

EasyLock™

User Manual



**Encryption Application for
portable Storage Devices**

User Manual Version 1.0.0.4

© 2004-2009 CoSoSys Ltd.

Table of Contents

Table of Contents	2
1. Introduction	3
2. System Requirements.....	4
3. Installation	5
4. Working with EasyLock	6
4.1. Setting up EasyLock	6
4.2. Setting up a Password	6
4.3. Password retries	9
4.4. Using Drag & Drop to copy files	9
4.5. Opening and modifying files within EasyLock	12
4.6. Security settings.....	12
5. TrustedDevice Levels	14
6. How EasyLock works with Endpoint Protector 2008	15
7. Configuring TrustedDevice use in Endpoint Protector 2008.....	17
8. Safely Remove Hardware.....	18
9. Support.....	19
10. Important Notice / Disclaimer	20

1. Introduction

Protecting data in transit is essential to ensure no third party has access to data in case a device is lost, misplaced or stolen. EasyLock allows portable devices to be identified as TrustedDevices (in combination with Endpoint Protector 2008) and protects data on the device with Government-approved 256bit AES CBC-mode encryption.

With the intuitive Drag & Drop interface, files can be quickly copied to and from the device for fast, secure and efficient workflow.

EasyLock is a portable application that does not require any installation process on the host PC and is always portable. Wherever the portable storage device goes EasyLock is saved on the device and can be used on any Windows XP and Windows Vista PC.

2. System Requirements

Operating Systems:

- Windows 2000 (Service Pack 4)
- Windows XP (Service Pack 2 is recommended)
- Windows Vista (all Versions)

Available USB port

Removable USB Storage Device to start the application from (e.g. USB Flash Drive, External Hard Drive, Memory Card).

If the portable storage device has a manual write protection switch (lock), it must be in the unprotected (writable) position to be able to use EasyLock.

EasyLock does not require Administrative rights.

3. Installation

To install EasyLock on a USB flash drive (or other portable USB storage device), simply copy the file "EasyLock.exe" to the root folder of a partition associated with that device.

If EasyLock is used in combination with Endpoint Protector 2008, access to TrustedDevices can be configured from the Global Rights module of Endpoint Protector 2008, under the Rights tab.

4. Working with EasyLock

4.1. Setting up EasyLock

To start EasyLock simply double-click the EasyLock.exe that is saved in the root folder of the portable storage device.

When using the portable storage device as a TrustedDevices in combination with Endpoint Protector the Client PC that the device is connected to must have received authorization from the Endpoint Protector 2008 server, otherwise the device will not be accessible on an Endpoint Protector protected PC or EasyLock will not autostart.

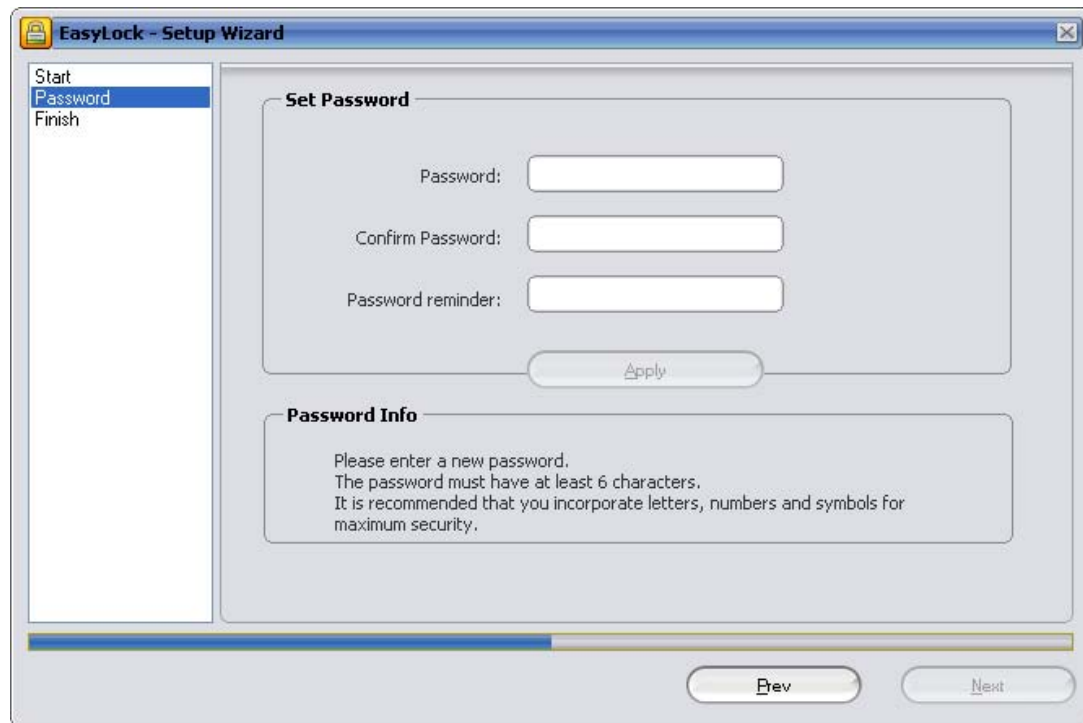
4.2. Setting up a Password

In order to secure (encrypt) your data, you will need to set up a password. The password must be at least 6 (six) characters long.

For security reasons, it is recommended that you incorporate letters, numbers and symbols into your password.



Click “Next” to proceed.



The screenshot shows the 'EasyLock - Setup Wizard' window. On the left, a vertical list contains 'Start', 'Password' (highlighted), and 'Finish'. The main area is titled 'Set Password' and contains three input fields: 'Password:', 'Confirm Password:', and 'Password reminder:'. Below these fields is an 'Apply' button. Underneath the 'Set Password' section is a 'Password Info' box with the following text: 'Please enter a new password. The password must have at least 6 characters. It is recommended that you incorporate letters, numbers and symbols for maximum security.' At the bottom of the window, there are 'Prev' and 'Next' buttons. A progress bar is visible above these buttons, showing the current step is 'Password'.

Enter your password, and then confirm it.

It is recommended that you also set up a password reminder that will help you in case you forget your password.

EasyLock - Setup Wizard

Start
Password
Finish

Set Password

Password:

Confirm Password:

Password reminder:

Password Info

Ready to proceed! Push <Apply> when ready.

EasyLock - Setup Wizard

Start
Password
Finish

Your security parameters are configured successfully!

To complete the Setup Wizard and begin using EasyLock, please press the <Finish> button below.

Thank You,
-Team CoSoSys



Easy Lock



Click "Finish" to continue.

4.3. Password retries

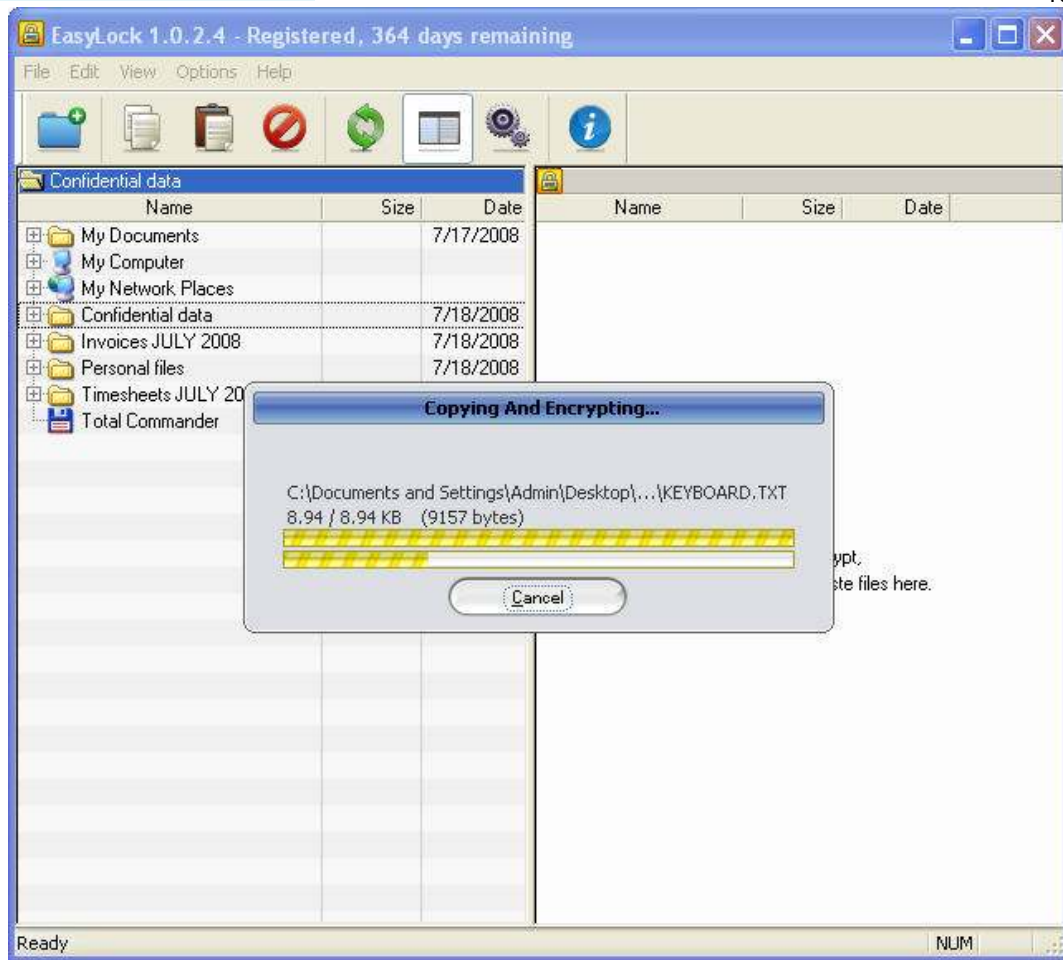
Each time the application starts, you will be asked, for security reasons, to introduce your password.

For that case that your drive was lost or stolen the number of password retries is limited to 10 (ten). After the password has been entered wrongly 10 (ten) times in a row, EasyLock will safely erase all encrypted files stored on the portable storage device.

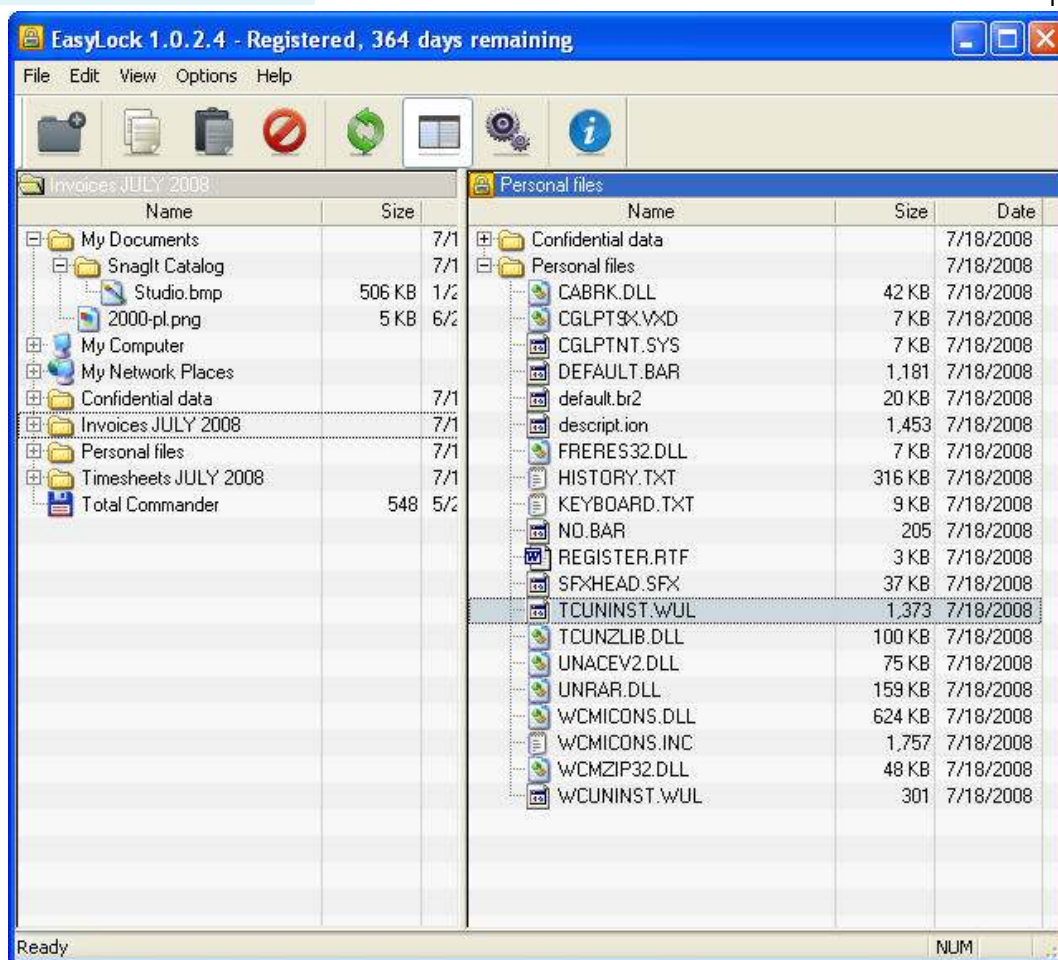
The data on the portable storage device can thereafter not be recovered or recreated. It is permanently erased.

4.4. Using Drag & Drop to copy files

A key feature of EasyLock is the Drag & Drop functionality which allows you to simply drag the file(s) and/or folder(s) that you want to copy on the device and drop them onto the window of EasyLock. These files will be automatically encrypted, ensuring that your data stay safe and private.



The file encryption and transfer status can be seen with the help of the progress bar. When the bar reaches the end, your files have been copied and encrypted.



You can navigate through your encrypted files if you are using Windows Explorer. Clicking on an item with the right mouse button will give you access to options such as “Refresh”, “Copy” and “Delete”.

Copying files from your HDD to the portable storage device using Explorer is **not recommended!**

We recommend using either the Drag & Drop feature or the shortcut keys for copying and pasting, Ctrl+C and Ctrl+V to transfer data to your portable storage device through the EasyLock interface.

In the toolbar area of EasyLock you can find additional icons that you can also use to copy and encrypt your files.



Note that the files on your portable storage device are not visible after encryption, unless EasyLock is running.

To exit EasyLock, select the File menu and choose Exit, or simply click the “X” button in the upper-right corner of the application window.

4.5. *Opening and modifying files within EasyLock*

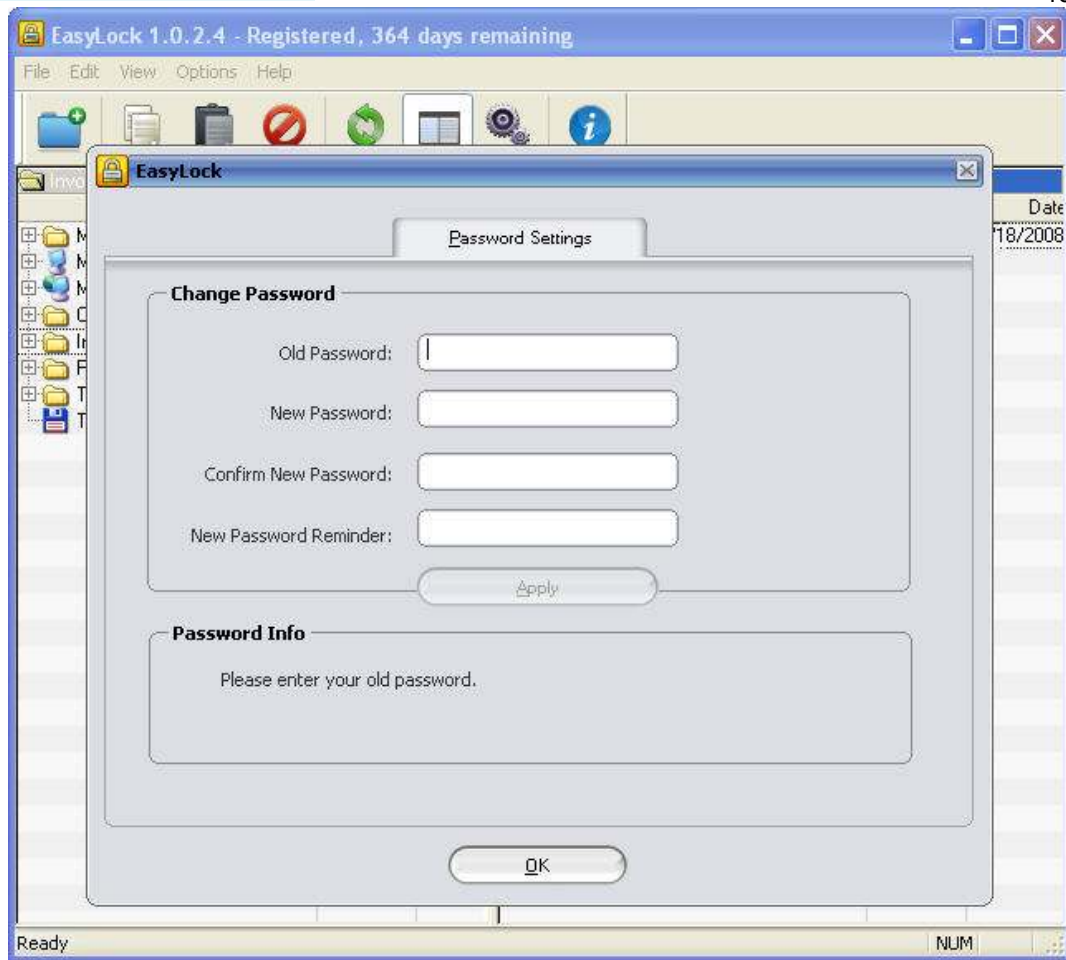
Copied data on device can be viewed and edited directly from within EasyLock. This function is accessible with the “Open” command or double clicking the desired file.

The user has to open documents from the device with the associated application. EasyLock will try to close these documents once it has exited. If a document is modified (saved with the same name or even to the same folder) it will be encrypted and stored on the device. If a document is modified and saved but fails to be encrypted, for example when the device is unexpectedly removed, it will be encrypted the next time EasyLock is started.

! Attention! When EasyLock is started by Endpoint Protector as a trusted application, opening documents from the device option is disabled as the associated application does not have access to the files.

4.6. *Security settings*

The security settings can be modified from within EasyLock. After logging in, you can modify your password. To do this you need to access the security settings menu. This can be done by either selecting Options->Security Settings from the toolbar area or by pressing the hotkey Ctrl + O.



5. TrustedDevice Levels

There are four levels of security for TrustedDevices:

- Level 1 - Minimum security for office and personal use with a focus on software based encryption for data security. Offers companies already regulatory compliance.

Any USB Flash Drive and most other portable storage devices can be turned into a TrustedDevice Level 1 with EasyLock Software from CoSoSys.

No hardware upgrade is required.
- Level 2 - Medium security level with biometric data protection or advances software based data encryption.

Requires special hardware that includes security software and that has been tested for TrustedDevice Level 2.

Hardware is widely available in retail stores.
- Level 3 - High security level with strong hardware based encryption that is mandatory for sensitive enterprise data protection for regulatory compliance such as SOX, HIPAA, GBLA, PIPED, Basel II, DPA, or PCI 95/46/EC.

Requires special hardware that includes advanced security software and hardware based encryption and that has been tested for TrustedDevice Level 3.
- Level 4 - Maximum security for military, government and even secret agent use. Level 4 TrustedDevices include strong hardware based encryption for data protection and are independently certified (e.g. FIPS 140). These devices have successfully undergone rigorous testing for software and hardware.

Requires special hardware that is available primarily through security focused resellers.

6. How EasyLock works with Endpoint Protector 2008

When using EasyLock on a portable storage device as a TrustedDevice Level 1, in combination with Endpoint Protector 2008 will ensure that all data copied from an Endpoint Protector secured Client PC to the device will be encrypted.

Normal Scenario for the use of a TrustedDevice Level 1 is.

1. User connects device to Endpoint Protector protected Client PC.
2. Device is checked for authorization (client PC is communicating with Endpoint Protector Server to check for authorization).
3. If device is an authorized TrustedDevice Level 1 and the User or Machine is authorized to use TrustedDevice Level 1, the EasyLock software on the device will automatically open.
4. User can transfer files via Drag & Drop in EasyLock.
5. Data transferred to the devices is encrypted via 256bit AES.
6. User cannot access the device directly using Windows Explorer or similar applications (e.g. Total Commander) to ensure that no data is copied on the portable device without being properly encrypted.
7. User does not have the possibility to copy data in unencrypted state to the TrustedDevice (on an Endpoint Protector client PC).
8. All file transfer from an Endpoint Protector client PC to the device can be recorded if file tracing and file shadowing are activated in Endpoint Protector. Actions such as file deletion or file renaming are also recorded.
9. Administrators can later audit what user, with what device, on what PC, has transferred what files.

If a TrustedDevice fails to get authorization from Endpoint Protector 2008 it will not be usable by the user. The device will be blocked and the user will not be able to access the device.

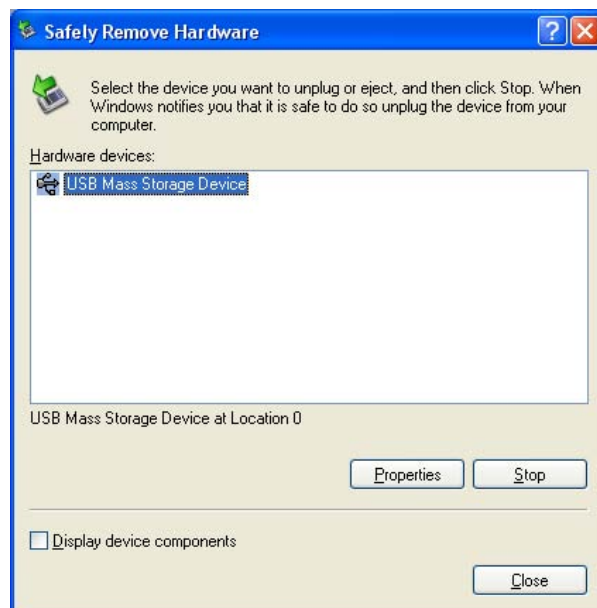
7. Configuring TrustedDevice use in Endpoint Protector 2008

To learn how to configure the use of TrustedDevice in combination with Endpoint Protector please consult the Endpoint Protector 2008 User Manual.

8. Safely Remove Hardware

Before you unplug your portable storage device from the USB port of your computer, you have to use the “Safely Remove Hardware” option from the system tray, otherwise you risk corrupting the data on your USB Drive (especially when using Windows 2000).

To Safely Remove Hardware, double-click on the system tray icon, then select the USB Drive you want to remove from the list and click on the “Stop” button.



A message will appear indicating that the portable storage device can now be securely removed. If a message saying “The ‘ ... ’ device cannot be stopped right now” appears, you have to close your Windows Explorer, EasyLock or any other application that is still accessing the data on the USB Drive.

9. Support

In case additional help, such as the FAQs or e-mail support is required, you can visit the support website directly at <http://www.cososys.com/help.html>.

10. Important Notice / Disclaimer

Security safeguards, by their nature, are capable of circumvention. CoSoSys cannot, and does not, guarantee that data or devices will not be accessed by unauthorized persons, and CoSoSys disclaims any warranties to that effect to the fullest extent permitted by law.

© 2004 – 2009 Copyright CoSoSys Ltd; Endpoint Protector, TrustedDevices and EasyLock are trademarks of CoSoSys Ltd. All rights reserved. Windows and .NET Framework are registered trademarks of Microsoft Corporation. All other names and trademarks are property of their respective owners.