (RDX Logical Volume mode), the original single-media rdxLOCK licenses must be revoked and a special multiple-media license be obtained from Overland-Tandberg Technical Support.

When switching to RDX Logical Volumes mode, to change licenses:

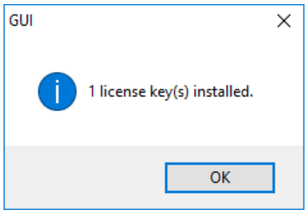
1. Submit **a** list of all the Capacity ID numbers from the license cards for the cartridges.
2. Those licenses will be revoked and a single, special **multiple-media license** will be provided for you to install.
3. After receiving the email with the multiple-media license key file, save the **file** to an easy-to-access location.

4. In the rdxLOCK GUI, right-click the **volume letter** and select **Install License** from the context menu.



5. Browse to the **license key file** and click **Open** to activate the license.

6. At the successful installation message, click **OK**.



1 license key(s) installed.

7. Check the license type and status on the right-side pane of the rdxLOCK GUI. It can take up to four (4) minutes before the license status is updated.

Index