TANDBERG DATA

rdx LOCK

rdxLOCK

Administration Guide

Version 2.2

(Rev. 14)

Contents

1 Product Information

1.1 Overview

rdxLOCK is a software product, that provides infinite WORM protection for data on **rdx QUIK**STOR cartridges.

Applications can write data locally, write via CIFS or FTP directly to **rdx**LOCK protected file systems, but are not allowed to make any modification after the data is locked. The locking mechanism and read/write-access is completely controlled by **rdx**LOCK and ensures that a file object is changed to read-only based on the selected protection policy.

rdxLOCK protection policies ensure that files can't be modified, renamed, moved or overwritten in any way. Additionally **rdx**LOCK prevents the alteration of file attributes.

As **rdx**LOCK is able to use the existing server and **rdx QUIK**STOR drive, an audit-compliant archive can be implemented in a cost effective manner.

rdxLOCK supports Windows 32-bit and 64-bit architectures.
Detailed information about supported OS versions is available in the readme file in the installation folder of the **rdx**LOCK software.

1.2 Key Features

1.2.1 Protection modes

Protection policies can be configured only once for an **rdx QUIK**STOR cartridge. The following protection policies are supported:

- Standard WORM mode

  Files copied to **rdx QUIK**STOR cartridge are automatically set to WORM mode after 10 seconds.

- Enhanced WORM mode

  The WORM mode for files copied to **rdx QUIK**STOR cartridges is controlled by the approved applications that transfer the data. These applications decide when a file is set to WORM mode.

  Files may also be manually set to WORM mode by setting the read-only attribute for the file. Once the read-only attribute is set, all further changes to the file or the file's attributes are prevented.

1.2.2 Enhanced Security Mode (ESM)

rdxLOCK protected volumes may be managed on the operating system level mostly like any volume. In particular you can mount them on any computer, even if there is no **rdx**LOCK software installed.

Enhanced security is a security level to encrypt the volume in a way that no content of the real volume is visible, unless **rdx**LOCK is installed. Instead of the real content of the NTFS volume, you see a small FAT volume with warning information. Enhanced security also inhibits the deletion of files on **rdx**LOCK protected volumes in the following cases:

- The **rdx**LOCK file system filter has been stopped.
- **rdx**LOCK has been uninstalled from the system.
- The **rdx**LOCK WORM cartridge has been moved to a system having no **rdx**LOCK installed.

1.3 Restrictions

- **rdx**LOCK Version 2.2 is designed only for NTFS formatted volumes on **rdx QUIK**STOR cartridges.
- File systems other than NTFS are not yet supported.
- Appending data to **rdx**LOCK protected files is not supported.
- Files having Extended Attributes or reparse points attached can't be set to WORM.
- The Enhanced WORM mode is not supported on WORM volumes which are exported via NFS protocol.
- **rdx**LOCK may not be installed on systems which do have any version of TrueCrypt installed.

2 Installation

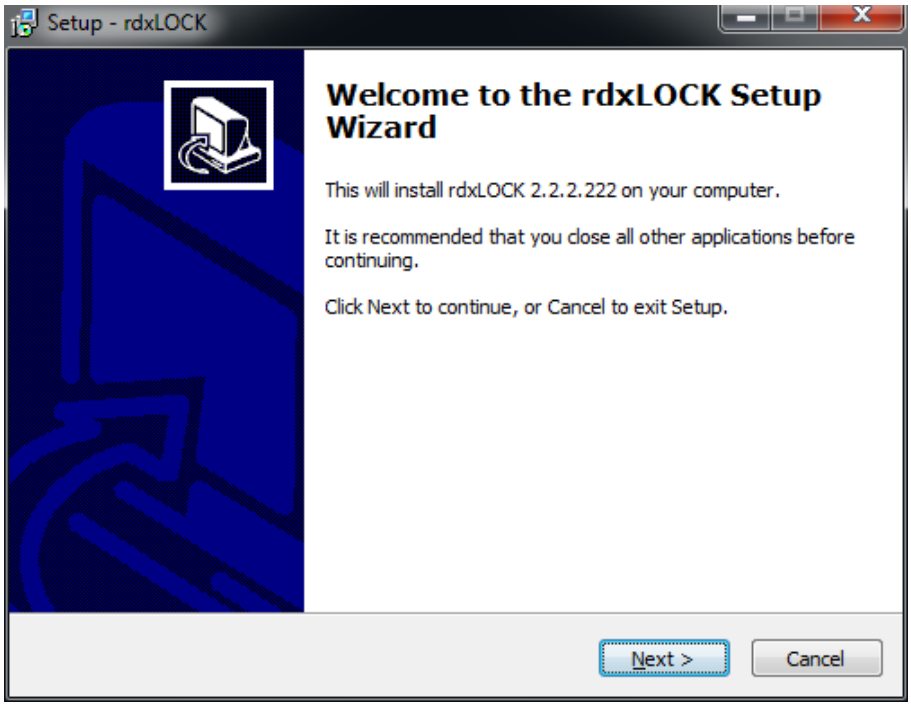
Administrative rights are required to install, configure, license or update **rdx**LOCK. When installing on Windows Vista, Windows 7 or Windows 2008 Server you need to be **logged in as Administrator**. - Just having **administrative rights** or being a member of the Admin group **is not sufficient**.
If the built-in domain administrator account is used for configuring **rdx**LOCK, the local security policy **"User Account Control: Admin Approval Mode for the Built-in Administrator Account"** must be disabled.

2.1 Installing rdxLOCK

2.1.1 Starting the Installation

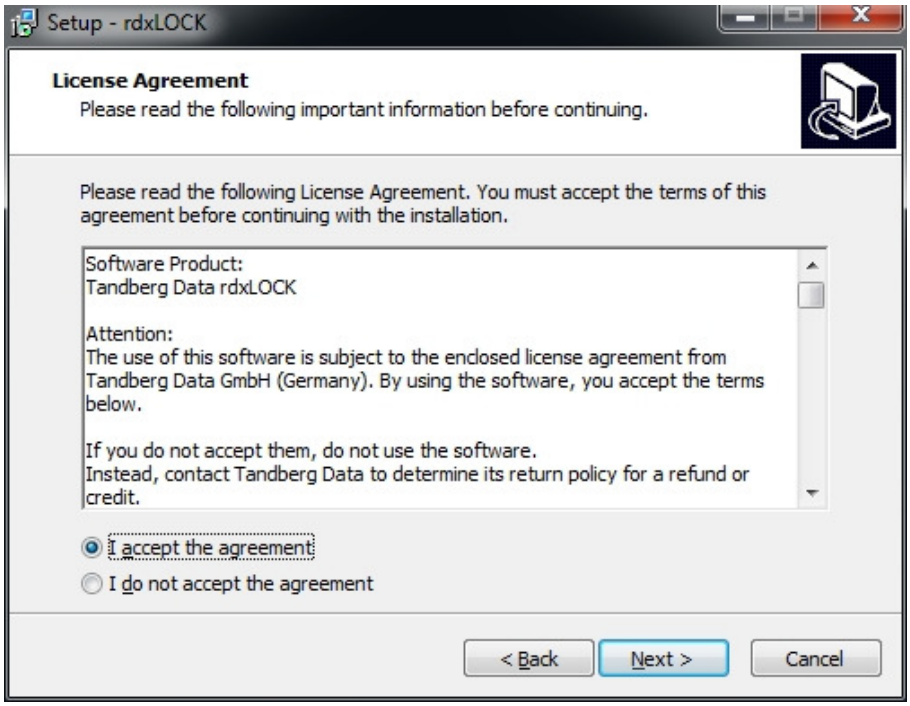
To install **rdx**LOCK

- Close all applications running on the file server.
- Run the program ***rdxlocksetup_<version>.exe*** to start the installation wizard.

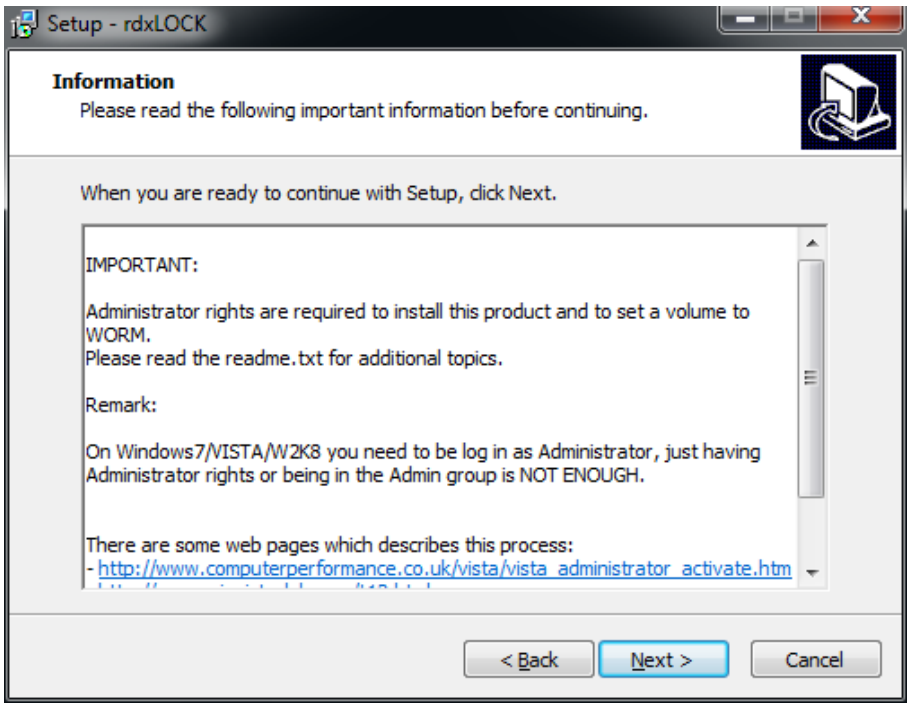


If no other application is opened at this time, you can proceed with the installation process by clicking the *Next* button.

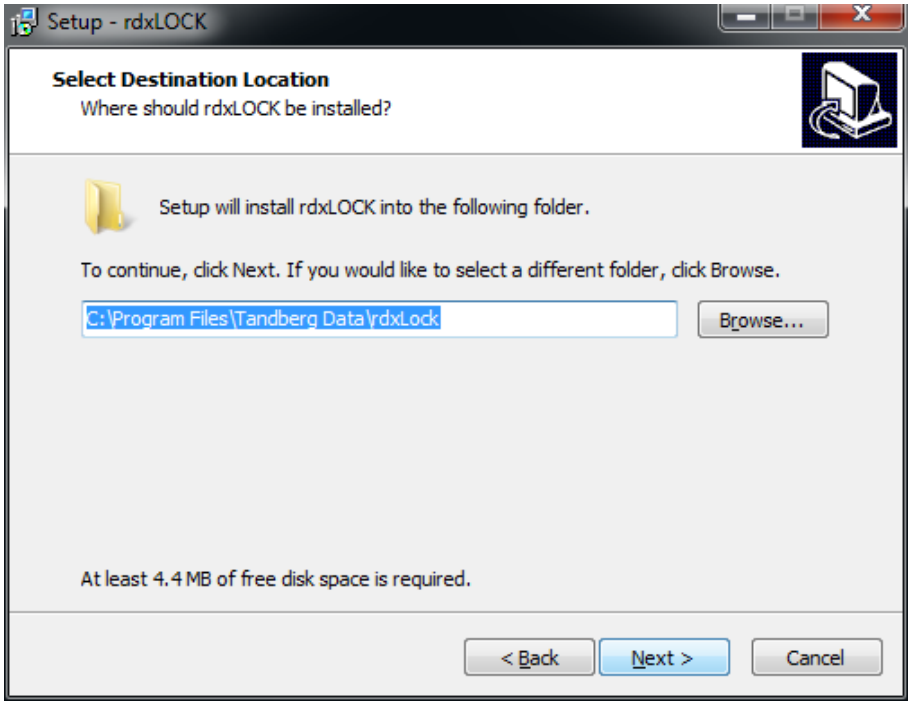
2.1.2 License Agreement

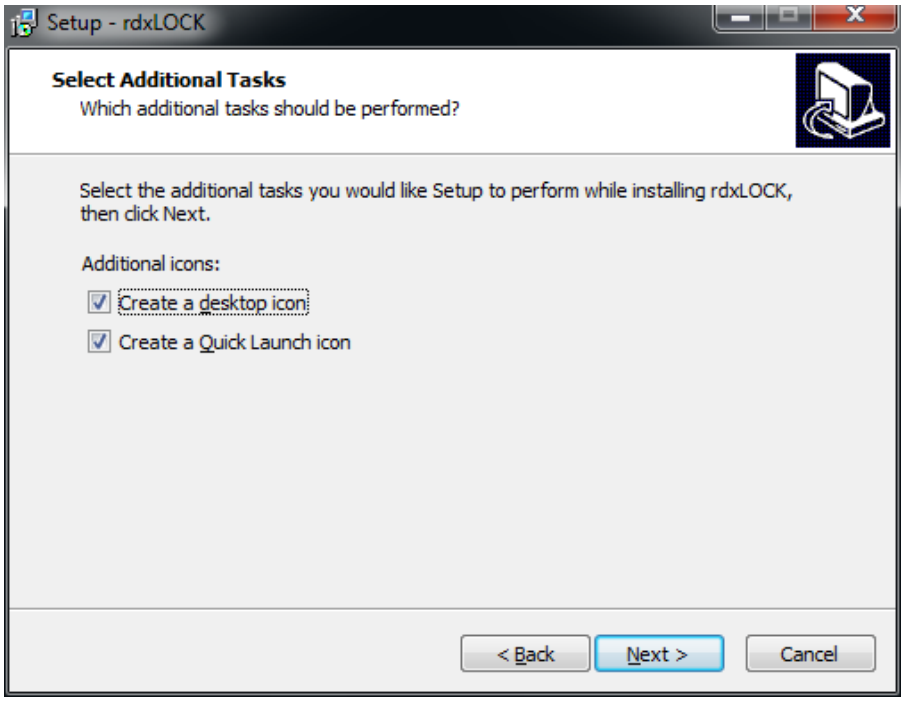


You must agree to the license contract in order to continue with the **rdx**LOCK installation procedure.

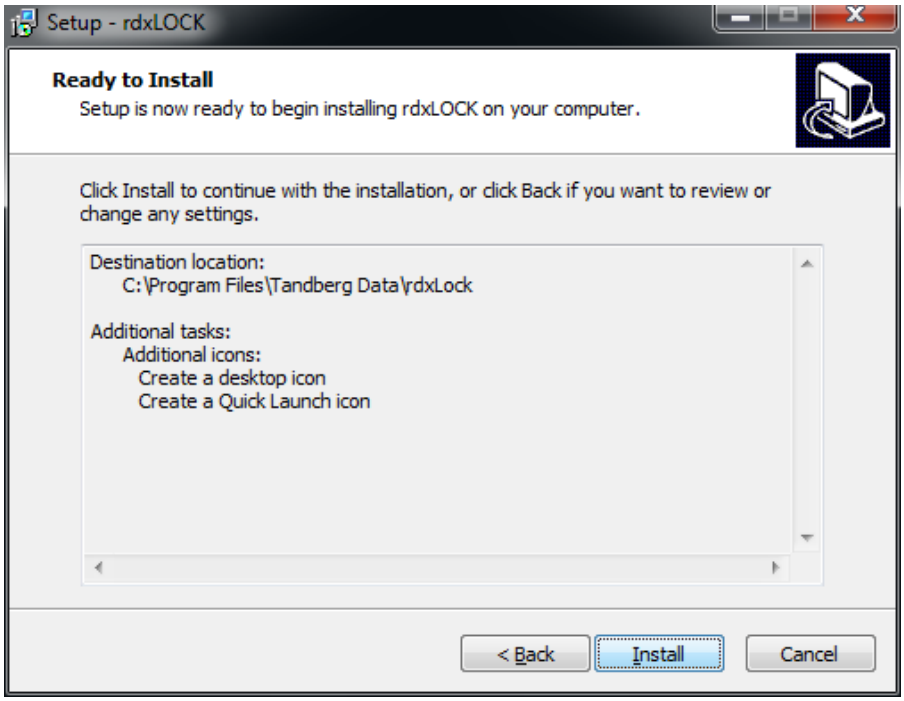


2.1.3 Select the installation path and additional tasks

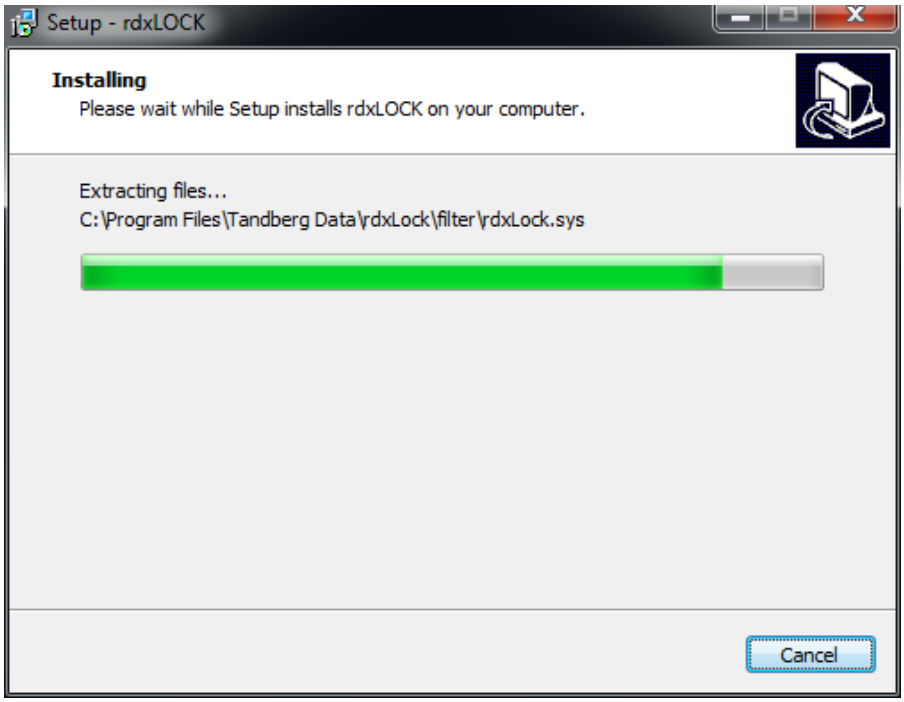




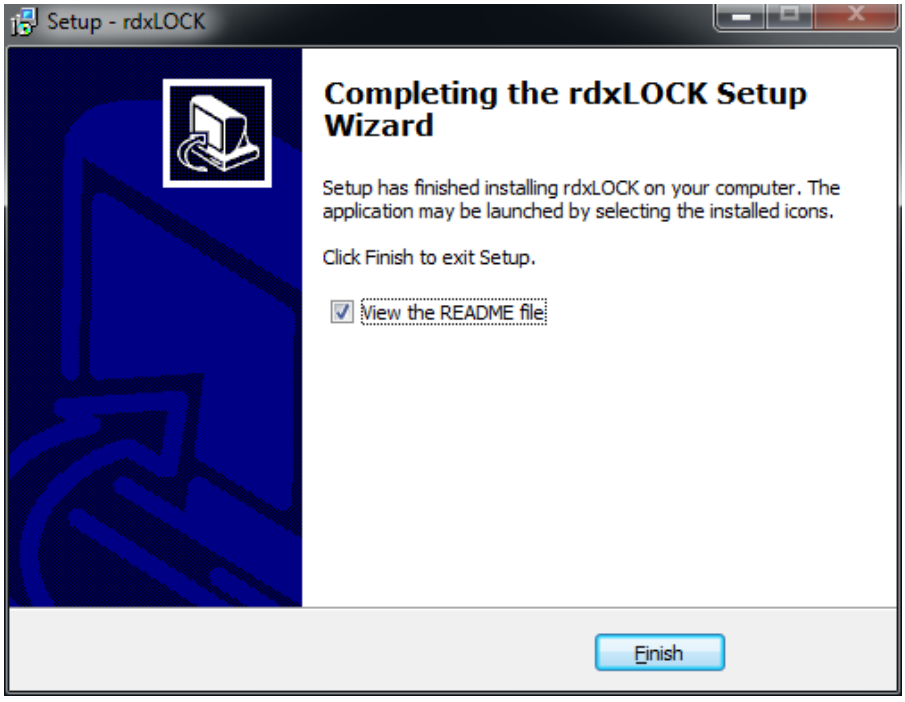
2.1.4 Start the installation



After clicking the *Install* button, **rdx**LOCK will be installed to the selected destination folder.

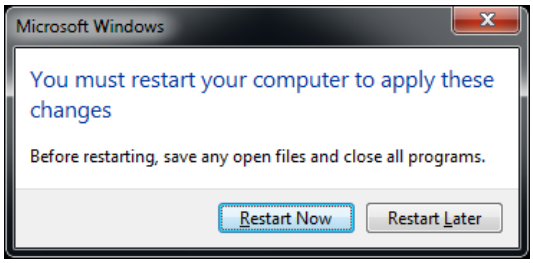


2.1.5 Completing the Installation



On the completion screen you have the option to view **rdx**LOCK readme file to get the latest information on the product.

Installing **rdx**LOCK requires a system reboot.



Attention: WORM functionality is only available after reboot!

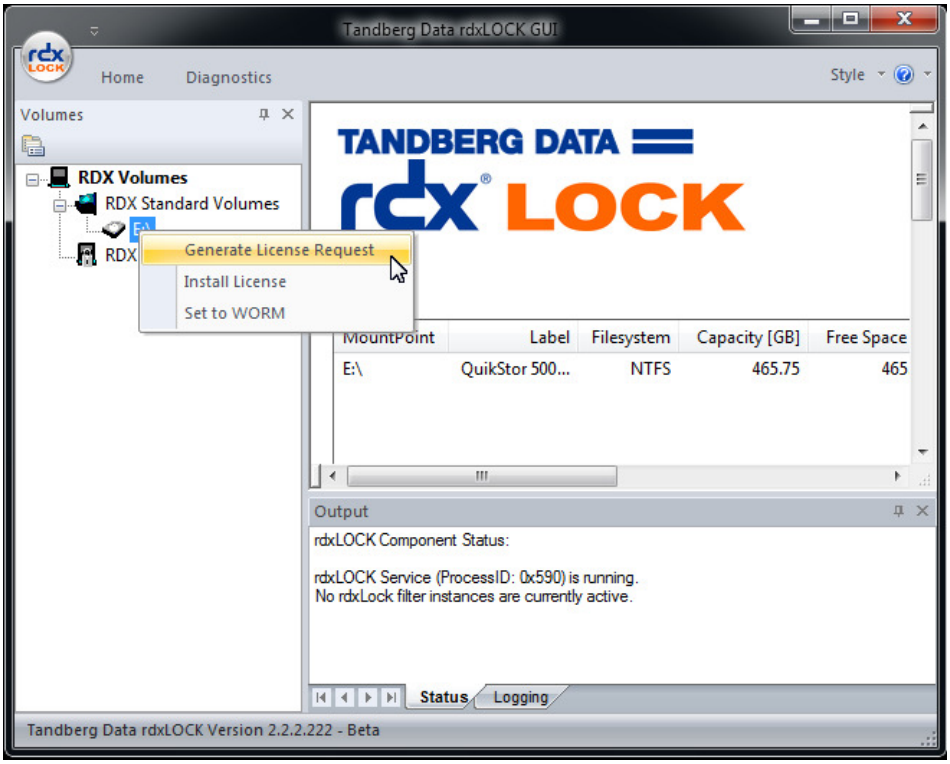
3 Configuration

3.1 Obtaining and entering license keys

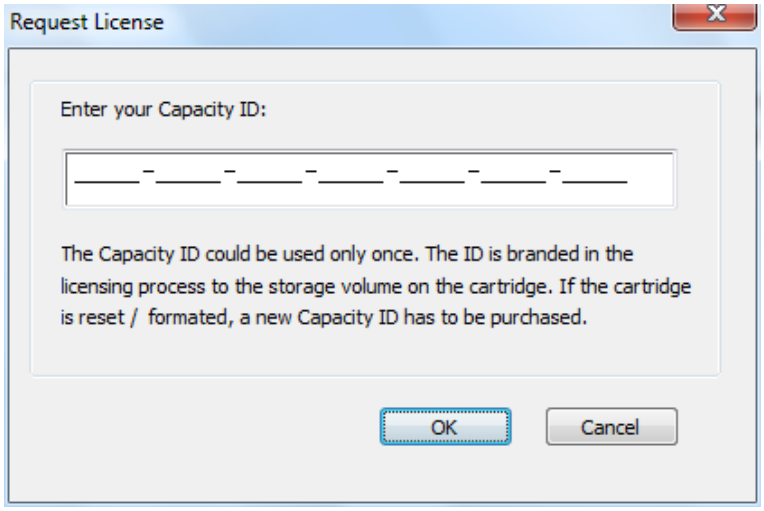
rdxLOCK needs a license for rdx WORM cartridges. Each cartridge is registered separately and therefore has its own **rdx**LOCK generated serial number. The key is stored after completing the licensing steps for the cartridge. There is no need to setup up this license again when reinserting the cartridge or moving it to another system.

To generate the license, take the following steps:

- Make sure the RDX cartridge is inserted into an RDX dock.
- In the Windows Start menu, select Programs - > Tandberg Data -> rdxLOCK -> rdxLOCK
- In the **rdx**LOCK user interface, select RDX Standard Volumes and right-click on the WORM volume for which you want to request an **rdx**LOCK WORM license.
- Click "Generate Request License"

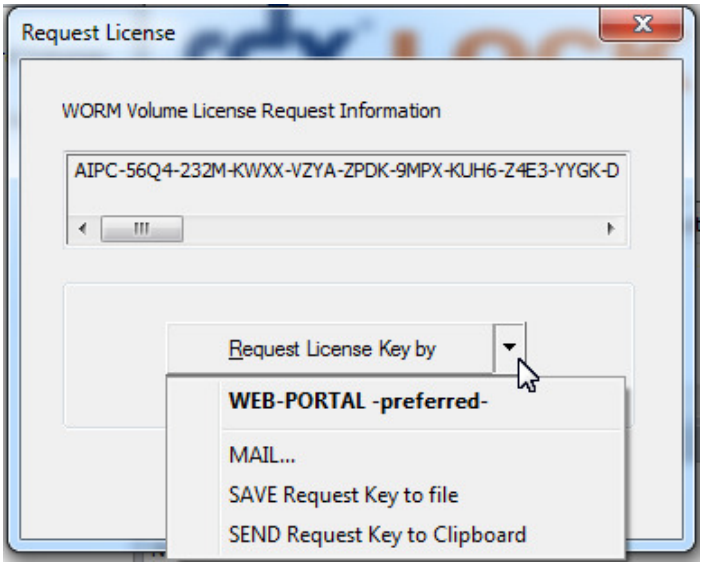


- Enter the Capacity-ID, which you have received with your rdx WORM cartridge (card inside the cartridge box).



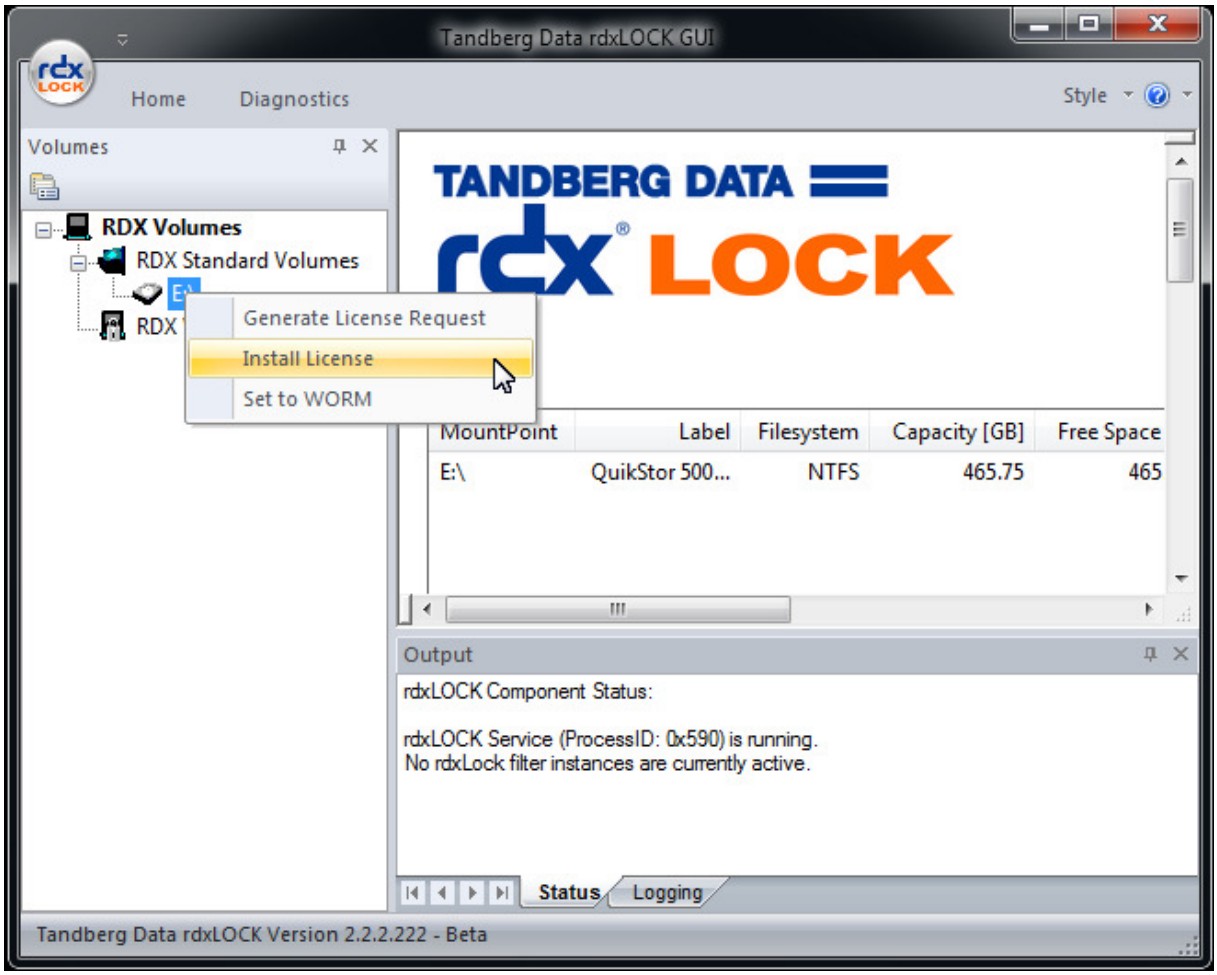
(Details about the Capacity ID usage are described in chapter 6.3)

- Decide the way you will request the license.



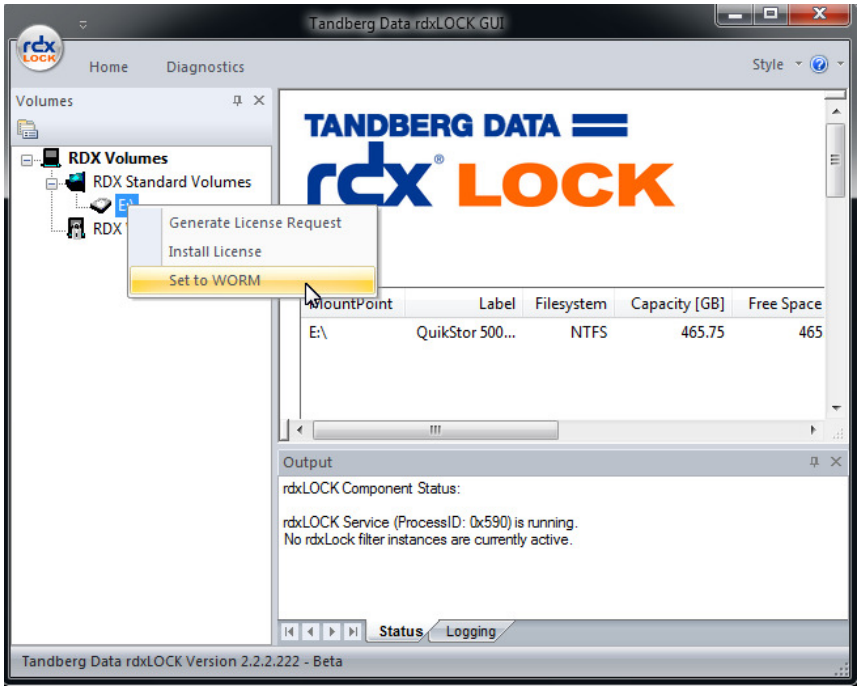
- 'Mail' will open your standard mail application to send the key request to **SupportEMEA@tandbergdata.com**
- 'WEB-PORTAL' will open your standard browser to request the license
- 'SAVE' will store the license request in a file you can use to request the license by an alternative mail client or from another system.

After receiving the license key file for the volume, right-click and select "Install License" and then select the file containing the license information.

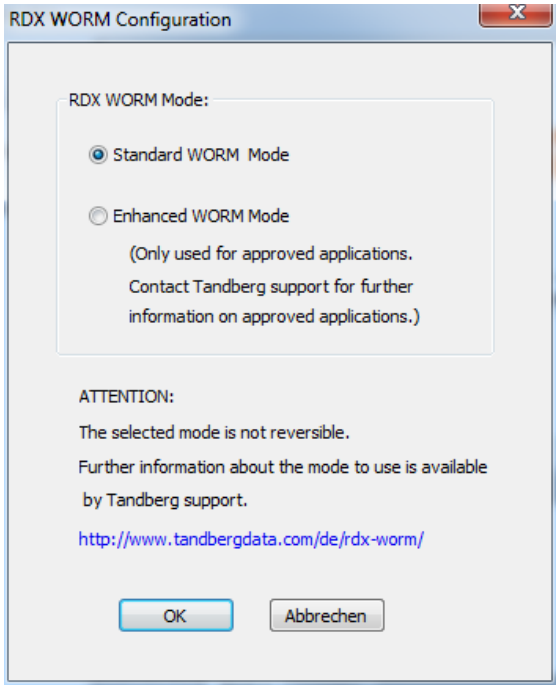


3.2 Setting up a WORM volume

- To convert an rdx standard cartridge into an rdx WORM cartridge, right-click the rdx drive's icon in the **rdx**LOCK GUI then select 'Set to WORM'.

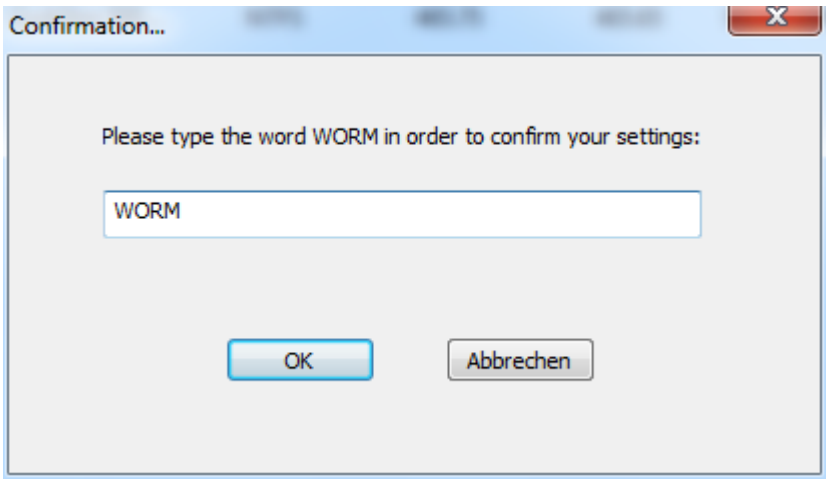


- Select standard or enhanced mode for the rdx cartridge.
  Detailed information about the modes is explained in the next chapter.

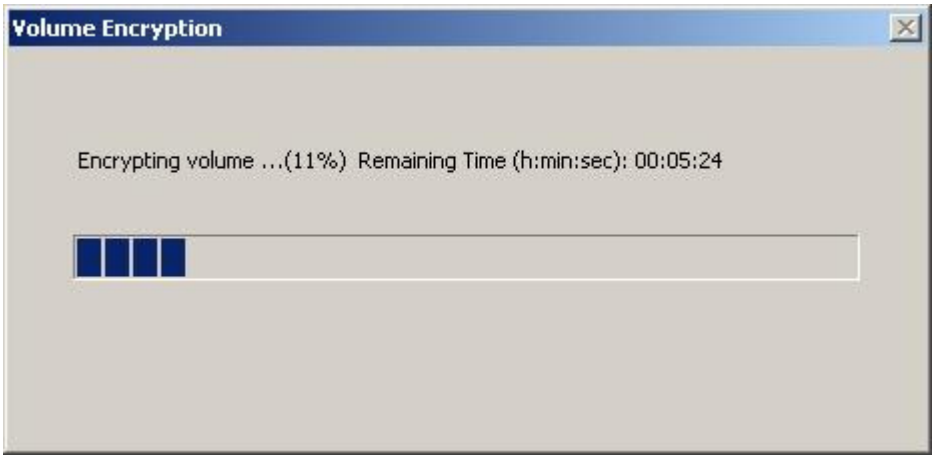


Attention:
The rdx cartridge cannot be reconfigured to another mode after it has been converted to WORM.

- To save your settings, press the ***OK*** button.
- Confirm you settings by typing 'WORM' and press the **OK** button.



- **After confirmation, the rdx cartridge will be encrypted and converted into an rdx WORM cartridge. This process could take some time (up to several hours) depending on the size of existing data in the volume and your hardware. Do not abort this process!**
  (See chapter 6.2)



3.3 rdx WORM protection modes

rdx WORM cartridges protects data against deletion or manipulation.

The way the protection works is defined by the selected mode.

If you are not sure about which mode to use, please contact Tandberg Data support (SupportEMEA@tandbergdata.com) to get information about the approved applications for the different modes.

3.3.1 Standard WORM mode

rdxLOCK standard WORM mode protects all new files stored on the cartridge against deletion or manipulation.

This protection will be active after a new file is stored and is not touched for 10 seconds.

The file state can be controlled by the standard read-only attribute in the file system.

This protected state cannot be reset and will last infinitely.

3.3.2 Enhanced WORM mode

rdxLOCK enhanced WORM mode is available for approved applications to control for the WORM state of single files by the application.

All new files stored on the RDX WORM cartridge will remain in an unprotected state until the application decides to activate protection (i.e. no automatic protection for files is done).

New files can be deleted or changed until protection is activated.

After protection is activated for a file, any further deletion and manipulation is prevented.

Files may also be manually set to WORM mode by setting the read-only attribute for the file. Once the read-only attribute is set, all further changes to the file or the file's attributes are prevented.

The protected state cannot be reset and will last infinitely.

The following rules apply to **rdx**LOCK protected files:

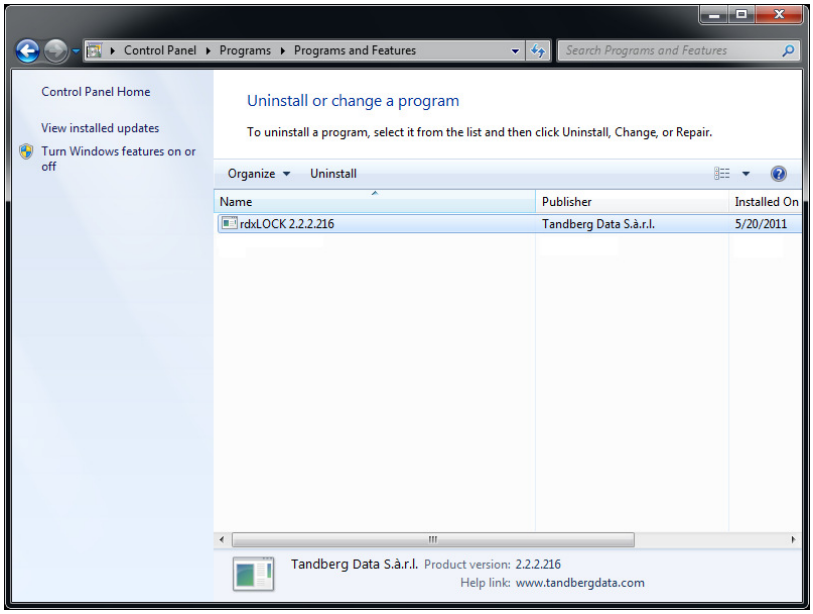
- WORM files cannot be modified, overwritten, renamed or deleted.
- WORM files cannot be changed back to non-WORM files.
- Security settings (ACL) on WORM files cannot be changed any more. Therefore we recommend always using security groups in order to be able to change security for single users by adding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

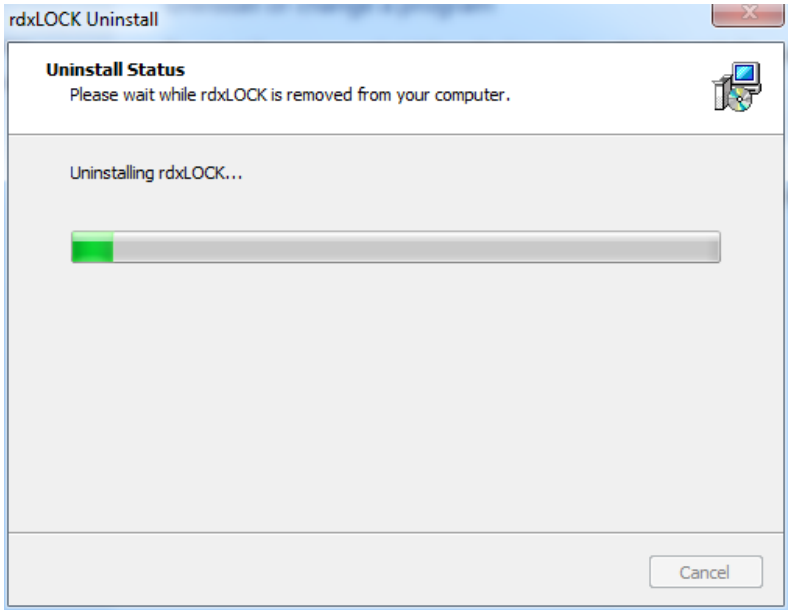
Attention:

- If you decide to use ACL's on WORM media take care to use standard groups to be able to exchange data with organizations outside your security structure (domain).

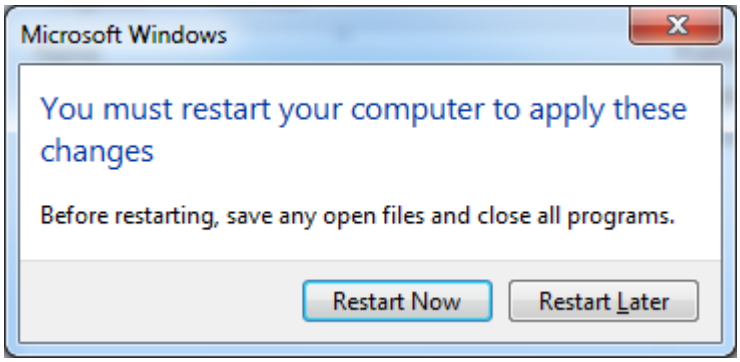
4 Uninstall

rdxLOCK can be uninstalled by using the Windows Software Manager. Click *Start -> Control Panel -> Add or Remove Programs*, select the **rdx**Lock product and press the *Remove* button.





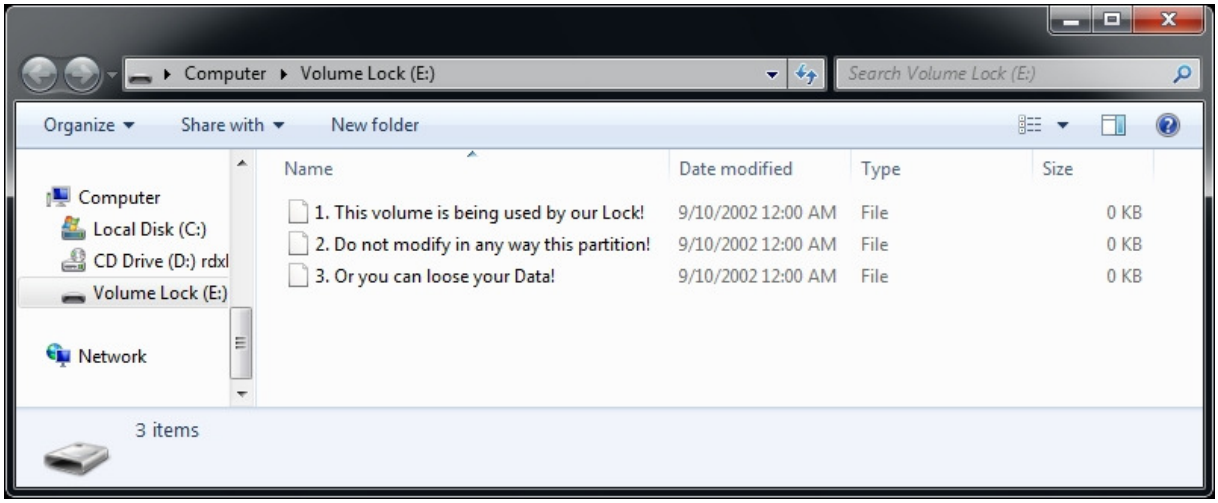
A reboot is required to completely remove **rdx**LOCK from your system.



NOTE:

If you remove the rdxLOCK **product from your system, you will not be able to access rdx WORM cartridges anymore.**

The WORM cartridge file system is hidden and inaccessible after uninstalling the rdxLOCK **product. Instead, the former NTFS WORM file system is displayed as a FAT file system with the label "Volume Lock".**



5 Troubleshooting

5.1 Reporting a Problem

For technical assistance with **rdx**LOCK, email your inquiries to **SupportEMEA@tandbergdata.com** . You may also visit the Tandberg Data website at http://www.tandbergdata.com/de/rdx-worm for additional contact and support information.

Please have the following information included in your email when you report an **rdx**LOCK 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?

- The **rdx**LOCK Service Report.

  The **rdx**LOCK GUI application automatically generates a Service Report by selecting the menu item <Diagnostics> -> <Generate Service Report>. All service information is stored to the file **FL_Diag.zip**, which is located in the directory **<rdxLOCK installation directory>\Diagnostics**.

- A list of third-party applications installed on your system, including antivirus scanners and backup management applications.

5.2 Application event log message: "Invalid license"

An invalid license may result from the following conditions:

- License information can't be read on the WORM cartridge. Please check, if the rdxLock service is running.

6 Appendix

6.1 Filter - Compatibility

rdxLOCK was successfully tested in combination with the following 3rd party applications:

- Symantec AntiVirus Version 10.0
- McAfee VirusScan Enterprise 8.7
- TrendMicro ServerProtect 5.58

- 3rd party replication tools have not been tested with **rdx**LOCK version 2.2.

For last minute information regarding limitations and known problems, please read the ReadMe.txt.

6.2 Duration of convert process

The conversion of rdx standard cartridges to rdx WORM cartridges is designed to generate a medium that meets the requirements of compliance.

To meet these requirements it is necessary to convert all used blocks on the cartridge into a format that can only be accessed by **rdx**LOCK software and cannot be modified or changed by any other software or operating system.

This process converts all used blocks on the cartridge and can last some time, depending on how many data are stored on the media when convert process was started.

Maximum performance for the conversion process is 100GB per hour. Performance depends on rdx drive configuration, interface and controller.

Empty cartridges should be converted in less than a minute.

Attention: Do not abort or interrupt this process, it will leave the cartridge in an undefined state that prevents the usage of the cartridge. The cartridge has to be reset to a standard rdx cartridge with operating system tools. The used capacity ID key cannot be reused for enabling WORM on the cartridge.

6.3 Usage of Capacity ID

A Capacity ID is used to generate a license for a storage volume on a rdx cartridge. The ID is branded during the licensing process to the existing storage volume on the cartridge. After the ID is branded to the existing storage volume it is not possible to use the ID again.

If the cartridge is reset / reformated the storage volume on the cartridge is regenerated with new internal tokens. The Capacity ID and the generated license could not be used for this storage volume again. You have to purchase a new Capacity ID.