Lockngo Professional

User Manual

Rev. 26-04.15

Updated for Version 7

Table of contents

1. System Requirements 3
2. Using Lockngo 3
2.1. The Lockngo user interface *3*
2.2. *Locking your portable drive using Lockngo* *5*
2.3. Unlocking your drive *5*
2.4. Visual feedback during drive unlock *6*
2.5. Lock reminder *6*
2.6. Auto lock *7*
2.7. Program Preferences *7*
3. Advanced features of Lockngo Professional 10
3.1. Private Directory *10*
3.2. Advanced command line functionality *10*
3.2.1. The command line *10*
3.2.2. Running Lockngo from the command line *10*
3.2.2.1. Available parameters *10*
3.2.2.2. Examples of use *10*
4. Important issues *11*
5. Frequently Asked Questions (FAQ) *11*

1. System Requirements

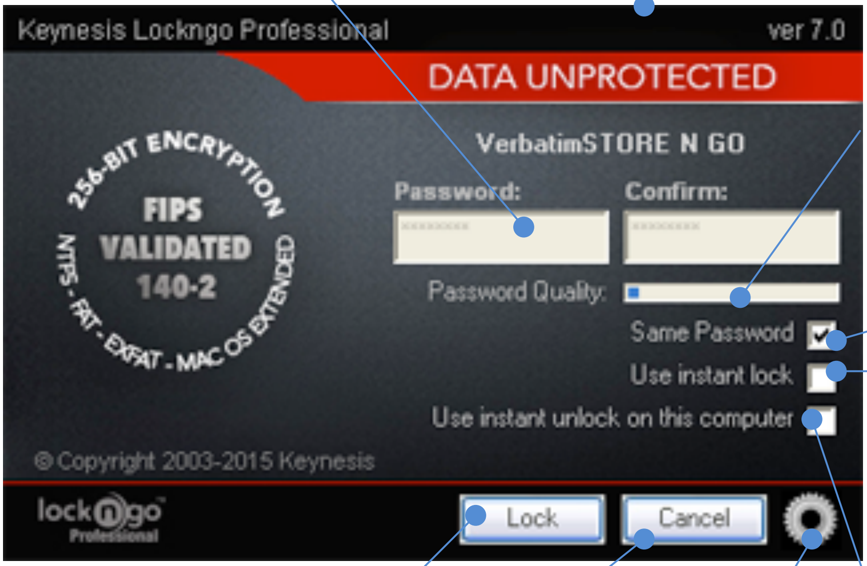
- Pentium and above
- 1MB of free space in the portable drive
- Supported operating systems: Windows 10, Windows 8, Windows 7, Windows Vista, Windows XP, Windows 2000, Windows Server 2003® versions.
- **Important**: Lockngo requires administrative privileges
- Supported file systems: FAT, FAT32, exFat, and NTFS file systems
- Supported media types: Flash memory drives and external hard drives of any size including Advanced Format (AF) disks.

2. Using Lockngo

2.1. The Lockngo user interface

Password entry text boxes

Lockngo title bar – use it to move Lockngo



Password quality indicator

Hide password while typing

Skips the lock screen. Double click Lockngo application to protect files.

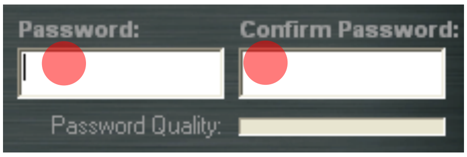
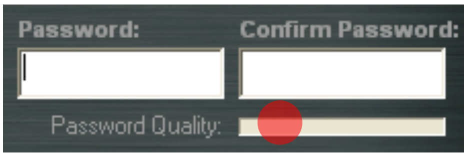
Figure 1 - Lock window

The lock button encrypts and hides your data

Cancel button closes Locngo without Locking

Program preferences

Skip the unlock screen on this computer

"**Password**" –you are required to select a password to protect your drive. You are required to fill in at least one character in the password field. To keep your data from being compromised, try to select a password that will not be easy to guess. A strong password usually contains character symbols ($@^) and a combination of lowercase and uppercase characters. Important: Lockngo has no "back doors". This means that if you forget your password, even we will not be able to unlock it for you, and you will be forced to format it.	
"**Password Quality**" - Graphical indicator for evaluation of your password quality.	
"**Hide Password**" - uncheck this option to make your password visible while you type	
"**Use instant Lock**" - Checking this option will allow you to lock your data instantly by double-clicking the Lockngo icon in your drive. When you use this function, Lockngo will use your current password. **To turn this feature off:** Lock your drive by double clicking the Lockngo icon. After the drive has been locked, double-click the Lockngo icon again to show the Unlock screen. Uncheck the Use Instant Lock option and click Unlock. Next time you launch Lockngo, it will be back in its default state, showing the lock screen.	
"**Use instant unlock on this computer**" – save password to this computer and use it for unlocking the drive.	

Activate this option only for trusted computers. If it is activated disk will be unlocked instantly when Lockngo is running from locked disk on this computer.	

2.2. Locking your portable drive using Lockngo

Locking your drive requires you to select a password, confirm it and click the 'Lock' button.

During drive lock, the Lockngo user interface will close along with your drive explore window.
During its locking operation, Lockngo displays its process dialog.

Locking...

Please wait

Figure 2 – Locking window

2.3. Unlocking your drive

Run Lockngo by double clicking on the Lockngo.exe inside the locked drive. Type the exact same password you used to lock the drive. Click the 'Unlock' button and wait for the unlock process to complete.

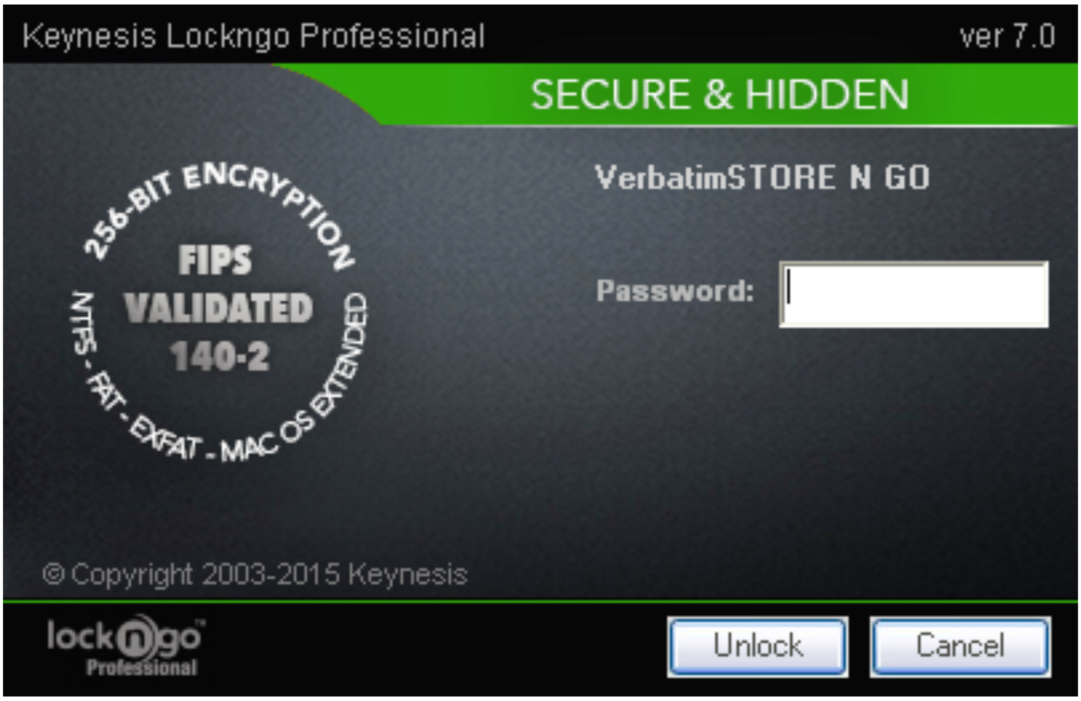
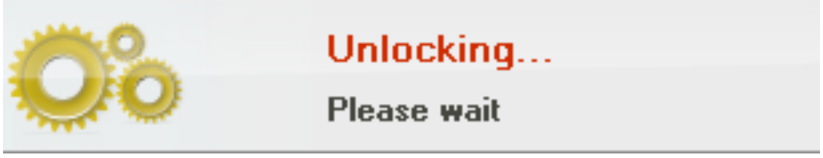


Figure 3 – Unlock window

2.4. Visual feedback during drive unlock

During drive unlock, the Lockngo user interface will close along with the explorer window of your drive. An "Unlocking…" message will appear. Next, the explorer window of the drive should reappear, showing the entire content of the drive.



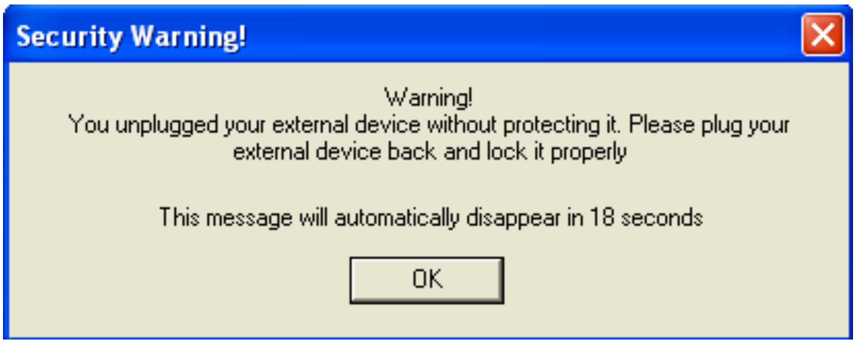
Unlocking...

Please wait

Figure 4 – Unlocking window

2.5. Lock reminder

If Lockngo was used to unlock the drive to access its content, and later the drive is unplugged unlocked, an alert window will appear reminding to lock the drive. This alert window can be turned off manually by clicking the "OK" button in the alert window. This alert window will self-close in 25 seconds if the "OK" button was not pressed manually.



Security Warning!

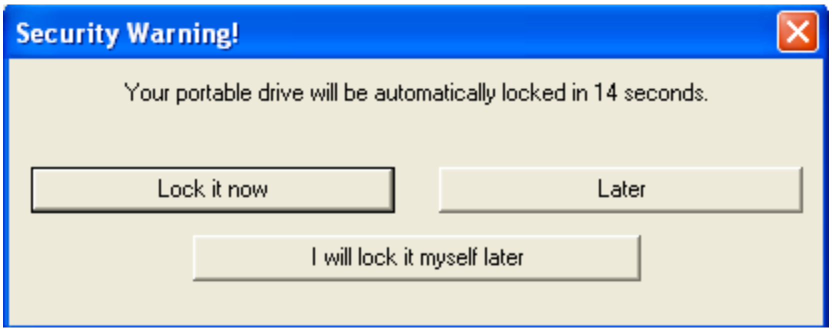
Warning!
You unplugged your external device without protecting it. Please plug your external device back and lock it properly

This message will automatically disappear in 18 seconds

Figure 5 – Lock remainder

2.6. Auto lock

The drive will be automatically locked automatically if you don’t work with computer during 10 minutes. Before locking drive Lockngo will show following window:



Security Warning!

Your portable drive will be automatically locked in 14 seconds.

Figure 6 – auto-lock dialog

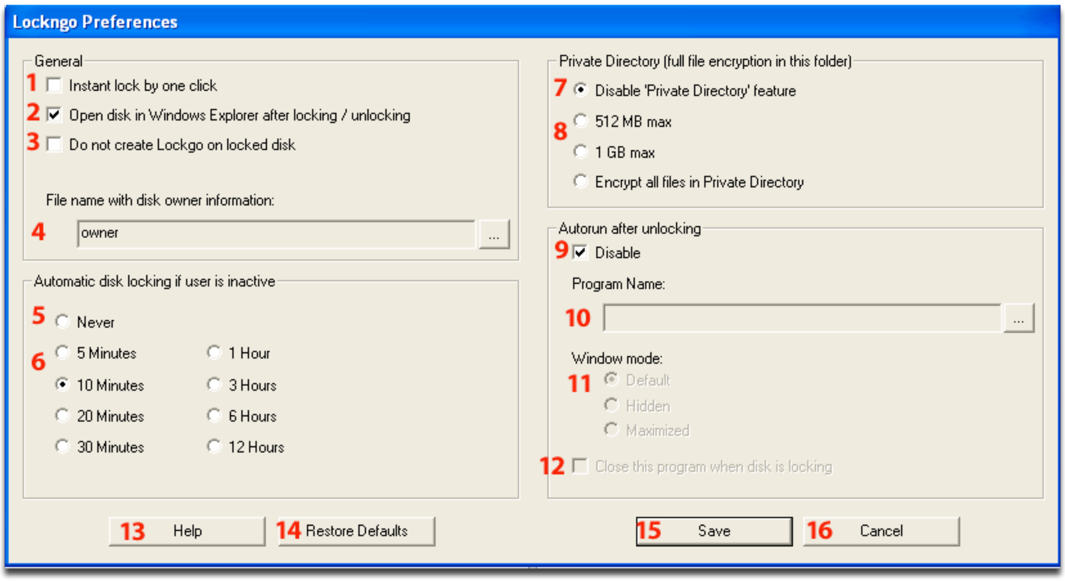
This dialog allows you to lock the drive immediately, postpone locking, or cancel this operation.
If you don’t do click any buttons during 25 seconds the drive will be locked with the previously used password.

Lock it now	Lock drive immediately with last used password
Later	Cancel this operation now and show this dialog next time when computer has not been used during 10 minutes.
I will lock it myself later	Cancel this operation now and disable auto-locking till the next time when disk is unlocked. Delay in 10 minutes can be changed or disabled (see Program Preferences)

2.7. Program Preferences

The program does not require changing its properties. It can be used immediately after installation to disk with default preferences.

Preferences window allows changing the default values if it is necessary.



Lockngo Preferences

General

1 □ Instant lock by one click

2 ☑ Open disk in Windows Explorer after locking / unlocking

3 □ Do not create Lockgo on locked disk

File name with disk owner information:

4 owner

Automatic disk locking if user is inactive

5 ○ Never

6 ○ 5 Minutes ○ 1 Hour

● 10 Minutes ○ 3 Hours

○ 20 Minutes ○ 6 Hours

○ 30 Minutes ○ 12 Hours

Private Directory (full file encryption in this folder)

7 ● Disable 'Private Directory' feature

8 ○ 512 MB max

○ 1 GB max

○ Encrypt all files in Private Directory

Autorun after unlocking

9 ☑ Disable

Program Name:

10

Window mode:

11 ● Default

○ Hidden

○ Maximized

12 □ Close this program when disk is locking

Figure 7 – Lockngo Preferences window

General	
1. Instant lock by one click	Checking this option will allow you to lock your data instantly by double-clicking the Lockngo icon in your drive. When you use this function, Lockngo will use your current password. **To turn this feature off:** Lock your drive by double clicking the Lockngo icon. After the drive has been locked, double-click the Lockngo icon again to show the Unlock screen. Uncheck the Use Instant Lock option and click Unlock. Next time you launch Lockngo, it will be back in its default state, showing the lock screen.
2. Open disk in Windows Explorer after locking / unlocking	If it is not checked Lockngo will not open Explorer neither after locking nor after unlocking.
3. Do not create Lockngo on locked disk	
4. File name with disk owner information	Lockngo Professional allows you to save a special personal details file in your removable drive's root directory. You can use this file to include your personal information and contact details, so that if the drive is found by anyone, it can be safely returned to you. Your personal details file will be excluded from

	the locking process and will remain available even when your drive is locked. The file can be of any type (textual, graphical, etc.). Make sure you keep the file size below 150 KB and its name contains only ASCII characters (don't use national alphabets in the file name).
Automatic disk locking if user is not active	
5. Never	Disable this feature
6. 5 minutes – 12 hours	Defines delay for Auto – locking function. Disk will be locked automatically if user does not work with computer during this time. See "Auto lock"
Private Directory (full file encryption in this folder)	
7. Disable "Private Directory" feature	Disable this feature.
8. 512MB – 1GB	Defines maximum limit for files in the Private Directory folder which should be fully encrypted. **Attention**: encryption of large amount of data is very time consuming operation. It may significantly increase locking / unlocking time. Make sure that you place into Private Directory only the most confidential files!
Autorun after unlocking	
9. Disable	Disable this feature.
10. Program name	The name of the application that should be executed. Do not include drive letter. If your application is located outside the root directory of your removable drive, you must include the relative path to it, starting from the root level, omitting the drive letter. If your application requires some command line parameters, include them right after its name.
11. Windows mode	Defines the window mode in which your application will open.
12. Close this program when disk is locking	Defines whether Lockngo will try to close the application before locking a disk. In case your application fails to terminate (for example while waiting for user input) Lockngo will make ten attempts to close it, waiting one second between each attempt. If the application still fails to shut down, Lockngo will disregard it and will start the locking process.
13. Button "Help"	Open a web page with help information for this window

14. Button “Restore Defaults”	Restore defaults values.
15. Button “Save”	Save updated parameters and close the window.
16. Button “Cancel”	Cancel changes and close the window.

3. Advanced features of Lockngo Professional

3.1. Private Directory

Lockngo Professional allows you to protect the most sensitive data by full encryption of such files. These files must be placed into the folder “Private Directory” on the external drive. Lockngo will encrypt them every time when disk is locking.
Since this operation is very time consuming it may increase locking and unlocking time. The total size of these files should not be more than 500Mb. If there are more that 500Mb in this folder than will be encrypted only the first 500Mb. This limit may be changed in Program Preferences.

The folder “Private Directory” will be automatically created after the first disk lock.

3.2. Advanced command line functionality

3.2.1. The command line

Command line window is sometimes referred to as a DOS window.

You can open the command line window by doing one of the following:

Sending command line actions to Lockngo from the 'Run…' menu (all versions of Windows): from the Windows Start menu select 'Run…". In the 'Open' text box type the drive letter where lockngo.exe is located (for example: x:\) followed by the command you wish to send to Lockngo and then press OK.

3.2.2. Running Lockngo from the command line

This option allows you to run Lockngo with certain features enabled or disabled directly from the command line. This can be handy if you would like to automate the usage of Lockngo using batch files for example.

3.2.2.1. Available parameters

Flag	**Mandatory**	**Description**
-p:<password>	★	This flag is the password flag and therefore mandatory (cannot be empty).

3.2.2.2. Examples of use

Example: Bypass lock window (lock without 'entire drive encryption').

```
Lockngo.exe –p:1234
```

Result: Lockngo will be executed and immediately lock the portable drive with the password '1234' without asking the user for any input and without showing the Lockngo user interface. During locking the 'locking' message will appear to indicate that the drive is being locked. The Lockngo user interface will only appear when Lockngo is executed when drive is locked – to allow the user to enter the password to unlock the drive.

Please note: it is also possible to unlock the drive from the command line. To unlock, just use:

```
Lockngo.exe –p:<the password you used for locking>
```

4. Important issues

Data backup

It is always a good practice to backup your data. Backing up your data will assure that if your drive is lost, stolen or if your data is deleted or corrupted for any reason (such as power shortage, accidental delete or format) you will have still have a safe copy. Please make sure to backup your data on a regular basis.

Backup copy of Lockngo

Always keep a backup copy of Lockngo. This might become handy if you accidentally delete Lockngo from your drive or if the file Lockngo.exe file is corrupted. This might happen in rare cases of power shortage during drive locking or in cases of a removable drive that was plugged out during the read or write operation. If, for some reason, Lockngo.exe does not work from your drive, copy the backup copy of Lockngo onto your drive (overwriting the existing file) and run it.

Uninstalling other removable drive utilities before using Lockngo

If you are using, or have installed any other removable drive software, we recommend uninstalling it before using Lockngo.

5. Frequently Asked Questions (FAQ)

Please refer to the Keynesis website for Frequent Asked Questions: www.keynesis.com/faq.

This document is subject to change without prior notice. Keynesis assumes no responsibility for any errors that may appear in this document. Keynesis products are not warranted to operate without failure.