



# GRAU DATA

YOUR DATA. YOUR CONTROL

## FileLock Administration Guide

GRAU DATA GmbH

Version 2.4.2.203 - SMR-3, 2026-03-13 10:51:24

# Table of Contents

1. Product Information .....	1
1.1. Overview .....	1
1.2. Key Features .....	1
1.3. Restrictions .....	5
2. Installation .....	7
2.1. Installing FileLock .....	7
2.2. Post-Installation .....	13
2.3. Uninstalling FileLock .....	14
3. Configuration .....	16
3.1. Obtaining and applying the "TimeSync" Key .....	16
3.2. Setting up a WORM volume .....	18
3.3. Protection policies and retention periods .....	21
3.4. Obtaining and entering license keys .....	30
3.5. WORM-TO-WORM Replication .....	34
3.6. Modification of Maximum Policy Folder Level .....	43
4. Best Practices .....	44
4.1. Data Protection .....	44
5. Troubleshooting .....	46
5.1. Reporting a Problem .....	46
5.2. FileLock Tab is not available on MS Explorer's property page .....	47
5.3. Application event log message: "Invalid license" .....	47
5.4. Missing privileges .....	48
Appx A: Filter - Compatibility .....	49
Index .....	50

# Chapter 1. Product Information

## 1.1. Overview

FileLock is a hardware-independent software product, which provides infinite or fixed (by date or period) WORM (Write Once, Read Many) protection for data on standard hard disk systems.

Applications can write data locally or remote via CIFS or NFS directly to a FileLock protected file system, but are not allowed to make any modification after the data was locked. The locking mechanism is completely controlled by FileLock on a directory-level or file-level basis and ensures that a file object is changed to WORM based on the selected protection policy. A special API is not necessary.

FileLock'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 a specified period of time or infinite. Additionally FileLock prevents the alteration of file attributes, however ACL changes are possible in certain cases. In order to meet governmental compliance requirements, FileLock allows the deletion of data after the pre-defined retention period, but still prevents the user from modifying expired data.

As FileLock is able to use the existing server and disk storage infrastructure, an audit-compliant archive can be implemented in a cost effective manner. FileLock supports NTFS and ReFS volumes on 64-bit Windows architectures.

## 1.2. Key Features



The availability of some functions and features depends on the installed license. This administration guide documents the full function and feature set.

### 1.2.1. Protection Policies

Protection policies can be configured either on the root, or on the 1st directory level. With a modification of the registry the policies can be configured up to the 9th directory level.

### The following protection policies are supported:

- DLR = Directory Level Retention The DLR policy is based on directories. The advantage of this policy is the option, to prolong the retention period of a data pool by changing only one single parameter.
- SFR = Single File Retention (SnapLock Interface) The SFR policy allows an individual retention period for every individual file. It provides compatibility with the NetApp, Inc. SnapLock interface.



The availability of most policies depends on the installed license. (The basic policy function there is DLR, infinite. The basic policy-level there is root.)

### 1.2.2. Enhanced Security Mode (ESM)

Enhanced Security Mode encrypts FileLock volumes on block level and prevents direct access to the protected content of the volume if FileLock is not running. Instead of the real content of the NTFS or ReFS volume, you will see a small FAT volume as placeholder with warning information. The protected content is hidden by the encryption layer. This also inhibits the deletion of files on FileLock protected volumes in the following cases:

- FileLock is not installed at all
- The FileLock file system filter has been stopped.
- FileLock has been uninstalled from the system.
- A FileLock WORM volume has been moved to a server system, which does not have FileLock installed.

Since FileLock 2.3.1 ESM is mandatory in the versions 6 or 7.

Volumes with ESM V5 and below are still supported but have to be migrated to ESM V6. Migration has to be performed in the FileLock GUI. New created volumes will only be created with ESM V7 to differentiate between migrated volumes (V6) and new created volumes (V7). The ESM version number is increased to prevent older FileLock version from mounting this volume.



Please run a backup of the WORM volume before changing the encryption or migrating to current ESM versions.



Up to FileLock 2.3.0 ESM mode was optional and WORM volumes without ESM were supported, while ESM mode is mandatory in FileLock 2.3.1 and up. Therefore WORM volumes without ESM will be mounted in READ-ONLY mode in recent FileLock versions. We strongly recommend to **not** activate ESM mode later on such a non-ESM volume as the resulting encryption of existing data would take a very long time and would cause complete data loss in case the encryption is interrupted for whatever reason.

To prevent data loss activating ESM mode is refused by FileLock if the WORM volume contains more than 1GB of data.

Please contact [support@graudata.com](mailto:support@graudata.com) if you need to access non-ESM mode volumes with FileLock version 2.3.1 and up.

### 1.2.3. Verified Retention Clock (VRC)

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

FileLock provides a secure and compliant retention time management, called Verified Retention Clock (VRC). This facility has to be synchronized directly after setting up the software by entering a special [TimeSync Key](#).

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



All WORM volumes created by a FileLock application with a **non-verified** system clock are marked as “TEST WORM VOLUMES” with a limited lifetime and can **not** be converted to valid, productive WORM volumes.

After a successful system clock verification, VRC closely monitors the system clock and ensures that system clock manipulations may not be used to delete files before they expire. Such manipulations may end in temporary prolongation of retention periods when the system clock is set in the future or to access restrictions when it is set to the past.

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 reasons, this does result in a prolongation of retention periods. In order to correct such artificially extended retention time periods, VRC allows a drifting of the retention time offset (RTT-Offset) up to a week per year in order to make up for downtimes due to system maintenance and other housekeeping events. Longer periods of downtime will need to be handled via a TimeSync Key, if the RTT-Offset is beyond an acceptable value.

VRC is designed to support removable WORM media as well. Taking a WORM volume offline for an extended time period does not end up in a temporary prolongation of retention periods registered in a volume.

## 1.3. Restrictions

- FileLock Version 2.4.2.203 - SMR-3 is designed for NTFS and ReFS formatted volumes on basic disks with MBR (master boot record) and GPT (GUID Partition Table) partitioning scheme. Partitions on dynamic disks are not supported.
- FileLock may not be installed on systems which do have any version of TrueCrypt installed.
- Additional encryption via Microsoft Bitlocker or other similar methods is not supported on FileLock volumes.
- FileLock supports local disks, certified removable media and certified removable devices.
- FileLock is not supported on Active Directory Domain Controllers.
- Other file systems than NTFS or ReFS are not supported.
- System volumes and cluster quorum disks are excluded by the configuration procedure. On a Failover Cluster only (failover) Cluster Disks can be set to WORM. Cluster Shared Volumes are not supported.
- Appending data to FileLock 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 FileLock 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 in order to make the deletion of expired WORM files possible. Please note that the Recycle Bin behavior in Windows are 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 FileLock version 2.1.0 Build 29 and higher. Previous versions need special support, so please contact our [support@graudata.com](mailto:support@graudata.com).
- 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.
- Running the FileLock GUI requires certain security privileges which are granted by default to admin users. See chapter [Troubleshooting](#) for details.
- The replication service user account needs administrative rights including the security privileges mentioned above (see [Troubleshooting](#)). When replicating to a remote share permissions and filesystem security rights must be granted to the service user account accordingly.
- Only empty volumes are supported for converting to WORM volumes. Existing volumes which already contain data are not supported. In case you need to convert existing data, please contact GRAU DATA support.
- FileLock WORM Volumes may be part of a Microsoft DFS namespace, however FileLock server and volumes are not supported for DFS root.
- Replication of FileLock WORM Volumes via DFS replication is not supported and will break FileLock volumes. For Replication of WORM volumes use the FileLock built-in replication instead.
- The "Controlled folder access" feature from built-in Windows Defender or Microsoft Defender for endpoint is not supported. This feature must be turned off when installing and using FileLock.
- On Microsoft Cluster Systems we strongly recommend to not use root level policy but only 1st directory level policies.

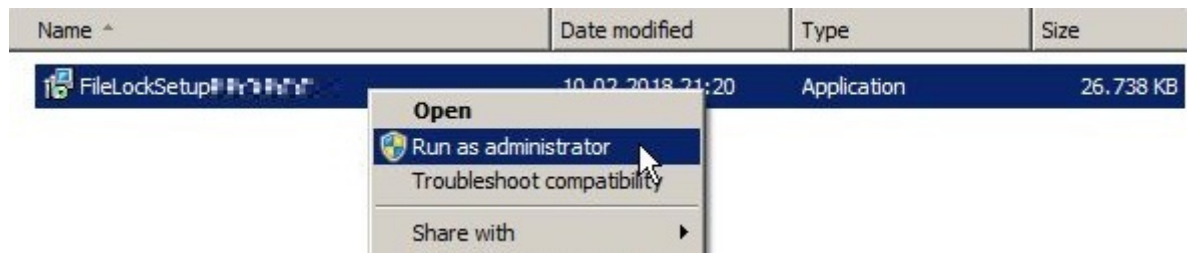


As noted above, FileLock is only supported on basic disks. Setting a dynamic disk to WORM mode will be prevented by FileLock. Although it is possible in Windows to convert a basic disk into a dynamic disk at a later time, this is **not** supported by FileLock and will render the WORM volume unusable!



# Chapter 2. Installation

Administrative rights are required to install, upgrade, configure and license FileLock and to set policies and retention times. When installing, you need to be logged in as Administrator or you need to run the installation program using the context menu option “Run as administrator”.

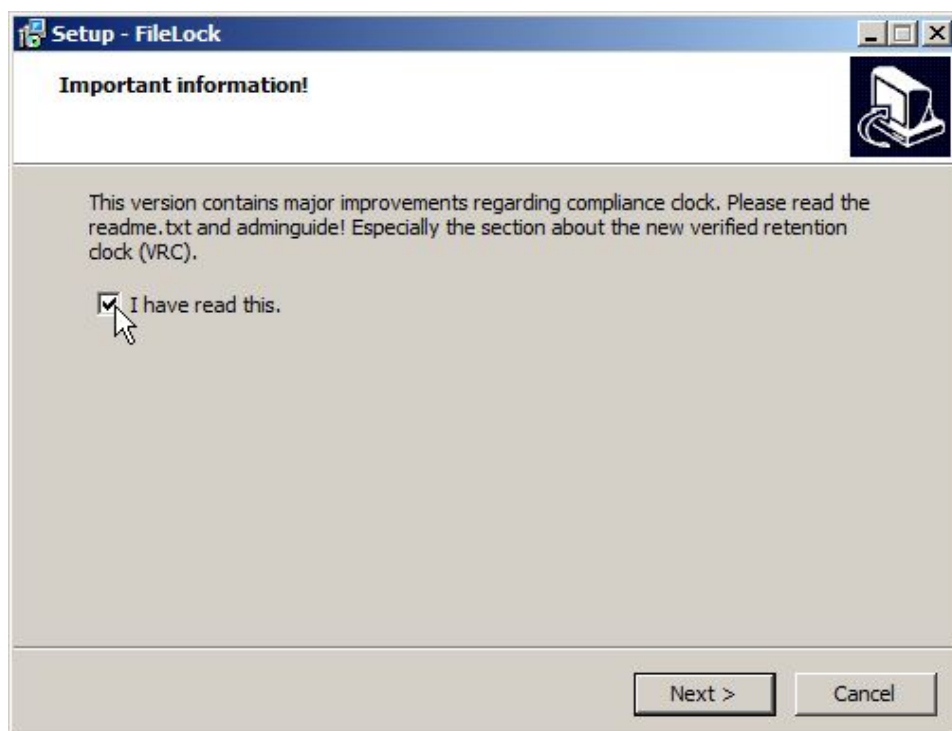


## 2.1. Installing FileLock

### 2.1.1. Starting the Installation

To install FileLock

- Close all applications running on the system.
- Run the program FileLocksetup\_<version>.exe to start the installation wizard.



If no other application is opened at this time, you can check the “I have read this” box and proceed with the installation process by clicking the Next button.

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

**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

*Example:*

```
FileLocksetup_<version>.exe /SILENT /NORESTART
```

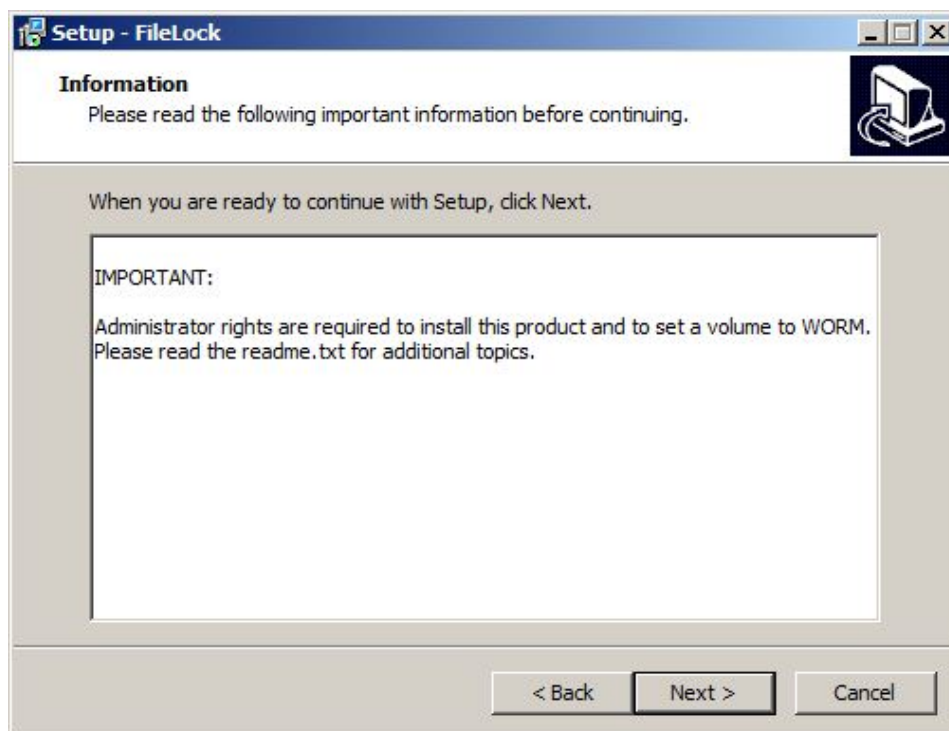


When reboot is deselected during silent installation, you must reboot the system later in order to properly activate the installed drivers.

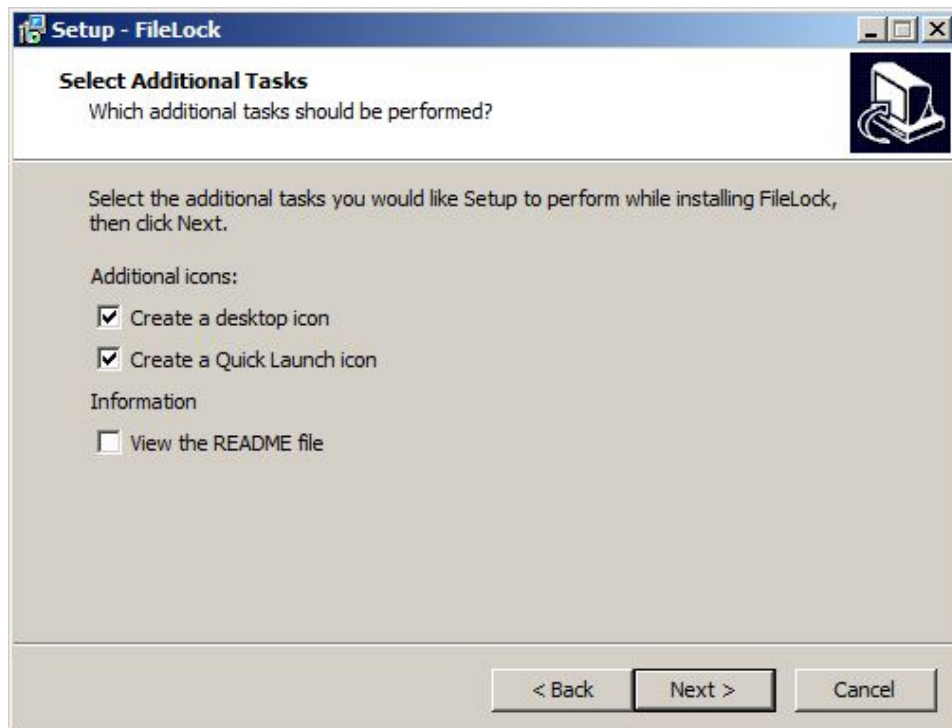
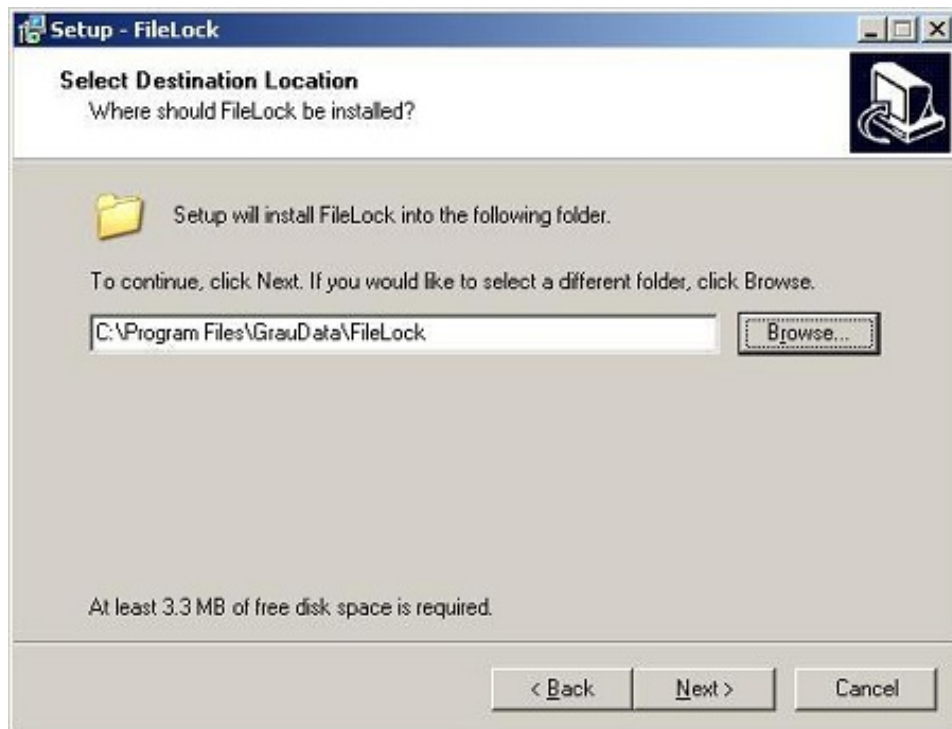
## 2.1.2. License Agreement



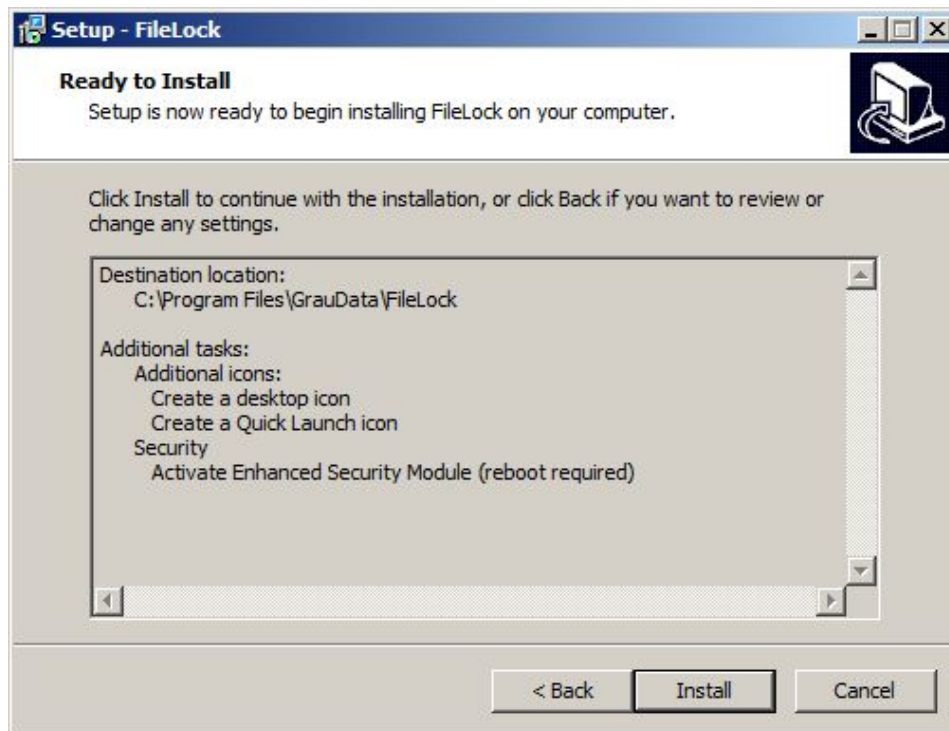
You have to agree to the license contract in order to continue with the FileLock installation procedure.



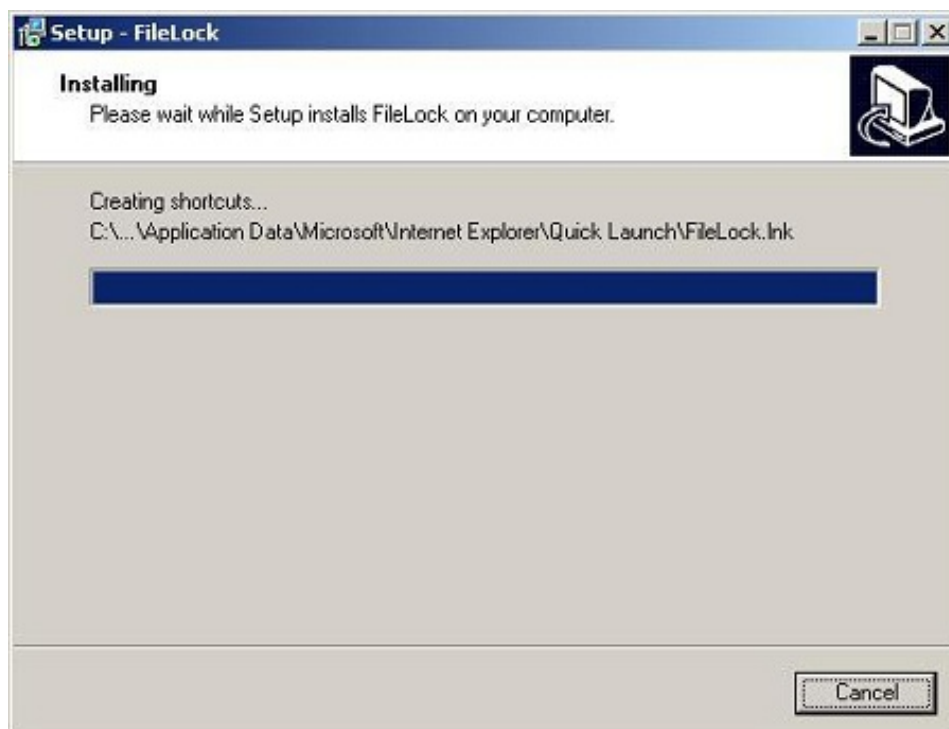
### 2.1.3. Select the installation path and additional tasks



## 2.1.4. Start the Installation



After clicking the Install button, FileLock will be installed to the selected destination folder.



### 2.1.5. Completing the Installation



To complete the installation, a reboot is required.

## 2.2. Post-Installation

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. Please refer to the chapter “Obtaining and entering the TimeSync Key” for further information.

**As long as the system clock is not verified, the following restrictions exist:**



- New Volumes are created as WORM test volumes that **cannot** be converted to regular volumes and become readonly after 60 days
- WORM Volumes created by FileLock version 2.2.5 or previous are put to READ-ONLY mode and are not switched to the regular WORM mode until the TimeSync verification has been succeeded.

After an upgrade from versions prior to 2.3.1 all WORM volumes need to be upgraded.

**To upgrade older WORM volumes take the following steps:**

- start the FileLock GUI application and select 'WORM Volumes'



- right-click on 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	
Upgrade						



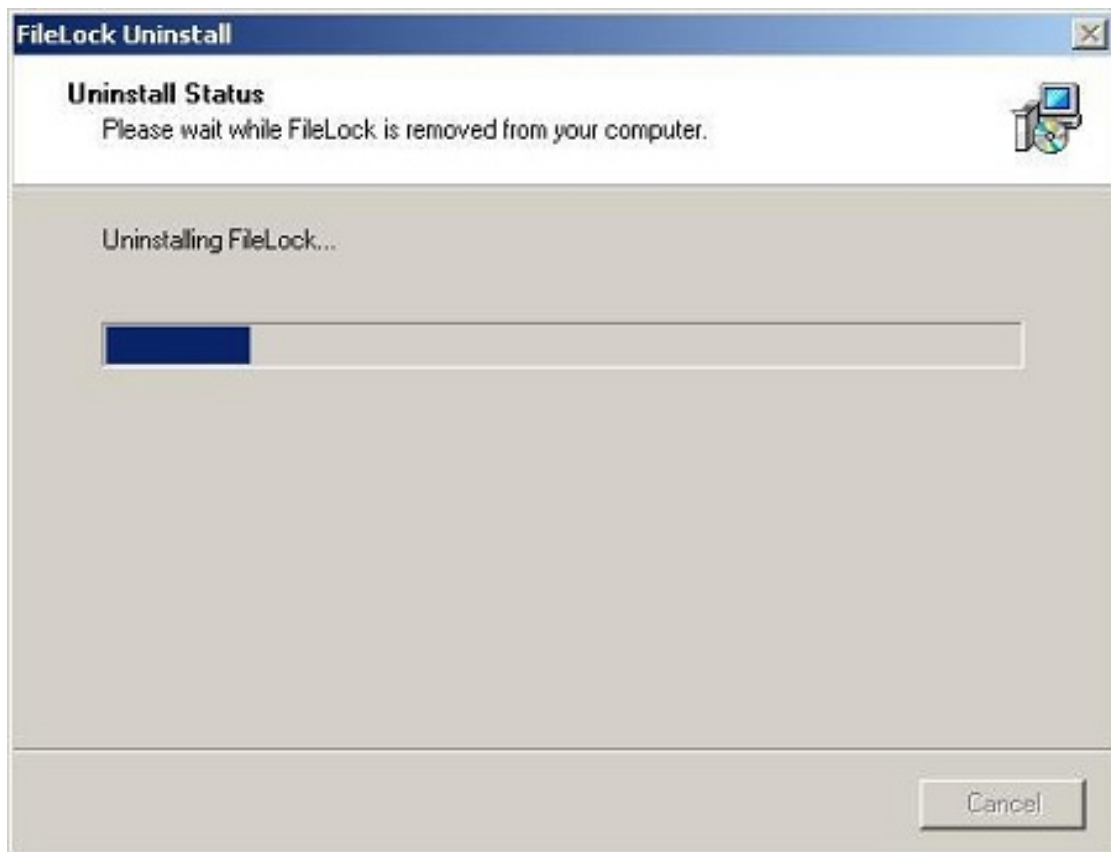
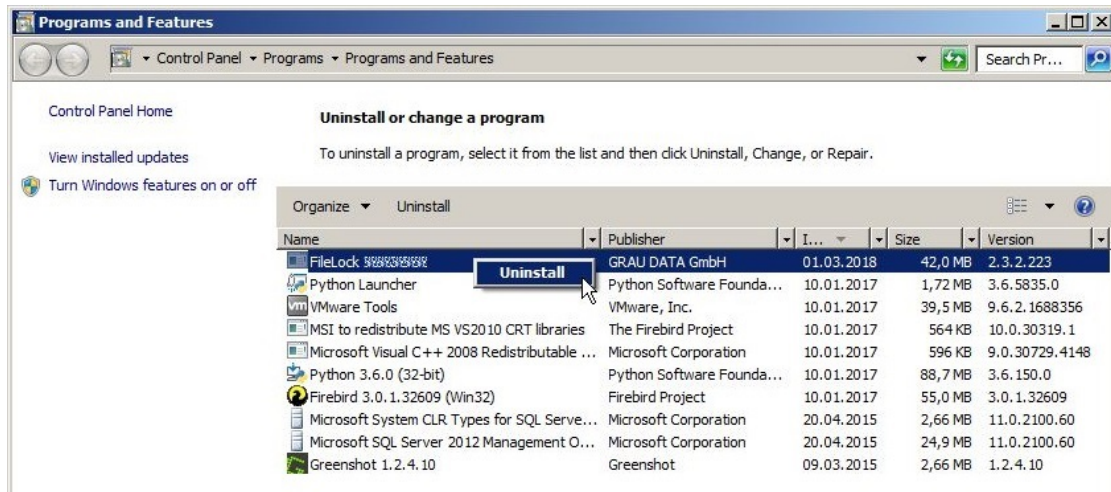
Upgraded Volumes can no longer be read by prior versions.



## 2.3. Uninstalling FileLock

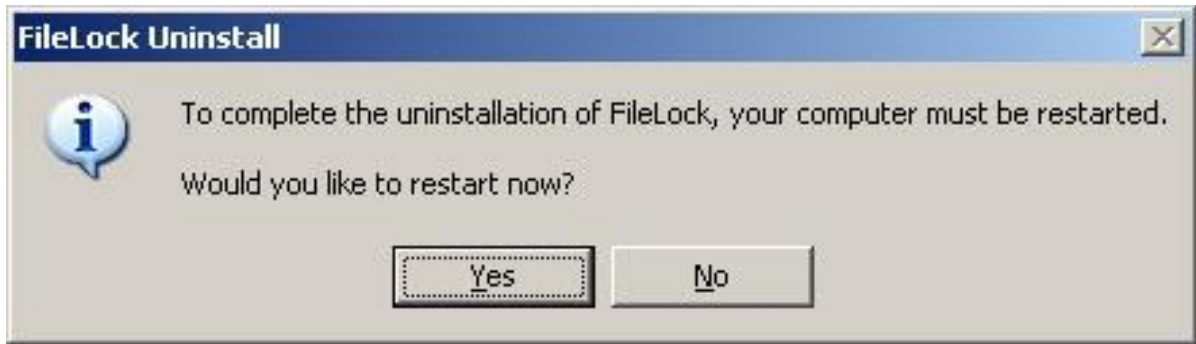
FileLock can be uninstalled by using the Windows Software Manager.

"Click Start" → "Control Panel" → "Add or Remove Programs",  
select the FileLock product and press the Remove button.

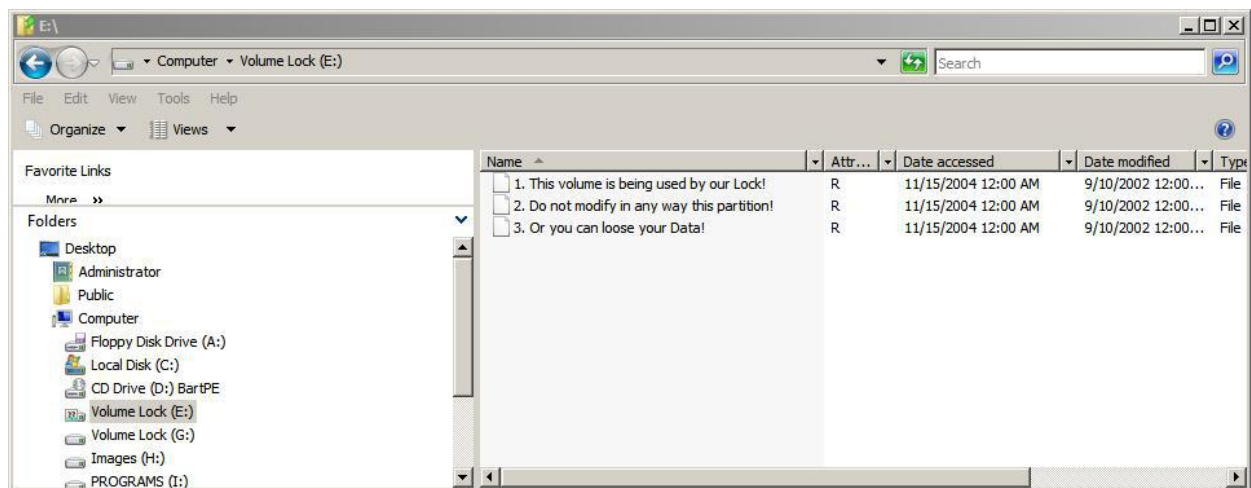


A reboot is required to completely remove FileLock from your system.





If you remove the FileLock product from your system, you will not be able to access WORM-committed files anymore. In addition the WORM file system is hidden and inaccessible after uninstalling the FileLock product. The former WORM volume is displayed as a FAT file system with the label "Volume Lock" in this case.



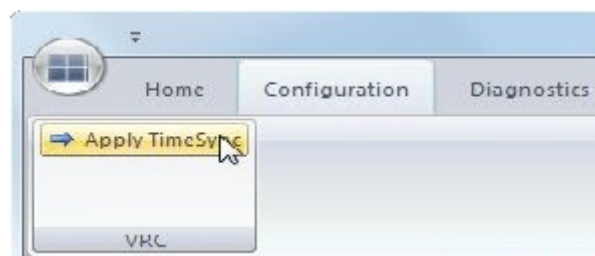
# Chapter 3. Configuration

## 3.1. Obtaining and applying the "TimeSync" Key

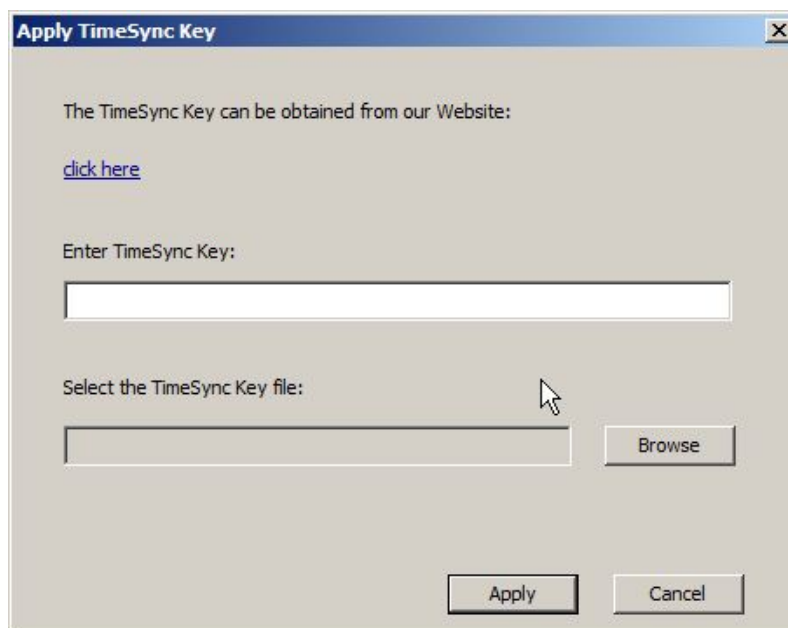
A TimeSync key is used to verify that the system clock is in a certain range compared to UTC and ensures that file retention times are managed in a safe and secure fashion. If the TimeSync key verification process succeeds for the first time, the system will be ready for handling WORM volumes. Every additional TimeSync operation resets the RTT-Offset. FileLock maintains this internal “corrective retention time offset” parameter (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 take the following steps:**

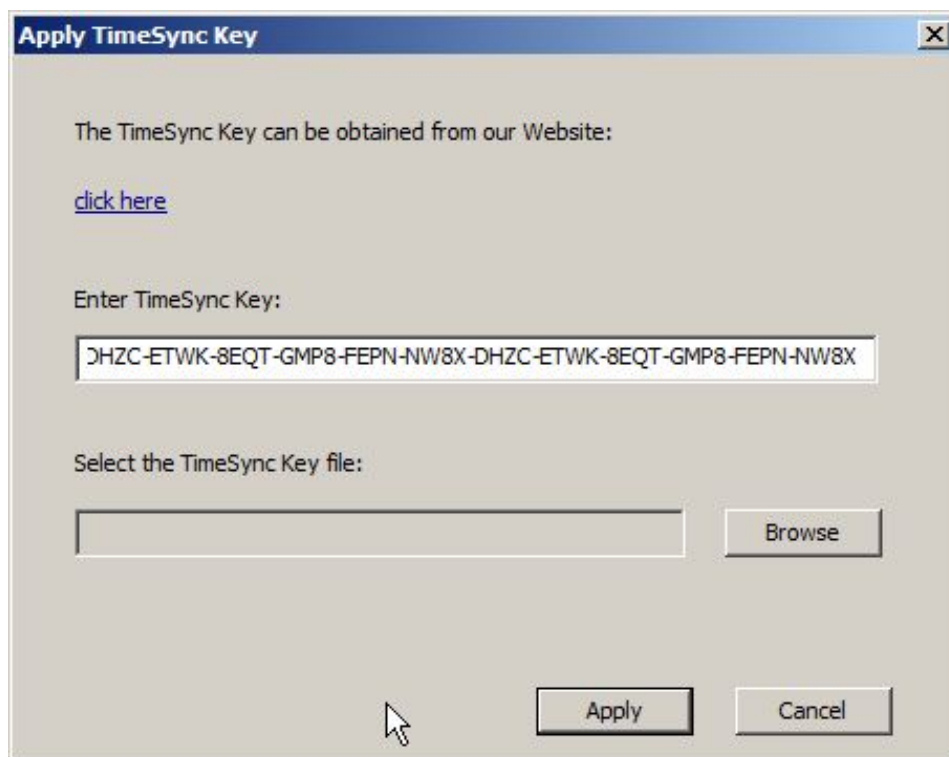
- start the FileLock GUI application and select the menu item "Configuration" → "Apply TimeSync"



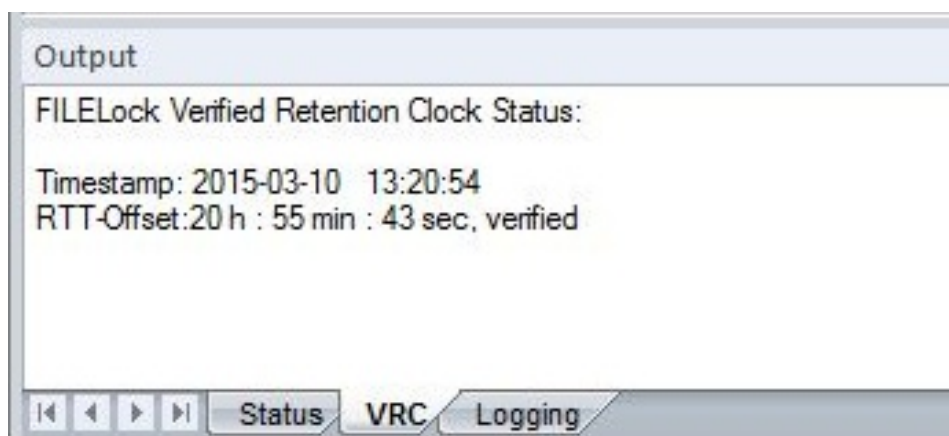
- click on the web link in the dialog below.



Copy the TimeSync key string from the web page directly to the corresponding dialog's input field and press the Apply button. Alternatively, you may save the key to a file first and select that file to apply the TimeSync key.

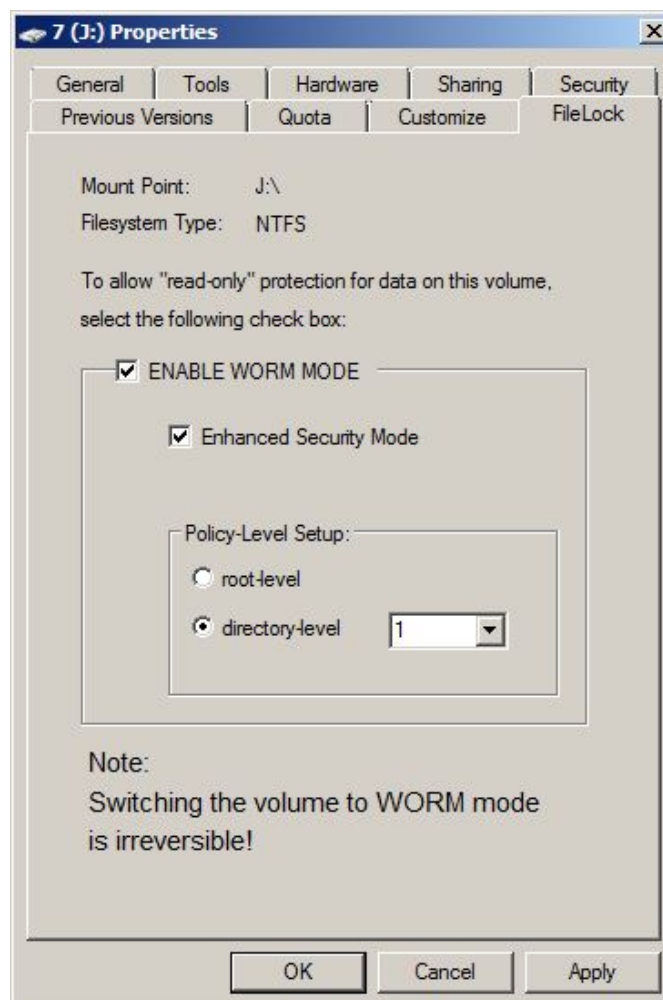


It may take up to 2 minutes until the system clock gets verified. The VRC information is displayed in the output panel view called "VRC" of the FileLock GUI application.



## 3.2. Setting up a WORM volume

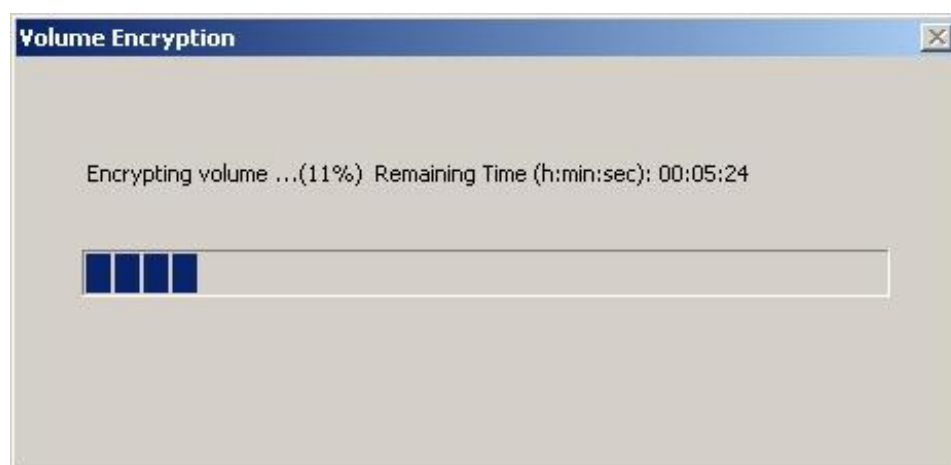
- For converting an NTFS or ReFS volume to a WORM volume, use MS Explorer, Disk Management or FileLock GUI to open the property page of the appropriate volume and select the FileLock tab. The FileLock tab in Explorer or Disk Management is only visible if you are logged in as the local administrator or as a domain administrator with special security options (see section [Troubleshooting for details](#)). Alternatively, you may run the FileLock GUI program, right-click the appropriate volume 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 in order to run the program with full elevated rights and privileges as an Administrator.
- To configure a volume for WORM you have to decide where protection policies can be configured. This could be defined on the root directory or on the 1st directory level. To activate WORM protection also a WORM policy has to be configured in the next step. If you need policies on a deeper directory level see chapter [Modification of Maximum Policy Folder Level](#).



- Select the “WORM MODE” checkbox and set up the directory-level, on which you want to configure protection policies.
- To save your settings, press the APPLY or OK button.
- Confirm you settings and press the OK button.



- After confirming the WORM – Mode, the whole volume is set to WORM status and can never return to non-WORM status.
- The volume will be encrypted after confirmation. This process could be long-lasting depending on the volume size, the amount of data blocks on the volume and your hardware



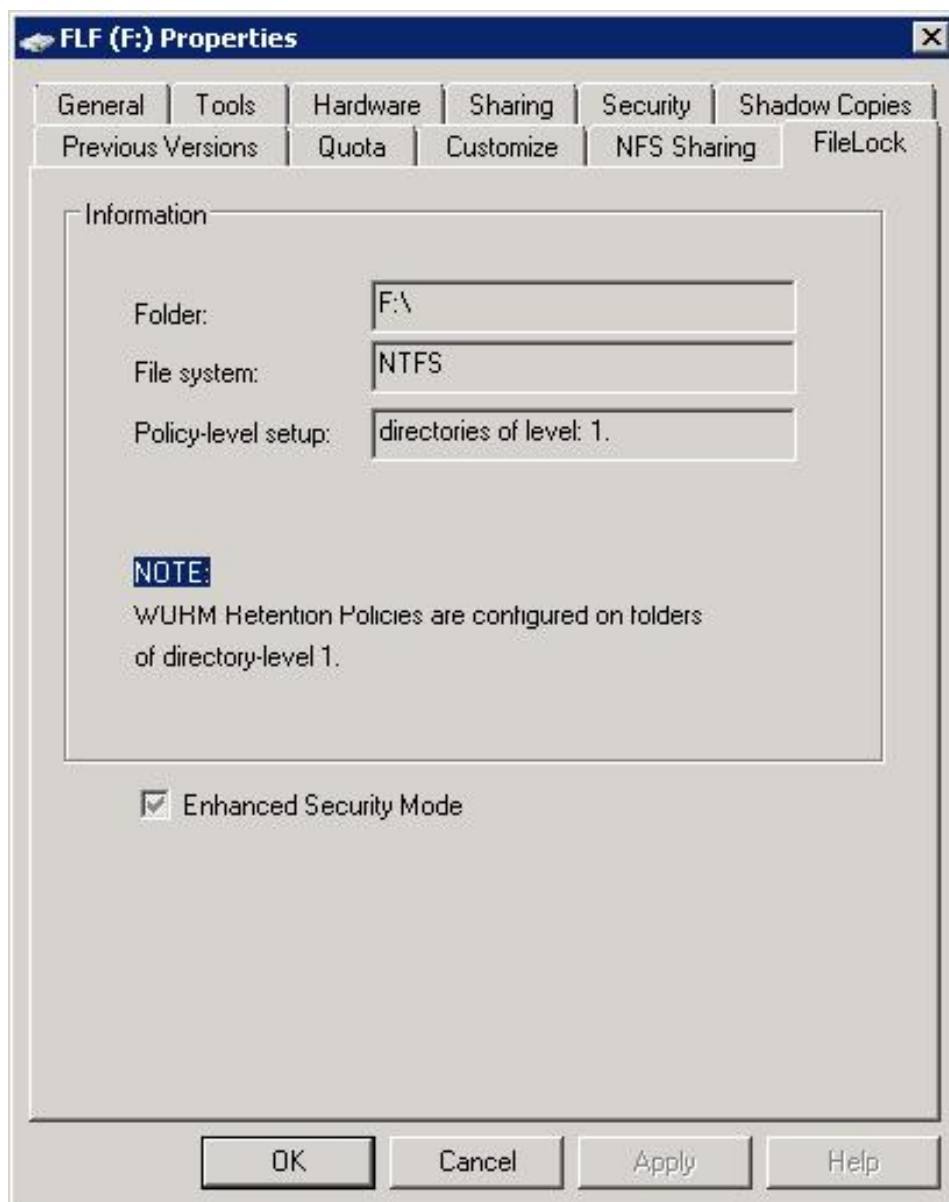
- Switch off the recycle bin functionality for the newly configured WORM volume

The Enhanced Security Mode should not be activated on a non-ESM WORM volume at a later time. ESM mode can not be switched off after its activation. See Chapter [Enhanced Security Mode](#) for details.



To prevent data loss activating ESM mode is refused by FileLock if the WORM volume contains more than 1GB of data.

(Only affects volumes from upgraded versions, where ESM was not mandatory)



(FileLock root directory tab information after converting a volume to WORM state.)

### 3.3. Protection policies and retention periods

After the base configuration of a WORM volume you have to setup the policies.

#### **The following rules apply to all WORM policies:**

- FileLock DLR and SFR policies may coexist on folders of the configured directory-level, except for policy on 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 may not be renamed.
- New created directories can be renamed and deleted as long as they are empty.

#### **Definition of Terms:**

##### **DLR (Directory Level Retention):**

The retention period is applied to all files within a certain directory and all its sub-directories.

##### **SFR (Single File Retention):**

Retention periods are related to individual files.

##### **Auto-commit:**

Files written into a certain location are committed to WORM state after a defined period of time (AUTOCOMMIT DELAY) by the FileLock Software. (No application activity is needed.)

##### **Application-commit:**

Files written into a certain location are NOT committed to WORM state without application activities. To set files to a WORM state the application has to follow the SnapLock procedure (Set the Read-Only Flag). Applies to SFR policies.

### **EBR (Event Based Retention):**

Files written to an EBR configured location are set on first WORM commit (via Auto-Commit or SnapLock interface) to infinite retention period if they do not have set an explicit retention date. This initial infinite retention period can be reduced once to a fixed retention date via the SnapLock interface. This new retention date is called Event Based Retention. After this event the retention times behave like any other Single File Retention and could be prolonged only. The retention times set via SnapLock are limited by the configured SFR policy values.



Empty Folders can be deleted and renamed.

### **3.3.1. Directory Level Retention**

The FileLock DLR policy determines the expiration date of a WORM file by adding the retention period, which is configured on the directory-level and inherited to all its sub-directories, to the WORM-commit timestamp of that file.

When using fixed date as retention policy, this fixed date is applied to all files after WORM-commit.

The DLR policy always uses the “auto-commit” mode. That means all files are set to WORM after the “AUTOCOMMIT DELAY” has passed. No file may stay on a non-worm status in such folders.

For DLR the expiration date is not attached to each file so you can easily increase the retention period of WORM files that are located in the same directory tree.

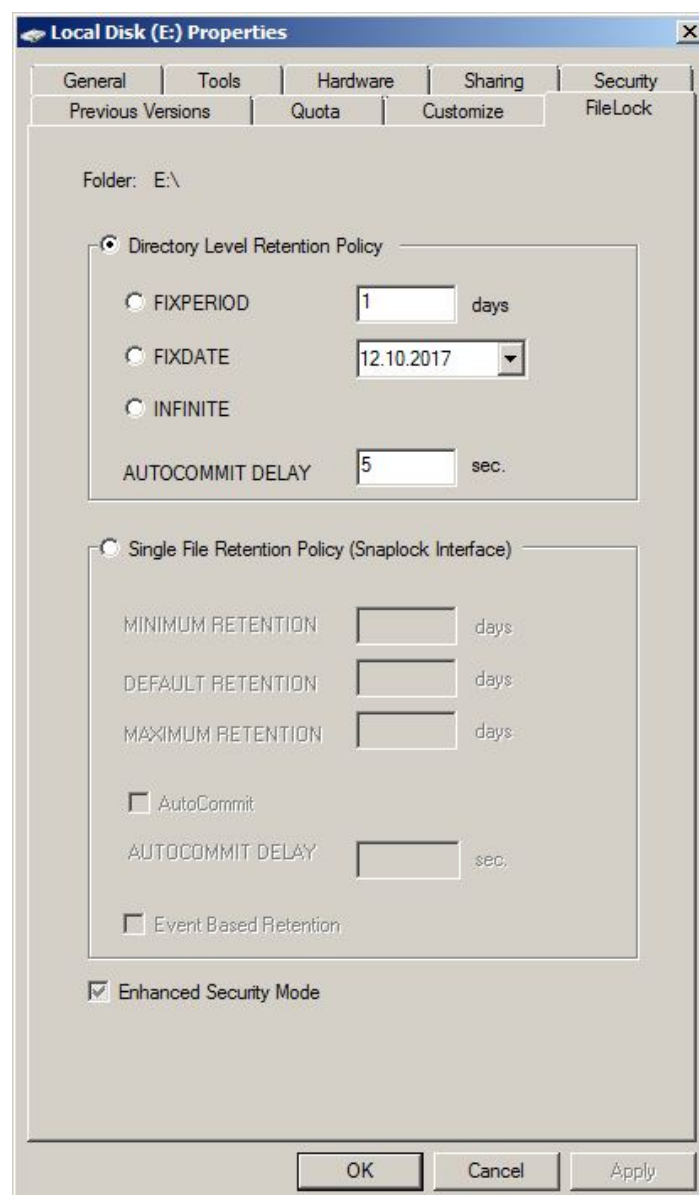


### 3.3.2. FileLock Directory Level Retention Policy

The FileLock DLR policy allows the configuration of a fixed period or infinite retention period or a fixed date when all files expire. Retention periods can be increased at any time, but it's not possible to decrease a retention period. Since FileLock associates the retention period defined on a directory with each WORM file inside that directory tree, extending the retention period will affect all WORM committed files.

The FileLock DLR policy automatically commits files to WORM after their creation, whereas the WORM trigger can be delayed by the AUTOCOMMIT DELAY parameter.

This value can be set between 0 and 3000000 seconds (~ 34.7 days). The value can be modified at any time (increase/decrease) to fit your needs. The following configuration dialog can be activated by right-clicking the appropriate folder using the MS Explorer and selecting "Properties" or "Configure" when using the FileLock GUI program.



**The following rules apply to WORM files covered by a FileLock DLR policy:**

- WORM files can not be modified, overwritten, renamed or deleted.
- WORM files can not be changed back to non-WORM files.
- File Metadata on WORM files can not be changed any more. However changing of security settings (ACL) is possible for migrating FileLock Servers into different ActiveDirectory Domains. Nevertheless we recommend to always use 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 expired WORM files covered by a FileLock DLR policy:**

- Expired files can only be deleted. Renaming or modifying an expired WORM file is not possible.
- Increasing the retention period of a DLR policy will also be reflected on expired WORM files, which means that an expired WORM file may be WORM protected again depending on the new retention period.

### 3.3.3. Single File Retention

The FileLock SFR policy allows the assignment of file expiration timestamp and WORM status at the granularity of individual files. Since the expiration date is written to the file's "last-access timestamp" (SnapLock Functionality), each WORM committed files can have an individual associated retention period. The expiration date is either set by an application through changing the file's last-access timestamp or the expiration date is derived from the configured default retention period, when the file is committed to the WORM state without modifying this timestamp.

The WORM commit operation is triggered either by an application by setting the read-only attribute of the file, or automatically after the Autocommit Delay has passed (autocommit mode).

In order to successfully commit a file to WORM state an application or user must convert the file from the writable to the read-only state after its creation on the SFR WORM storage by setting the read-only attribute. Files which have been set to read-only before they are copied to a SFR folder are not automatically set to the WORM state after copying them.

If autocommit mode is not active and the file's read-only attribute is not set via the application-commit mode, the file remains unprotected.

The auto-commit mode of the SFR policy is similar to the auto-commit mode of the DLR policy. When retention periods have to be prolonged in SFR configured directories, each WORM file has to be set individually to the new expiration date



Special rules apply when copying existing read-only files into a WORM volume with SFR policy attached. To trigger the WORM commit operation an application must set the read-only attribute after copying such files, even if the file has the attribute already set. Omitting to set the read-only attribute may result in read-only files which are not WORM committed.

This behavior is identical to NetApp SnapLock functionality. For details see NetApp KB: [https://kb.netapp.com/app/answers/answer\\_view/a\\_id/100413](https://kb.netapp.com/app/answers/answer_view/a_id/100413)

**FileLock Single File Retention Policy** The FileLockSFR policy provides compatibility with applications using the SnapLock interface to write data to a NetApp filer or similar systems.

**FLJ (J:) Properties** [X]

General | Tools | Hardware | Sharing | Security | Shadow Copies | Previous Versions | Quota | Customize | NFS Sharing | FileLock

Folder: J:\

☐ Directory Level Retention Policy

☐ FIXPERIOD  days

☐ FIXDATE  [v]

☐ INFINITE

AUTOCOMMIT DELAY  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

OK Cancel Apply Help

## **For Single File Retention it is mandatory to define the following values:**

### **MINIMUM RETENTION**

The value defines the minimal retention period that is used to calculate the minimum expiration date that can be set via the SnapLock interface.

If a file expiration timestamp earlier then the sum of the current timestamp and this minimum value is set, the resulting expiration timestamp is set to this sum on WORM commit.

The minimal allowed value is 0 days. The maximal allowed value is the configured MAXIMUM RETENTION.

### **DEFAULT RETENTION**

This value defines the default retention time used on a WORM commit if no retention time was defined via the SnapLock interface.

The allowed value is larger or equal to the MINIMUM RETENTION and less or equal to the MAXIMUM RETENTION.

### **MAXIMUM RETENTION**

This value marks the maximal retention period that can be set via the SnapLock interface.

If a file expiration timestamp later than the sum of the current timestamp and this maximum value is set, the resulting expiration timestamp is set to this sum on WORM commit.

The maximal allowed value is 3.651.770 days [~9998 years, means infinite in practice].

### **AUTOCOMMIT DELAY**

This value defines the time delay of the WORM file system when auto-committing new objects to the WORM state after the last file handle has been closed.

The maximal value is 3.000.000 seconds [~34,7 days].

This can be used to make sure that objects are WORM committed even if the process via SnapLock interface is not triggered.

On Autocommit the current DEFAULT RETENTION value is used unless an explicit retention timestamp has been set via SnapLock interface.

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

- Copy a writable file to a directory, which is covered by the SFR policy.
- Set the last-access timestamp of the file to the desired expiration date. If this step is skipped the “DEFAULT RETENTION” parameter is used.
- Setting the read-only attribute of the file triggers the WORM commit operation.

If the AutoCommit feature is enabled, files are automatically converted to the WORM state if they have not been modified for the specified AUTOCOMMIT DELAY.



Additionally the Microsoft Explorer context menu offers the service to set files to WORM or extend the retention time of WORM files residing on a path which is covered by a SFR policy.

**The following rules apply to WORM files covered by a FileLock SFR policy:**

- WORM files can not be modified, overwritten, renamed or deleted.
- WORM files can not be changed back to non-WORM files.
- WORM files reflect their expiration date in the last-access timestamp.
- Expiration dates can only be extended.
- Since the expiration date of a WORM file is stored in its last-access timestamp attributes, the last-access timestamp is not updated on a read access as on a standard NTFS or ReFS file system.
- File Metadata on WORM files can not be changed any more. However changing of security settings (ACL) is possible for migrating FileLock Servers into different ActiveDirectory Domains. Nevertheless we recommend to always use 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 expired WORM files covered by FileLock SFR policy:**

- FileLock permits applications to reset the read-only attribute of expired WORM files back to writable. However, the files remain in WORM-commited state.
- Expired files can only be deleted. Renaming or modifying an expired WORM file is not allowed.
- A new expiration date may be set on expired WORM files and the file's read-only attribute may be set again for re-committing the file to WORM state.

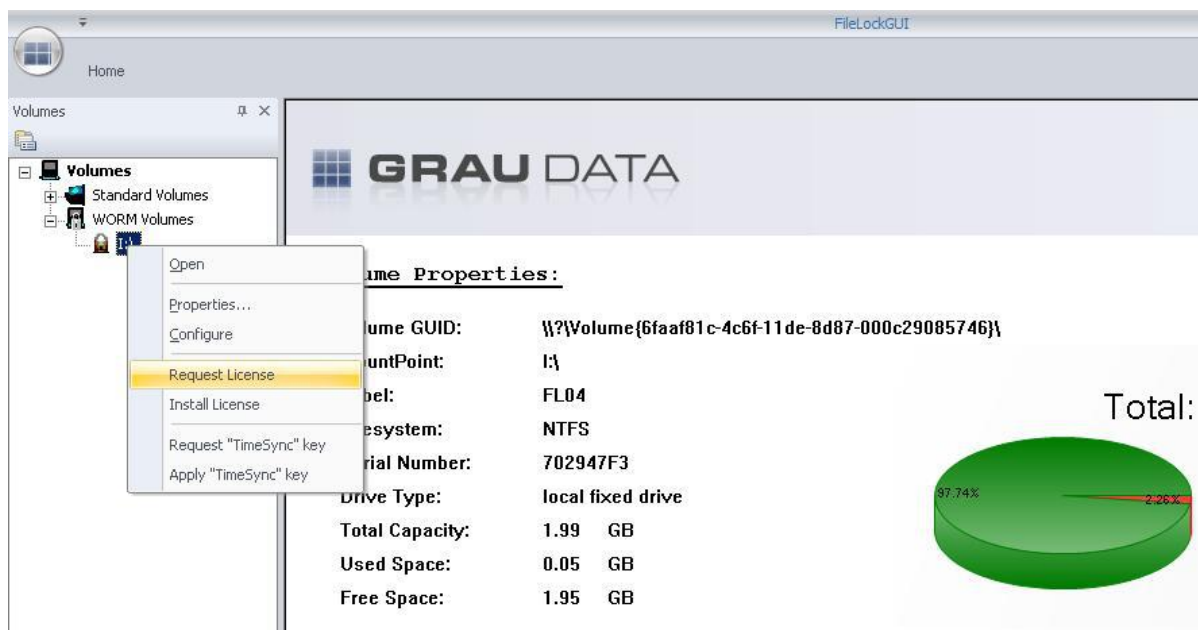
## 3.4. Obtaining and entering license keys

FileLock includes a trial license that allows the use of a WORM volume for 60 days. The trial license has neither a capacity limit nor a limit on the amount of WORM volumes. If you want to keep a WORM volume past the trial period, you need to register the volume while the trial license is valid to obtain a key for a permanent license.

Each WORM volume is registered separately and therefore has its own FileLock generated serial number, which is needed when requesting a permanent license key for a WORM volume.

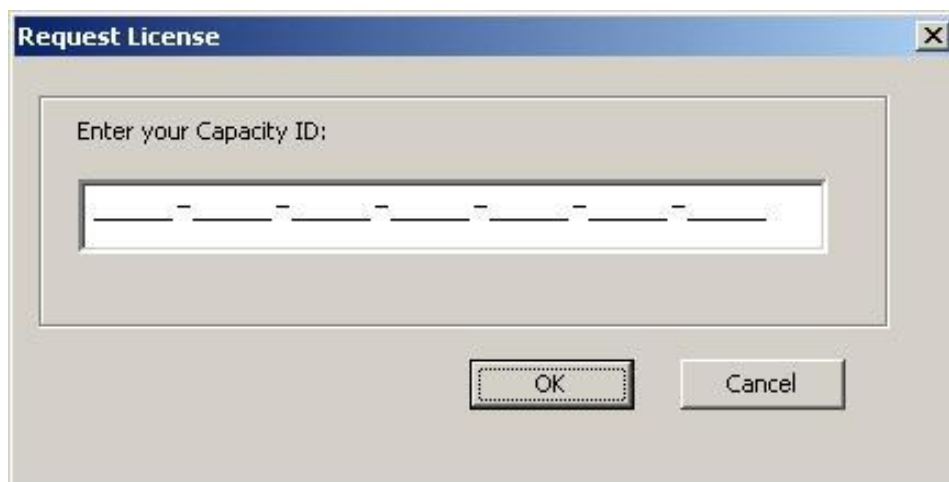
**To find the WORM volume serial number and install a permanent license, take the following steps:**

- In the Windows Start menu, select Programs "FileLock → FileLock GUI"
- In the FileLock user interface, select WORM volumes and right-click on the WORM volume for which you want to request a permanent license.
- Click "Request License"



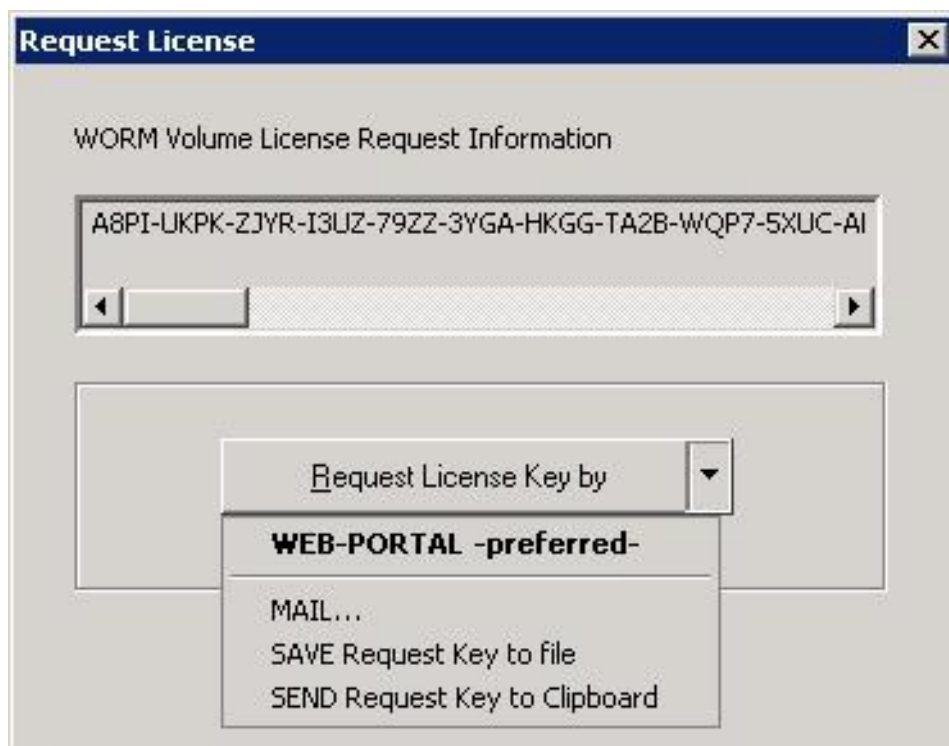


- Enter the Capacity-ID, which you have received from your FileLock sales representative. Characters are automatically converted to upper case when entering lower case.



A screenshot of a Windows-style dialog box titled "Request License". It has a blue title bar with a close button (X) in the top right corner. The main area is light gray and contains the text "Enter your Capacity ID:" above a white text input field. The input field has a dashed line indicating a specific format. At the bottom right, there are two buttons: "OK" and "Cancel".

- After pressing the "OK" button FileLock generates the license request key, which must be sent to the licensing service by using either the on-line WEB-PORTAL or sending the information via email.



A screenshot of the "Request License" dialog box after the "OK" button was pressed. The title bar remains the same. The main area now displays "WORM Volume License Request Information" above a text box containing the generated key: "A8PI-UKPK-ZJYR-I3UZ-79ZZ-3YGA-HKGG-TA2B-WQP7-5XUC-AI". Below the key is a horizontal scrollbar. At the bottom, there is a button labeled "Request License Key by" with a dropdown arrow. The dropdown menu is open, showing four options: "WEB-PORTAL -preferred-", "MAIL...", "SAVE Request Key to file", and "SEND Request Key to Clipboard".

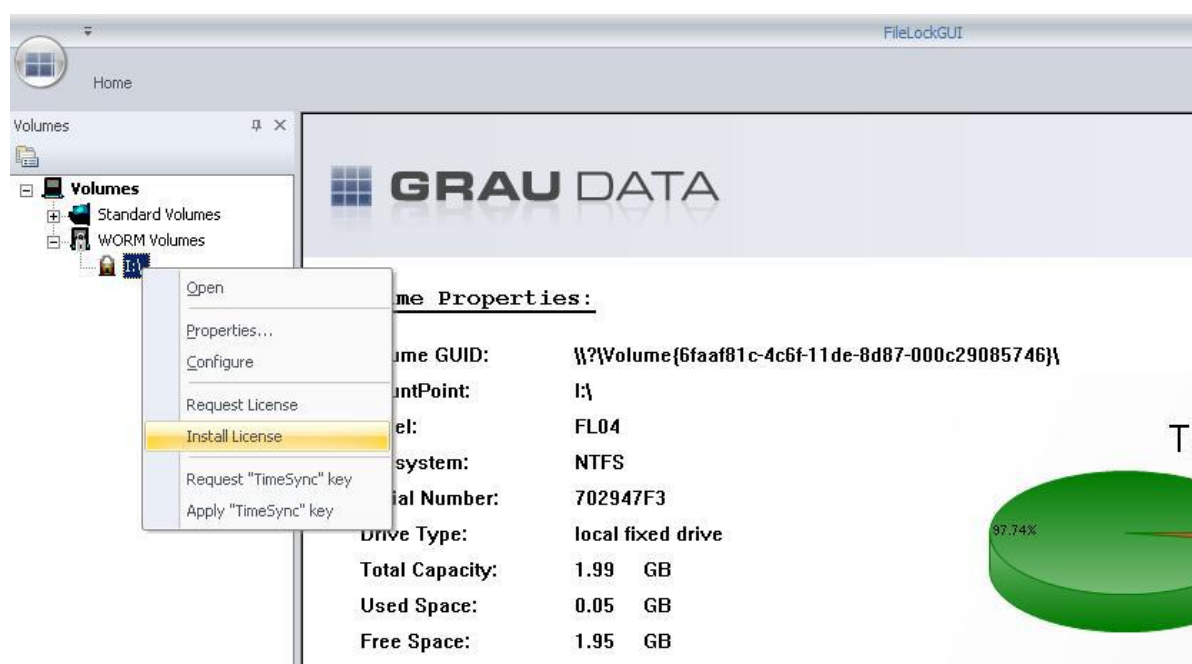
Please ensure that your server is connected to the internet, when choosing the "WEB-PORTAL" for requesting the license key.

To access the licensing service you have to log in to the WEB-PORTAL. If you do not yet have log-in credentials, please register and provide a valid email address, which is used by the licensing service to respond back to you.

- If you decide to send the license key request via email, you may either use the menu item "EMAIL...", which launches your email client and automatically generates an email with the necessary information or you may copy the license request key to a text file and send it as an email attachment to [support@graudata.com](mailto:support@graudata.com).

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

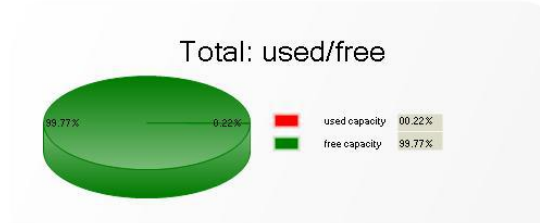
Alternatively select the menu item "Configuration" → "Install License Key(s)", which automatically assigns license keys to the corresponding WORM volumes.



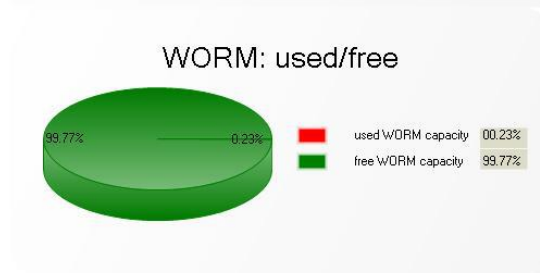
- Check the license status on the right-side pane of the FileLock GUI. It may take up to 4 minutes until the license status is updated.

**Volume Properties:**

Volume GUID: \\?\Volume{bb3341f7-2a5c-11de-a5ad-000c298f4d08}\  
MountPoint: G:\  
Label: FL03  
Filesystem: NTFS  
Serial Number: 482DE294  
Drive Type: local fixed drive  
Total Capacity: 4.00 GB  
Used Space: 0.01 GB  
Free Space: 3.99 GB



Access Mode: WORM  
Retention Time: 3650 day(s)  
License Type: permanent  
License Status: Valid  
Licensed Capacity: 4.00 GB  
free WORM Capacity: 3.99 GB



- After you have installed a permanent license, you can still add additional WORM capacity to a WORM volume by an add-on license. The new add-on license key is installed via the volume's context menu item "Install License" as well.

FileLock monitors the capacity on each WORM volume and displays a warning message in the application event log when a WORM volume comes close to its capacity limit. If the capacity limit is exceeded, write operations on the volume will be denied until additional WORM capacity is licensed for the volume.

The FileLock user interface provides an overview of the installed license types, status and used/free WORM capacity.

**SIMPLIFY COMPLIANCE –  
COST EFFECTIVE DATA ARCHIVING**

MountPoint	Label	Filesystem	Total [GB]	Free [GB]	Access Mode	Encryption	Key	Policy-Level	License	Lic. Status	Lic. Cap. [GB]	Free LicCap. [GB]	Lic. Expiration
E:\	Volume	NTFS	1.00	0.96	ACCESS DENIE...	FAST		1st. directory	temporary (60)	Expired	no limit	0.96	2014-12-27
F:\	Volume	NTFS	1.00	0.96	WORM (ESM)	FAST		root	temporary (60)	Valid	no limit	0.96	2015-05-03

## 3.5. WORM-TO-WORM Replication



The availability of any replication depends on the installed license.

### **FileLock provides the following replication facilities:**

- FileLock Replication Service
- Command Line Replication FileLockFSR

#### **3.5.1. FileLock Replication Service (FileLockRepSvc)**

This service is designed for automatic, one-way synchronization of FileLock WORM volumes. Files are expected to be added, changed or deleted in one location (Source) only. Therefore it is highly recommended to not add, update or delete files on the target location.

FileLock Replication Service keeps track of changes to files and directories on a WORM volume by monitoring the Windows USN Journal. Therefore changes on a volume are detected as they occur and the replication of the changes is triggered immediately. This approach provides an exact 1:1 replica of all files in the source location to the target location in real-time, preventing the need for more time consuming methods like scanning the entire source volume for changes. In addition all associated meta data of the original WORM file are maintained in the replicated file copy such as timestamps, attributes, file permissions and retention period.

Since files are pushed from source to target location asynchronously, there may occur a temporary difference between the two locations depending on the replication backlog. In case of a data loss situation the source volume can be replaced by the target volume without any additional modifications.

If the replication is configured for a non-empty WORM volume, a “manual” replication tree walk must be run in advance to get the target volume synchronized. The necessary tool FileLockFSR is explained in chapter [FileLockFSR](#).

## Configuring WORM volumes for replication

- Set up the source volume for WORM
- Set up the target volume for WORM (use identical set-up as source)

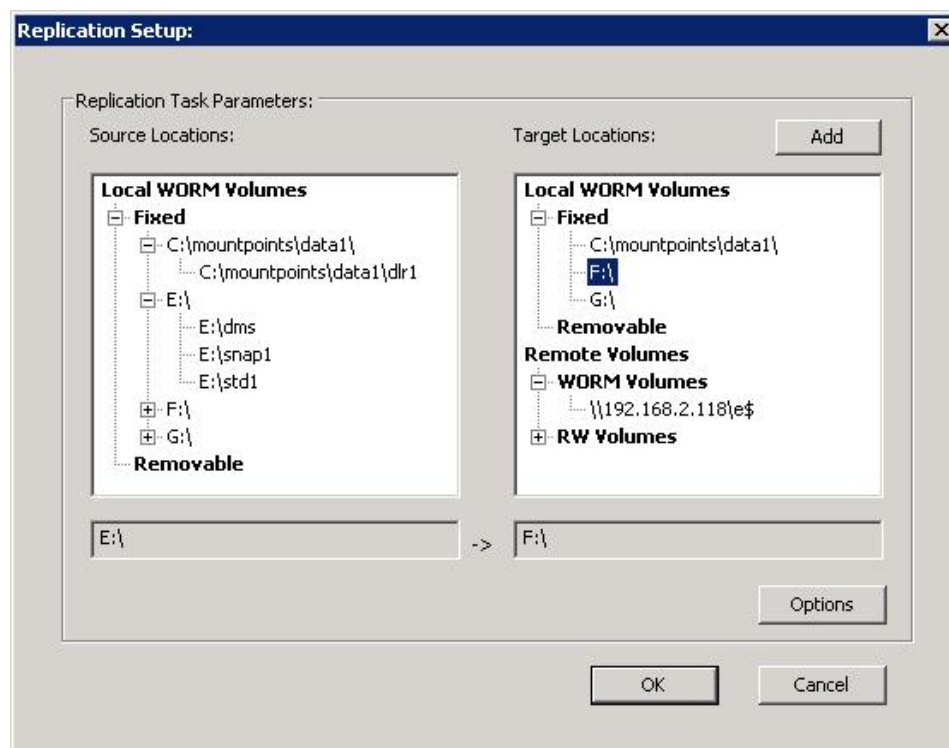


The WORM policy-level of the target volume must be equal or higher than the policy level of the source volume.

If the target volume is mounted on a remote system, create a share on the root directory of the target volume with the appropriate share permissions (FULL CONTROL) for the user account of the FileLockRepSvc service. The FileLockRepSvc service runs per default under the local system account, this needs to be changed to an account that can access the remote share.

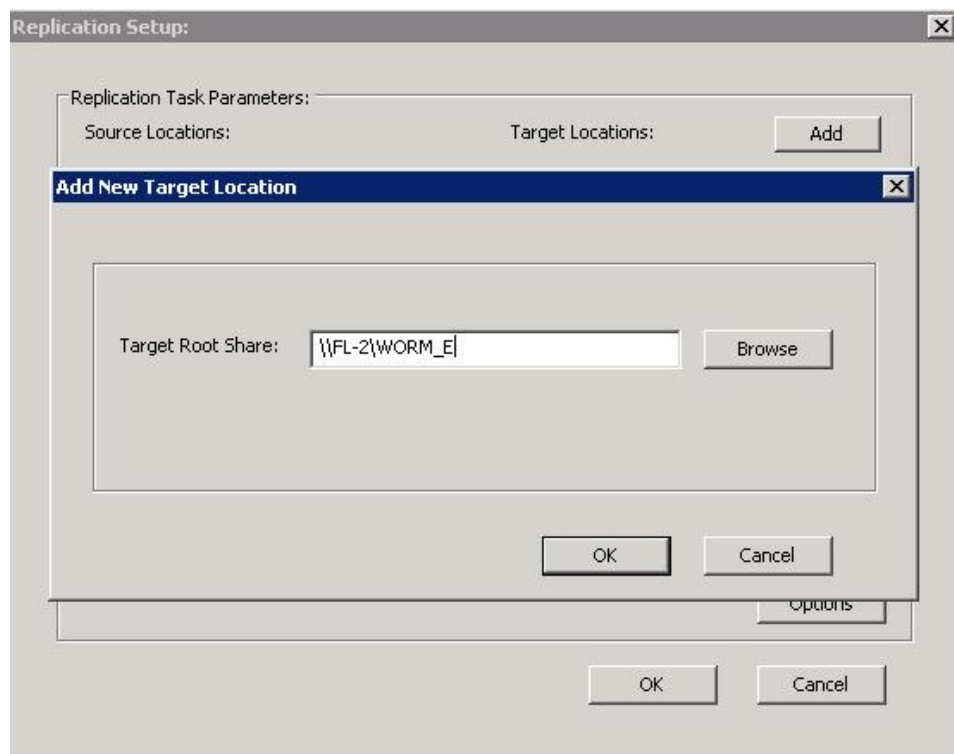
### Run the FileLock GUI application

- Select the menu item "Replication → Configure"



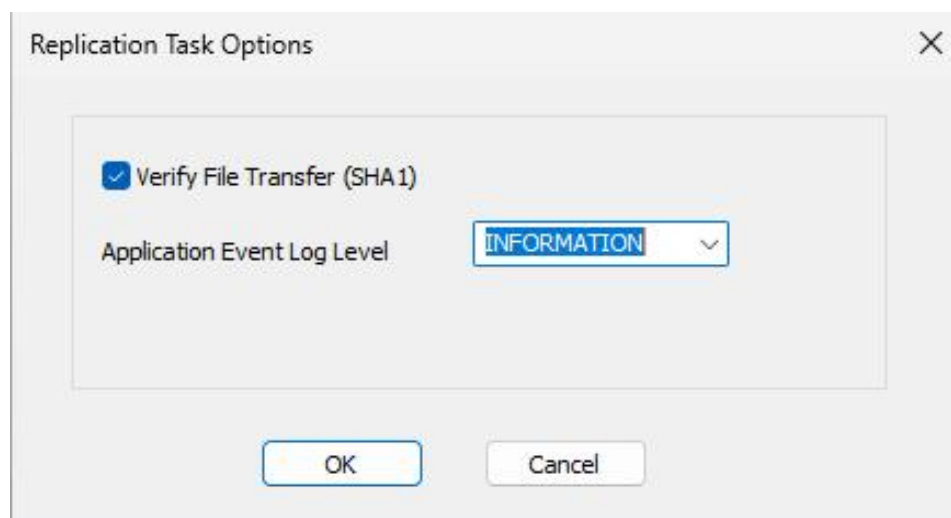
- Select the source location. A valid source location is either the root of a WORM volume or a folder with an attached WORM policy.

- Select the target location. If a remote target location is not available, use the ADD button to define the new location.



Depending on the source path selection, the corresponding target path is automatically determined. If the WORM policy-level of the target volume is greater than the policy-level of the source volume an additional directory is added on the target path. The directory name is the internal FileLock volume identifier of the source volume. Thus, several source WORM volumes can be combined on a single target WORM volume.

## Select Options



- **Verify File Transfer**

After file replication the SHA1 hash value of the content of the source and target file object is calculated and compared. The result is recorded in the replication logging file.

- **Windows Application Event Log Level**

**Press the OK button to save the replication task.**

**Set up the appropriate user for the FileLockRepSvc. The service must run under a user account with the following privileges:**

- Backup files and directories (SeBackupPrivilege)
- Restore files and directories (SeRestorePrivilege)
- Take ownership of files and other objects (SeTakeOwnershipPrivilege)
- Perform security-related functions (SeSecurityPrivilege)
- Receive notifications of changes to files or directories (SeChangeNotifyPrivilege)

See chapter [Missing privileges](#) for more details on privileges.

Additionally, the user account must have the appropriate Share Permissions (FULL\_CONTROL) on the target WORM volume(s)

After configuring the WORM volume for replication, proceed with creating your WORM folders on the source WORM volume and apply the appropriate FileLock WORM policies on the folders. The policies will be automatically replicated to the target volume.

### **Managing WORM volume replication**

Select the menu item "Replication → Display" of the FileLock GUI application

**When right-clicking on an entry in the replication task table, the following actions can be selected:**

- Enable / Disable replication
- Edit replication options
- Delete the replication task
- ReSync

Walks through the directory tree which is located under the directory <SourcePath> and checks each file entry in the tree, if it is a candidate for replication. The ReSync operation runs in parallel to the standard event-based replication.



## Monitoring WORM volume replication

### a) Using the FileLock GUI

Select the menu item "**Replication** → **Status**" of the FileLock GUI application

- replication backlog information

#### Replication Task Status:

Source Path	Target Path	Replication TaskID	Current SQN	Last SQN	ObjectsToADD	ObjectsToMove	Data To Transfer
C:\mountpoints\data...	G:\002616CB\dlr1	76f6b32c-b693-4e6b-ad39-baaa4fe3e216	11159	11159	0	0	0 kB
C:\mountpoints\data1\	\\FL-1\landingZone\	23dac4e3-d34b-4bf7-841d-df79e2cf2a4e	11159	11159	0	0	0 kB
E:\	F:\	a94f52d1-dec4-4643-bf2a-c6bdccc38396	171880	171880	0	0	0 kB
E:\dms	\\192.168.2.118\efs\dms	252284ef-f3a7-4b1e-b8a8-09edc7ad1e9f	171880	171880	0	0	0 kB

The Replication Task table shows the progress of the single tasks.

#### The values are:

- CurrentSQN:  
executed. sequence number of operation which has been already
- LastSQN:  
sequence number of last operation in the change journal.
- ObjectsToAdd:  
amount of file objects which need to be copied.
- ObjectsToMove:  
amount of file objects which need to be moved.
- DataToTransfer:  
outstanding amount of data which needs to be copied.

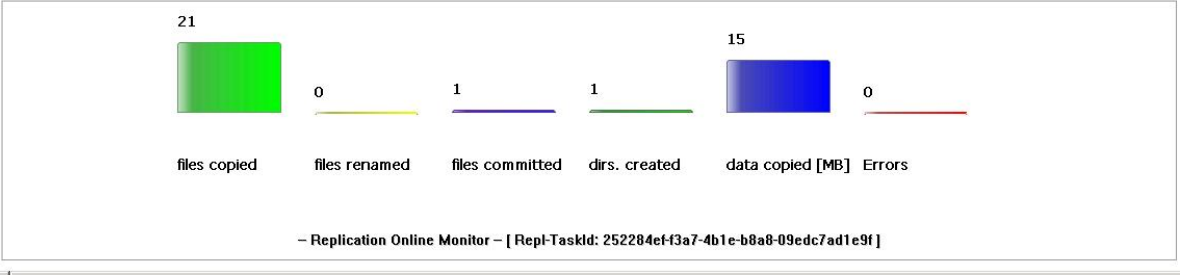
**When right-clicking on the corresponding replication task you may select the following information:**

- execution summary



**Replication Task Status:**

Source Path	Target Path	Replication TaskID	Current SQN	Last SQN	ObjectsToADD	ObjectsToMove	Data To Transfer
C:\mountpoints\data...	G:\002616CB\dir1	76f6b32c-b693-4e6b-ad39-baaa4fe3e216	11155	11155	0	0	0 kB
C:\mountpoints\data1\	\\FL-1\landingZone\	23dac4e3-d34b-4bf7-841d-df79e2cf2e4e	11155	11155	0	0	0 kB
F:\	E:\	b3e09dc4-d2a2-4898-96c4-1ca506b3758c	157613	157613	1	0	38 kB
E:\	F:\	a94f52d1-dec4-4643-bf2a-c6bdccce38396	171876	171876	0	0	0 kB
E:\dms	\\192.168.0.119\p...	252284ef-f3a7-4b1e-b8a8-09edc7ad1e9f	171876	171876	0	0	0 kB
Show execution summary							
Show file system summary							

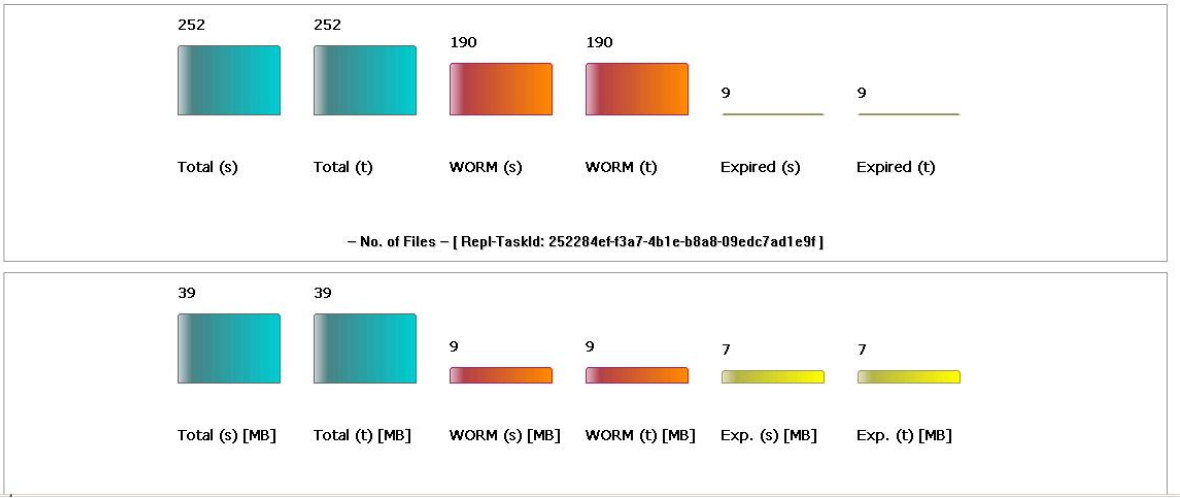


The execution summary gives information about processed file objects. The values are reset on each restart of the replication task.

- file system summary

**Replication Task Status:**

Source Path	Target Path	Replication TaskID	Current SQN	Last SQN	ObjectsToADD	ObjectsToMove	Data To Transfer
C:\mountpoints\data...	G:\002616CB\dir1	76f6b32c-b693-4e6b-ad39-baaa4fe3e216	11155	11155	0	0	0 kB
C:\mountpoints\data1\	\\FL-1\landingZone\	23dac4e3-d34b-4bf7-841d-df79e2cf2e4e	11155	11155	0	0	0 kB
F:\	E:\	b3e09dc4-d2a2-4898-96c4-1ca506b3758c	157613	157613	1	0	38 kB
E:\	F:\	a94f52d1-dec4-4643-bf2a-c6bdccce38396	171876	171876	0	0	0 kB
E:\dms	\\192.168.0.119\p...	252284ef-f3a7-4b1e-b8a8-09edc7ad1e9f	171876	171876	0	0	0 kB
Show execution summary							
Show file system summary							



The file system summary compares the amount of files and data capacity stored on source (s) and target (t) location.

The numbers are determined by scanning the file systems every two hours. The scan frequency can be adjusted by the registry value `StatScanInterval` in hours. The value "0" switches off file system scanning. `StatScanInterval` can be found under the registry key `HKEY_LOCAL_MACHINE\Software\GrauData\FileLock`. In order to keep the workload small the processing is executed by a background thread with low priority. Therefore the treewalk may take a considerable amount of time to complete for large file systems.

## **b) Locating the FileLock Replication log file**

The FileLockRepSvc service records replication activities in the file `<FileLock installation directory>\log\FIReplication.log`.

## **c) Windows Application Event Log**

Search for 'FileLockRepSvc' to find replication events.

## 3.5.2. FileLockFSR

### FileLockFSR

#### a) General Information

FileLockFSR is a command line tool and can be used to run manual or scheduled replication operations on FileLock WORM volumes. FileLockFSR determines the file candidates to be replicated by scanning the source and target volume for file differences.



FileLockFSR can only be executed on the WORM source and target volume of an existing replication task. (for further information see chapter [Configuring WORM volumes for replication](#))

#### b) Syntax

```
FileLockFSR <options> <source_path> <target_root_directory>
```

#### c) Options

<b>-l</b>	<b>&lt;logfile-path&gt;</b>
-----------	-----------------------------

<b>-c</b>	<b>verify checksums</b>
-----------	-------------------------

The SHA1 checksums of source and target files will be calculated and compared. Checksum mismatches will be reported in the fsr.log file.

<b>-o &lt;n&gt;</b>	<b>remove orphaned files on target location</b>
---------------------	---

This option deletes files on the target for which their counterparts on the source have already been deleted. The target files can only be deleted if they are expired at least for <n> days. Therefore expired files can be retained for a certain period of time.

<b>-t</b>	<b>simulation mode</b>
-----------	------------------------

## 3.6. Modification of Maximum Policy Folder Level

By default WORM protection and policies can be configured **EITHER** on the Root-level **OR** on any folder of the **1st directory-level**. If this is not adequate, the policy directory level can be increased by the registry value `MaxPolicyFolderLevel` to a maximum value of 9. `MaxPolicyFolderLevel` can be found under the registry key `HKEY_LOCAL_MACHINE\Software\GrauData\FileLock`. Please note, that you can not set policies on more than one directory level on a single WORM volume, but you can configure different WORM volumes with different policy directory levels. You can also set policies to some folders and leave others rewritable.

# Chapter 4. Best Practices

## 4.1. Data Protection

The following data protection strategies are available for FileLock WORM volumes:

### 4.1.1. WORM-TO-WORM Replication

FileLock Replication Service is configured at the volume level and maintains an exact 1:1 replica of the original WORM volume in real-time. Target volumes can reside on the same host or remotely on a warm-standby server.

WORM-TO-WORM replication significantly improves application reliability in the event of a disaster. If the primary WORM volume fails, businesses can switch to the target WORM volume immediately and use it as a new source WORM volume or the administrator can rebuild a new source WORM volume by copying the files from the target to a new source using FileLockFSR.

Since changes are propagated to the associated target locations as they occur rather than at discrete time intervals, replication provides users a higher level of protection than automatic backup at a certain time. Using scheduled automatic backups will cause data loss of all modifications made between the last backup and the point in time when the fault occurred.

Data replication combined with automatic backups offers the highest level of business continuity and safety.

### 4.1.2. Backup / Restore

In order to meet regulatory compliance rules and preserve the WORM aspects of the original files you have to 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 2 TB (GPT disk)
- Command line support  
This functionality is needed for automating backup and restore procedures.
- Optional Compression mode
- Optional Data Encryption

**The following Image Backup product has been evaluated with FileLock:**

- Image for Windows, TeraByte Inc. <http://www.terabyteunlimited.com/image-for-windows.htm>



- The option “Backup unused sectors” must be selected when backing up an ESM encrypted WORM volume on a GPT disks.
- A new permanent license key is required when restoring a WORM volume from a full image backup copy.

# Chapter 5. Troubleshooting

## 5.1. Reporting a Problem

For technical assistance with a registered version of FileLock, email your inquiries to [support@graudata.com](mailto:support@graudata.com).

**Please have the following information included in your email when you report a FileLock 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?

**FileLock Service Report:**

The FileLock 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 `<FileLock installation directory>\Diagnostics`.

**Additional informations:**

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



## 5.2. FileLock Tab is not available on MS Explorer's property page

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

**Please set up the User Account Control accordingly:**

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

If other domain admin accounts than the built-in domain administrator are used, the local security policy "**User Account Control: Run all administrators in Admin Approval Mode**" must be disabled.

## 5.3. Application event log message: "Invalid license"

**An invalid license may result from the following conditions:**

- The temporary license has expired.
- License information can't be read on the WORM volume. Please check, if the FileLock service is running.
- The WORM volume has been restored. In this case a new permanent license must be requested.

## 5.4. Missing privileges

The FileLock GUI and other FileLock components require certain privileges to run properly, so you have make sure, the user is able to gain such privileges.

The required privileges are:

- SE\_BACKUP (SeBackupPrivilege)
- SE\_RESTORE (SeRestorePrivilege)
- SE\_TAKE\_OWNERSHIP (SeTakeOwnershipPrivilege)
- SE\_LOAD\_DRIVER (SeLoadDriverPrivilege)
- SE\_SECURITY\_NAME (SeSecurityPrivilege)
- SE\_CHANGE\_NOTIFY\_NAME (SeChangeNotifyPrivilege)

In standard installations, any local or domain admin user is allowed to gain these privileges by default. However it is possible to restrict these privileges via local security policies or domain group policies. Please make sure to **not** restrict these policies for users who need to run the FileLock GUI or other FileLock tasks.

# Appx A: Filter - Compatibility

## Antivirus:

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

- Symantec AntiVirus
- McAfee VirusScan Enterprise
- TrendMicro ServerProtect
- Microsoft Defender



Compatibility of FileLock with antivirus solutions named above is subject to change. FileLock may not work with recent versions.



We strongly recommend to exclude all FileLock WORM volumes from automatic AV scan. Any attempt to quarantine WORM committed files may lead to unexpected behaviour.

## Replication:

3rd party replication tools are not tested with FileLock. Use [FileLock Replication](#) instead

## Last minute informations:

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

# Index

## A

Additional tasks, [10](#)  
Antivirus, [49](#)  
Application event log message, [47](#)  
Application-commit, [21](#)  
Auto-commit, [21](#)  
Autocommit Delay, [27](#)

## B

Backup / Restore, [44](#)  
Best Practices, [43](#)

## C

Complete Installation, [12](#)  
Configuration, [15](#)  
Configuring WORM volumes for replication, [35](#)

## D

Data Protection, [43](#)  
Default Retention, [27](#)  
Directory Level Retention, [2](#), [21](#), [22](#)  
DLR, [2](#), [21](#)

## E

EBR, [22](#)  
Enhanced Security Mode, [2](#)  
ESM, [2](#)  
Event Based Retention, [22](#)

## F

FileLock Directory Level Retention Policy, [23](#)  
FileLockFSR, [42](#)

## I

Installation, [6](#)  
Installation path, [10](#)  
Installation start, [11](#)  
Invalid license, [47](#)

## K

Key Features, [1](#)

## L

License Agreement, [9](#)

## M

Managing WORM volume repliactaion, [38](#)  
Maximum Retention, [27](#)  
Minimum Retention, [27](#)  
Missing privileges, [48](#)  
Modification of Maximum Policy Folder Level, [43](#)  
Monitoring WORM volume replication, [39](#)

## O

Obtaining and entering license keys, [30](#)

## P

Post-Installation, [13](#)  
Product Information, [1](#)  
Protection Policies, [1](#)  
Protection policies and retention periods, [21](#)

## R

Replication, [34](#), [49](#)  
Replication Service, [34](#)  
Reporting a Problem, [45](#)  
Restrictions, [5](#)

## S

Select target location, [36](#)  
Setting up a WORM volume, [18](#)  
SFR, [2](#), [21](#)  
Single File Retention, [2](#), [21](#), [25](#)  
Starting the Installation, [7](#)

## **T**

Troubleshooting, [45](#)

## **U**

Uninstallation, [14](#)

## **V**

Verified Retention Clock, [4](#)

VRC, [4](#)

## **W**

WORM-TO-WORM Replication, [34](#), [44](#)