Keynesis Ltd.
www.keynesis.com

Lockngo Professional

User Manual

Rev. 29-08.11

Updated for Version 5

Keynesis Ltd.
www.keynesis.com

Table of contents

Keynesis Ltd.
www.keynesis.com

1. **System Requirements**

    ▪   *Pentium III and above*

    ▪   *1MB of free space in the portable drive*

    ▪   *Supported operating systems: Windows 7, Windows Vista, Windows XP, Windows 2000, Windows 98® Second Edition, Windows Me®, Windows Server 2003® versions.*

    ▪   ***Important****: Running Lockngo on Windows 7, XP, Windows 2000 and Windows 2003 requires administrative privileges*

    ▪   *Supported file systems: FAT, FAT32, exFat, and NTFS file systems*

    ▪   *Supported media types: Flash memory drives and external hard drives*

2. **Using Lockngo**

2.1. **The Lockngo user interface**

Lockngo title bar – use it to move Lockngo on your screen

Password entry text boxes

Password quality indicator

Hide password while typing

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

Figure 1: The user interface

The lock button encrypts and hides your data

Cancel button closes Lockngo without Locking

Keynesis Ltd.
www.keynesis.com
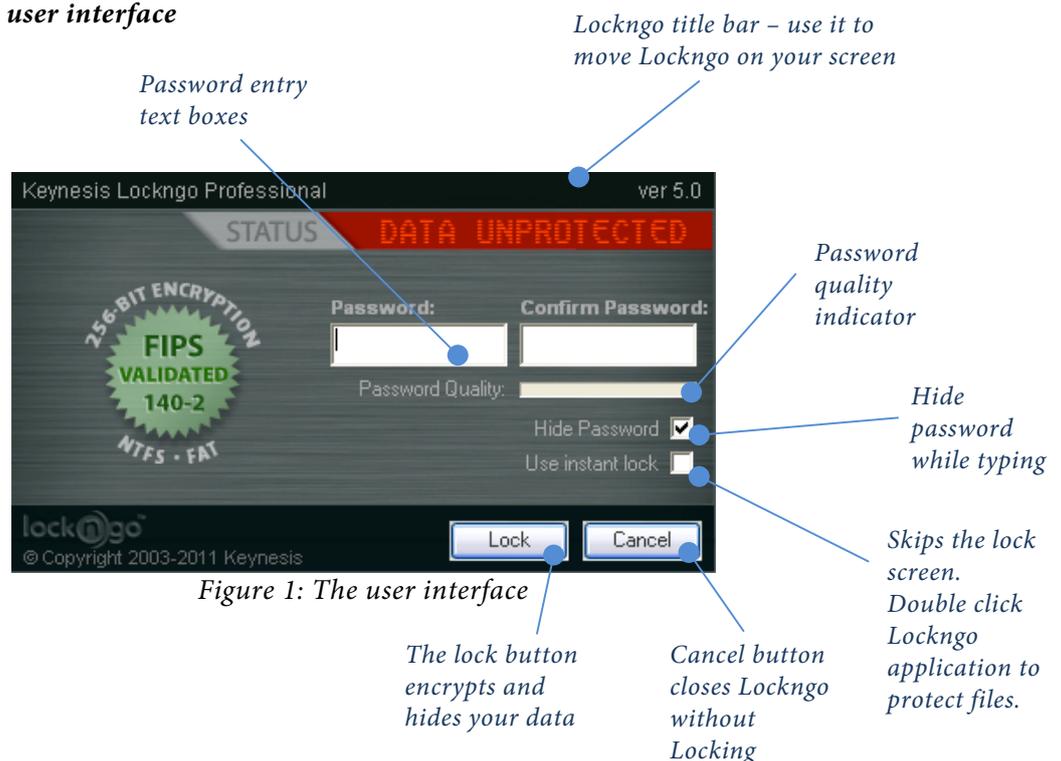
*"**Password**" –you are required to select a password to protect your drive. You are required to fill in at least one character in the password field.*

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.

2.2. *Locking your portable drive using Lockngo*

Locking your drive requires you to select a password, confirm it and click the 'Lock' button.
* For additional, more advanced features, please refer to the '<u>Advanced features of Lockngo</u>' chapter.

Keynesis Ltd.
www.keynesis.com

During drive lock, the Lockngo user interface will close along with your drive's explore window.

During its locking operation, Lockngo displays its process dialog. To make sure you are notified when Lockngo completes its locking operation, leave the 'Always on top' option checked. Alternatively, you can check off this option to have the process dialog out of the way of other windows.

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.
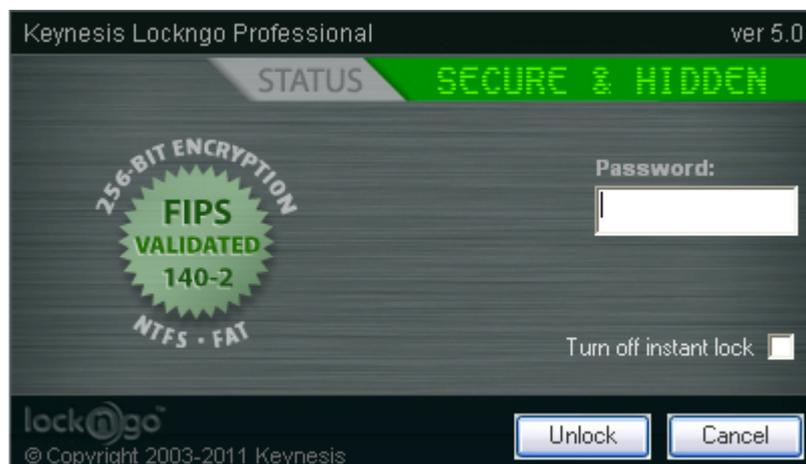

Figure 7: Unlock screen

2.4. 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.

2.5. 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:

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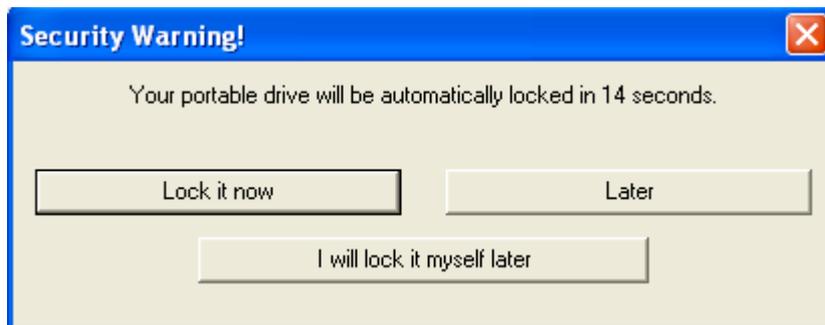
This dialog allows you to lock the drive immediately, postpone locking, or cancel this operation.
If you don't do click any buttons during 25 seconds the drive will be locked with the previously used password.

 "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 <u>Advanced features of Lockngo'</u>).

2.6. 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.

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 should 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.
The folder "Private Directory" will be automatically created after the first disk lock.

3.2. Special file exclusion

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.

To create a personal details file, please follow the instructions below:

- *Create a file containing your personal details such as your name, address and phone number. The file can be of any type (textual, graphical, etc.). Make sure you keep the file size below 150 KB.*
- *Name your file 'owner.*' (depending on its type. For example: for text file you will name your file "owner.txt".*
- *Try to lock your drive making sure it is still accessible. (if not, double check your file's name)*

3.3. Automatically launching applications after Unlock operation

As of version 3.4 it is possible to automatically launch an application after a successful unlocking operation.

To set this option, create a file named "autorun.l&g", and place it in the root directory of your removable drive.

Note: The file will be hidden when the disk is locked, this behavior is normal.

The file must contain the mandatory parameters below:

Parameter	Mandatory	Description
open	★	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 (see examples). If your application requires some command line parameters, include them right after its name (see examples).
window		Defines the window mode in which your application will open. Possible values are: normal(default), minimize, maximize, hide
close		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

Keynesis Ltd.
www.keynesis.com

		locking process. Possible values: yes, no. If set to "no" Lockngo will not open Explorer neither after locking nor after unlocking
explorer		

Notes:
1. *Each parameter should be written in a separate line.*
2. *Parameter names should be all lower case.*
3. *Between the parameter names and their values a"=" sign must be included with no spaces before or after it.*

Examples:

Example 1 – notepad should be launched with a specific file for editing. It should open in a maximized window, and should be closed before the disk is locked.

open=notepad.exe C:\WINDOWS\nsw.log
window=maximize
close=yes

Example 2 – Firefox should be launched. In this example, its executable file is located in a removable drive - under directory X:\firefox\ (X – portable drive letter as assigned by the system).

open=firefox\firefox.exe

Keynesis Ltd.
www.keynesis.com

3.4. Advanced command line functionality

3.4.1. General

Command line features are mainly intended for configuring Lockngo for predefined behavior, while simplifying or limiting its user interface operation.

Command line actions are divided into two categories:
1. Running Lockngo directly from the command line; and
2. Setting and storing parameters inside the Lockngo file.

3.4.2. 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.
Example:
x:\lockngo.exe –dap –p:1234

Opening the command line window in Windows 2000/XP/Vista/7: from the Windows Start menu, select 'Run…". In the 'Open' text box type 'cmd' (without the apostrophes) and then press OK.

Important:
Always make a backup of lockngo.exe file before running any command line actions. Doing so will enable you to keep a clean copy of Lockngo for future use, or for going back to factory settings.
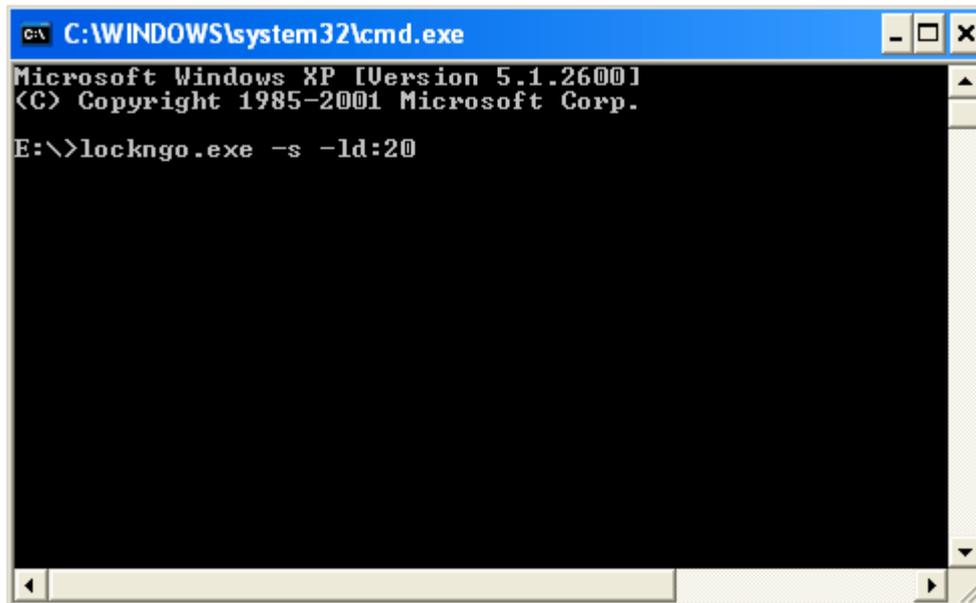

Figure 9: The command line

3.4.3. 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. To store your choices in Lockngo, please use the storing action parameters option.

3.4.3.1. Available parameters

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

3.4.3.2. 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>

3.4.4. Changing and storing parameters from command line

This option allows you to set different options that you would like to store inside the lockngo file for future use. This is a handy and powerful option to simplify the day-to-day use of Lockngo.

Important:
Make a backup of lockngo.exe file before running command line actions on it so that you will have a clean copy of Lockngo for future use

Keynesis Ltd.
www.keynesis.com

3.4.4.1. Available parameters

Flag	Mandatory	Description
-s	★	This flag tells Lockngo that it should store the command line parameters inside the lockngo.exe file for future use.
-dap		Enable 'Do not ask for password when locking disk'.
-per		This flag makes the chosen parameters permanent. Once this flag is used, Lockngo cannot accept future command line parameters. If this flag is chosen, the flag –dap will be also turned on by default. **Important**: Make a backup of lockngo.exe file before running this option so that you will have a copy of Lockngo for future use without permanent settings
-ld:<minutes>		Change delay for Auto – locking function. Default value – 10 minutes; To disable auto- locking set this value to 0; Maximum value – 720 minutes (12 hours)
-reset		Reset previously used parameters to factory settings (will not work if '–per' flag was used)
-p:<password>	★	This flag is the password flag and therefore mandatory (cannot be empty).

3.4.4.2. Examples of use

<u>Example</u>: Bypass lock window (lock without 'entire drive encryption').

Lockngo.exe –s –dap –p:1234

<u>Result</u>: when Lockngo will be executed next time (double-click on file) it will 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 '<u>locking</u>' 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.

<u>Example</u>: Disable auto-locking by idle time.

Lockngo.exe –s –ld:0

<u>Result</u>: auto-locking function will be disabled.

Keynesis Ltd.
www.keynesis.com

Example: Change default delay of auto-locking function to one hour.

Lockngo.exe –s –ld:60

Result: Disk will be locked automatically if you don't use computer during one hour.

Example: Bypass lock window and set current parameters permanent.

Lockngo.exe –s –per –p:1234

Result: when Lockngo will be executed next time (double-click on file) it will immediately lock the portable drive with the password '1234' without asking the user for any input and without showing the Lockngo user interface. Notice that the '-dap' (do not ask for password) was not used – this is because when the '-per' option is used the 'do not ask for password' is the default value. 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. No future command line actions can be sent to Lockngo after using this parameter. Lockngo will refuse to accept new parameters. This is handy when you wish to prevent anyone from changing the password or accessing the Lockngo lock user interface. The only way to enable command line again is to use the original saved backup copy of the lockngo.exe file.

Example: Reset previously used parameters to factory settings.

Lockngo.exe –s –reset

Result: when Lockngo will be executed next time it will return to its default factory settings.

* Notice that the '-reset' option (will not work if '–per' flag was used.

Keynesis Ltd.
www.keynesis.com

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.