EasyLock

User Manual Version 2.0.0.2

User Manual

COSOSYS

Table of Contents

1. Introduction

Protecting data in transit is essential to ensure no third party has access to confidential information. Regardless where the data is stored - saved on USB storage devices, CDs and DVDs or, local folders or, cloud storage solutions – encryption can be the best solution in case a device is lost, misplaced or stolen.

EasyLock is a cross-platform, enterprise-grade, data encryption solution designed to keep confidential data safe. It is suitable for any type of user, from novice to expert, from home users to multinational employees.

There are several EasyLock versions available. Although they are very similar and both offer the same encryption capabilities and ease of use, there are some things to consider when choosing the right version, based on your scenarios.

- **EasyLock** – a stand-alone application that does not require any installation process on computer itself. It protects data on USB storage devices with government-approved 256bit AES CBC-mode encryption. *also available for local folders, CDs & DVDs and cloud storage solutions

  The application also allows USB storage devices to be identified in Endpoint Protector and My Endpoint Protector as TrustedDevices

- **EasyLock Enforced Encryption –** also a stand-alone application, offering the same functionalities for USB storage devices. The difference is that it does require a small installation also on the computer itself.

  The applications also allow USB storage devices to be identified in TrustedDevices 1+. It can only be used in combination with Endpoint Protector as it provides enforce encryption options for any USB storage device that connects to the protected computer and, also remote management of those devices (resetting passwords, sending messages, resetting devices, etc.)

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

2. System Requirements

Both EasyLock and EasyLock Enforced Encryption work on almost any Mac or Windows computers and have a very small footprint.

Supported Operating Systems:

- Starting with Windows XP (with the latest Service Packs and updates) up to the latest versions of Windows 10
- Starting with Mac OS 10.8 up to the latest macOS 10.14 - Mojave

Available USB port

A removable USB storage device to start the application from (e.g. USB Flash Drive, External Hard Drive, Memory Card etc.).

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.

Information
If EasyLock is being used to encrypt local folders, CDs & DVDs or cloud storage applications, the USB port is not required.

3. Deployment

3.1. Download EasyLock

For EasyLock for USB storage devices (or cloud storage, etc.), the software can be downloaded from: https://www.endpointprotector.com/products/easylock.

For EasyLock Enforced Encryption, the software needs to be downloaded from the related Endpoint Protector Server. It is corelated with that particular server and that specific device. For each device, a new installer would need to be downloaded.

Tips

Although the EasyLock Setup will include both the Windows and Mac versions, ensure a proper corelation for the initial deployment phase.

E.g.: if the initial setup will be made on a Windows computer, use the EasyLockSetup.exe

E.g.: if the initial setup will be made on a Mac, use the EasyLockSetup.dmg

Information

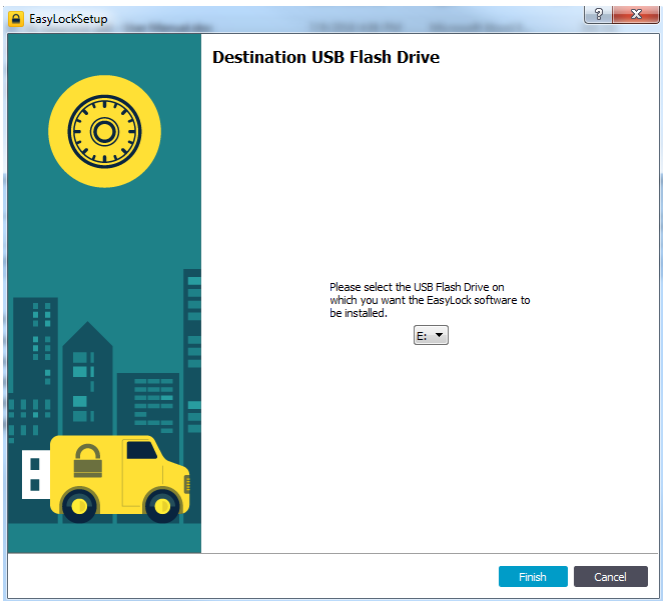
Alternatively, for EasyLock Enforced Encryption, configurations can be made on the Endpoint Protector Server for an automatic deployment. This will eliminate the need to download the installation software.

For more information on EasyLock Enforced Encryption used in correlation with Endpoint Protector, please read the Endpoint Protector User Manual.

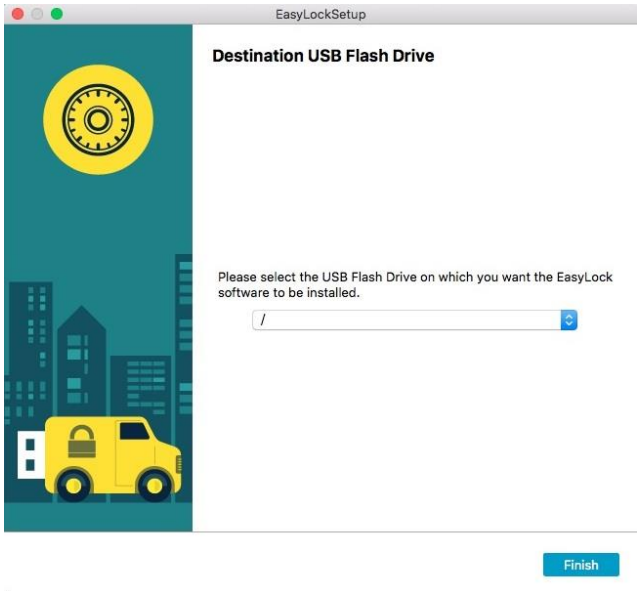
3.2. Install EasyLock on USB storage devices

To install EasyLock on a USB storage device:

- **On Windows**: run the “EasyLockSetup.exe” file, select the drive letter corresponding to the USB device and press Finish. The EasyLock application will be installed automatically in the Root folder of the selected device.



- **On macOS**: run the "EasyLockSetup.dmg" file, select the drive letter corresponding to the USB device and press Finish. The EasyLock application will be installed automatically in the Root folder of the selected device.



3.3. Install EasyLock on Local Folders, Cloud Storage and more

To install EasyLock on CDs & DVDs, local folders or cloud storage solutions, the process is similar with the steps described in paragraph 3.2 Introduction.

The main difference is that the initial location will be a local folder. After the installation, EasyLock can be moved either in the cloud storage solution or, burned on a CD or DVD.

3.4. Install EasyLock Enforced Encryption on USB storage devices

To install EasyLock Enforced Encryption on a USB storage device, the process is similar with the steps described in paragraph 3.2 Introduction.

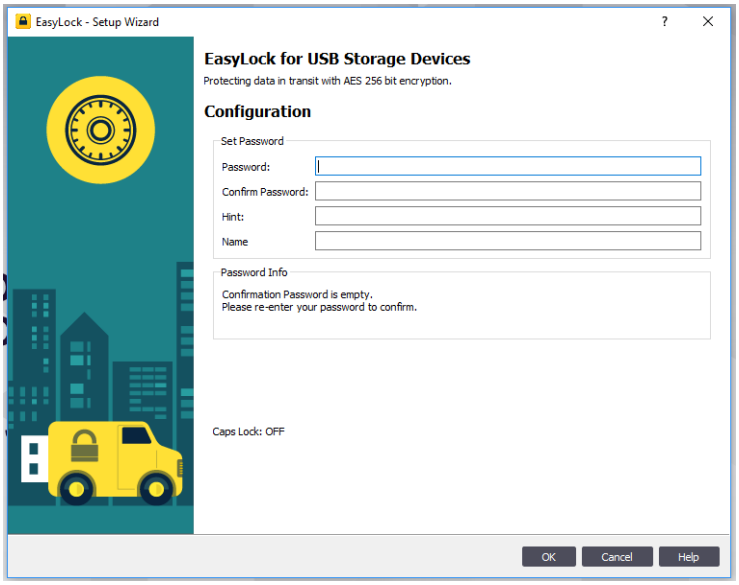
- For automatic deployment, EasyLock will be automatically copied onto the Root of the device
- For manual deployment, EasyLock will have to be copied onto the Root of the device

3.5. Setting up EasyLock (all versions)

Regardless of the EasyLock version (EasyLock Enforced Encryption, EasyLock for USB storage devices, cloud storage, etc.), the main requirement is setting up a password.

The password must be at least 6 characters long. For security reasons, incorporating letters, numbers and symbols is recommended.

It is also recommended to setup a password reminder as there are no other ways to recover the password. CoSoSys does not store any customer data.



Information

For EasyLock Enforced Encryption, the Endpoint Protector Administrator might have additional tools available to help in case a user lost their password. However, this is not always the case as it depends on multiple circumstances.

3.6. Password retries

Each time EasyLock starts, the user will be asked to enter the password. For security reasons, the password retries limit is set to 10. After the password has been entered incorrectly 10 times in a row, all data within EasyLock will be safely erased.

This security measure ensures data protection in case the device is lost or stolen. Therefore, data on the portable storage device cannot be recovered or recreated. It is permanently erased.

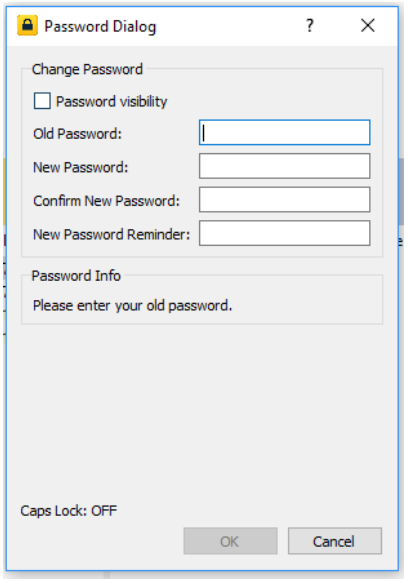
Information

For EasyLock Enforced Encryption, the Endpoint Protector Administrator has the option to customize several password settings. This includes password retries, validity, format, history, etc.

4. Features and functionality

4.1. Password

The password can be changed at any time from within EasyLock, after login. This can be done either from the toolbar area by going to Options > Security Settings or by pressing the hotkey Ctrl + O.

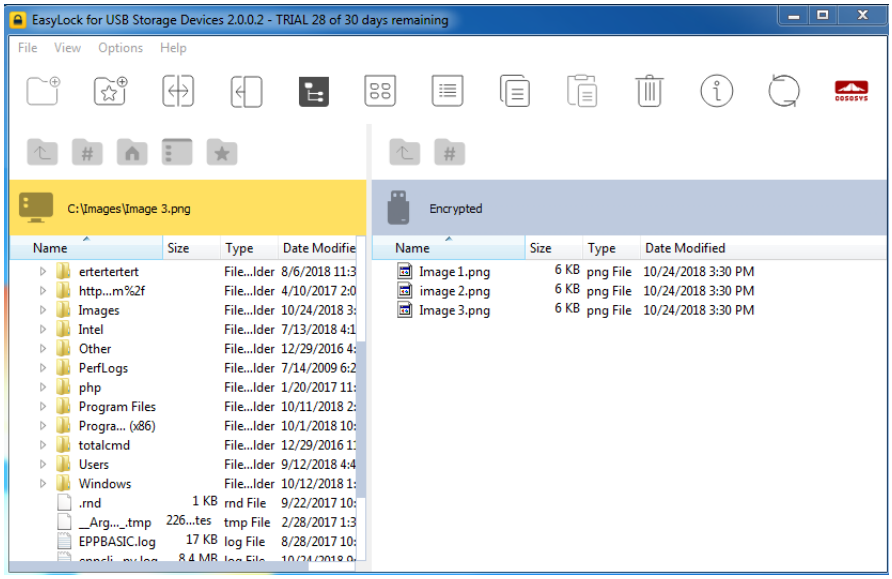


For the EasyLock Enforced Encryption version, this can be changed from Options > Change Password.

4.2. Display Customization

The toolbar area offers several customization options for the EasyLock display windows. The main functionalities are available from the toolbar or from the Main Menu > View section.

By selecting or deselecting them in the View > Toolbar, they can be displayed or hidden in the toolbar.



4.3. Main Functionalities

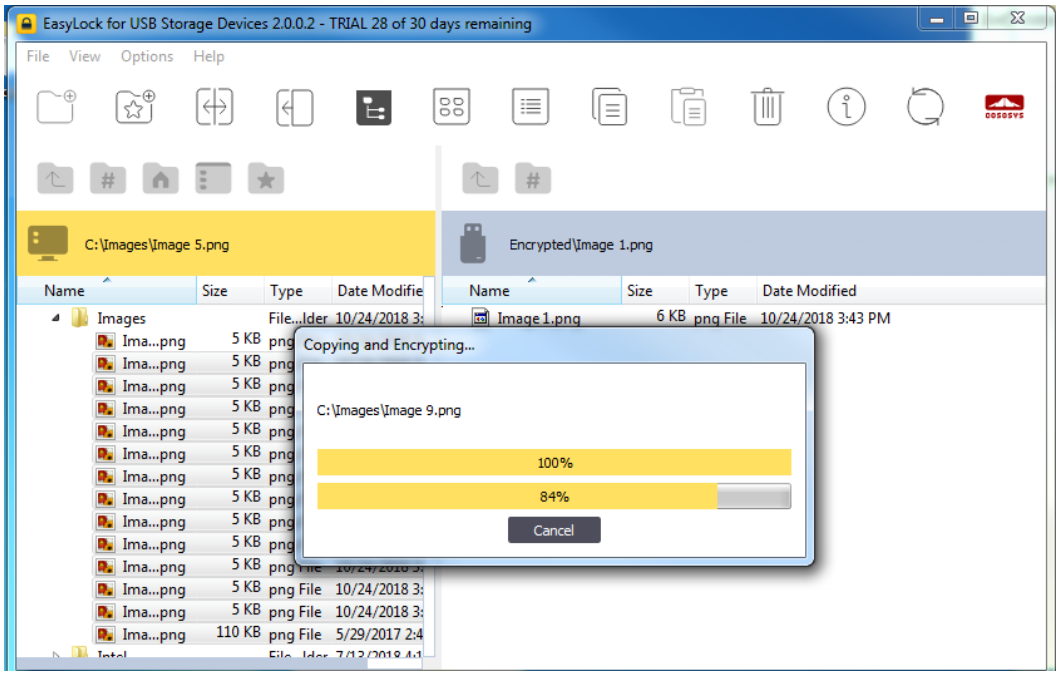
As mentioned above, these can be access either from the toolbar or from the Main Menu > View section.

- **New Folder** – create new directory in the active window
- **Favorites –** manage favorites locations
- **Swap Panels** – interchange the display of the USB Drive and My Computer panels
- **Show or hide My Computer Panel** – display the My Computer Panel
- **Tree View –** display a tree-like structure
- **Detailed View –** show additional information about the files
- **List View –** display the items as a list
- **Copy to Clipboard –** copy content to clipboard
- **Insert Clipboard –** insert the clipboard content
- **Delete –** delete items
- **About–** display information about EasyLock version
- **Refresh–** show additional information about the files

4.4. Drag & Drop Functionalities

The copy & paste or the drag & drop functionalities are available when working with files.

The drag & drop functionality makes working with files and folders as simple as possible. A user only has to drop the desired items that need to be copied on the EasyLock windows and files and folders will be safe and secure.

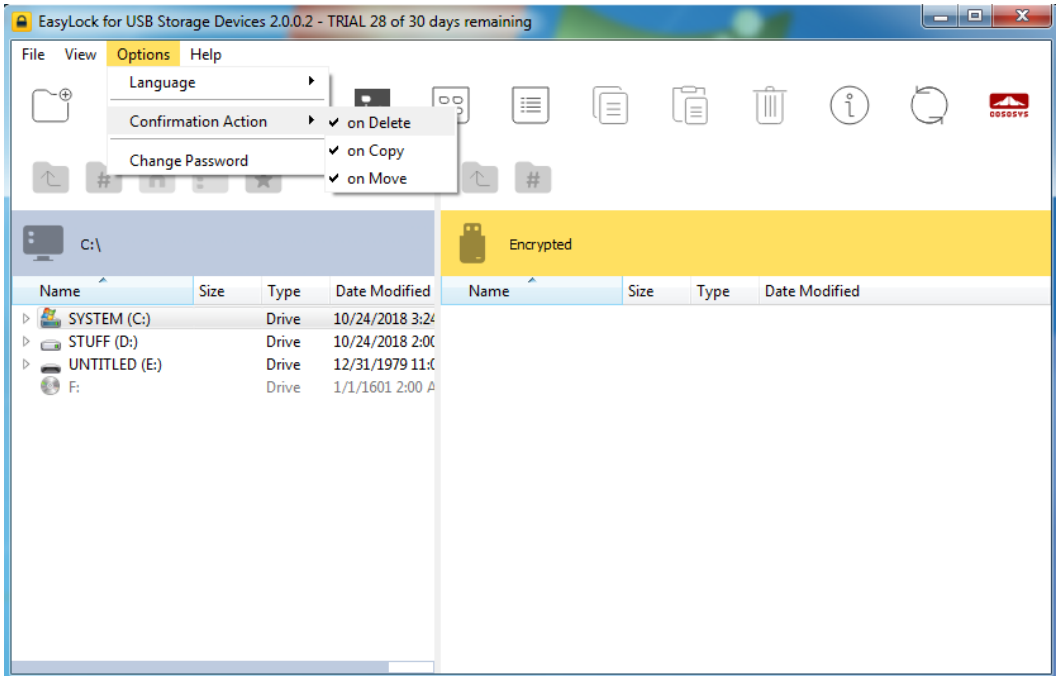


The transfer status is displayed with the help of a progress bar.

4.5. Options section

In addition to changing the password (see paragraph 4.1 Password), this section provides the option to change the Language of the User Interface, as well as some other Preferences.

The Preferences settings allow for confirmation messages for actions such as Delete, Copy or Move to be displayed or disabled. In the Enforced Encryption version, this section is called Confirmation Action.



4.6. Opening and modifying files

Data can be viewed and edited directly from within the application. EasyLock will try to close these documents once they are closed by the user. If a document was modified (saved with the same name or even to the same folder) it will be encrypted. If a document is modified and saved but fails to be encrypted (e.g.: the USB device is unexpectedly removed) it will be encrypted the next time EasyLock is started.

For the EasyLock Enforced Encryption version, data cannot be viewed or edited directly within the application. The desired documents will need to be copied from EasyLock onto a different location (e.g.: user's desktop) in order to be modified.

Tips

Data can be viewed or edited directly from the EasyLock application. EasyLock remains locked while files within encrypted area are accessed.

5. Endpoint Protector and EasyLock

Both the stand-alone EasyLock for USB storage devices and the EasyLock Enforced Encryption versions can be used in combination with Endpoint Protector, turning any USB storage device into a TrustedDevice Level 1.

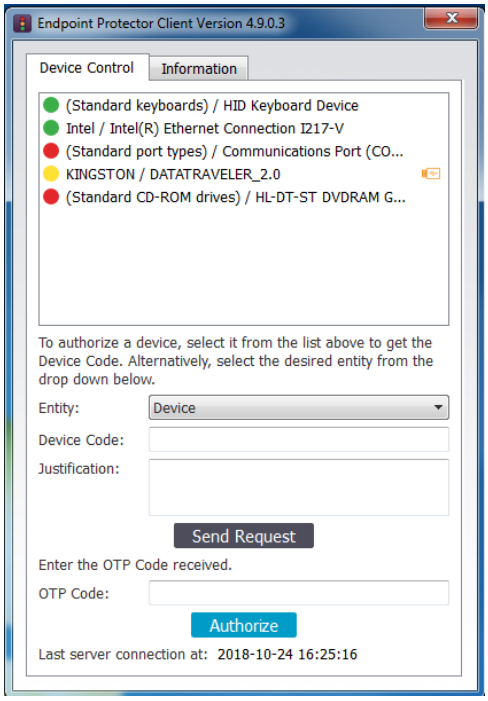
Endpoint Protector is a server-client Data Loss Prevention solution. Its Device Control module offers monitoring and control of USB and peripheral ports.

A typical scenario would imply deploying the Endpoint Protector Client on an endpoint. To avoid data loss or data theft, device rights will be configured to block any USB storage device. However, if EasyLock is present on that specific device, access to it would be allowed as any copied documents would be encrypted and secured.

The TrustedDevice Level 1 implies that the EasyLock application has to be preinstalled on a USB storage device in order to be allowed through Endpoint Protector.

The TrustedDevice Level 1+ implies that EasyLock Enforced Encryption is also activated and licensed through Endpoint Protector. In this situation, EasyLock can be deployed automatically on any USB storage device that connects to the protected endpoint (if not otherwise specified).

The TD Level1 +, otherwise Read Only access right is also available. The USB storage device is on Read-Only and EasyLock Enforced Encryption can be automatically deployed from the Endpoint Protector Client. The deployment can be done by pressing the yellow device icon that is allocated to the USB device in the Endpoint Protector Client.



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

Tips

The TrustedDevice Level 1 is also available within My Endpoint Protector. Therefore the EasyLock for USB storage devices can also be used in cobination with the SaaS version of our DLP solution.

5.1. File Tracing on EasyLock TrustedDevices

File Tracing on EasyLock TrustedDevices allows monitoring of files copied onto the encrypted USB device.

By activating the File Tracing option, all data transferred to and from devices using EasyLock is recorded and logged for later auditing. The logged information is automatically sent to the Endpoint Protector Server (if Endpoint Protector Client is present on that computer and there is a working Internet connection).

In case the Endpoint Protector Client is not present, the information is stored locally in an encrypted format on the device. It will be sent to the Endpoint Protector Server at a later time when, the device is connected to a protected computer, with a working internet connection.

On another hand, the EasyLock Enforced Encryption version can be configured to only work on computers where the Endpoint Protector Client is present. If the Client is not detected, EasyLock cannot be opened.

5.2. Master Password

A Master Password can be configured from within the Endpoint Protector Server. This allows the Administrators to gain access to the EasyLock device in unique circumstances (e.g.: the employee left the company and data needs to be recovered from the device).

The complexity of the Master Password is configurable and includes several settings like length, special characters, upper- and lower-case characters, validity, history, etc.

Tips

The same complex password settings are also available for the user password. These can be enforced by the Endpoint Protector administrators to ensure compliance with the internal security policies.

5.3. Endpoint Protector Client presence required

For extra security measures, EasyLock Enforced Encryption can be restricted to be used only on computers where the Endpoint Protector Client is installed.

There is also the option to extend this functionality to include a list of other trusted Endpoint Protector Servers.

6. Support

Additional support resources are available. Please visit our website for more manuals, FAQs, videos and tutorials and more at: www.endpointprotector.com/resoruces.

For more details about EasyLock, Enforced Encryption, TrustedDevices and Endpoint Protector, please contact your Endpoint Protector Representative.

7. 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.