



EasyLock

User Manual Version 2.0.0.0

User Manual



Table of Contents

1. Introduction	1
2. System Requirements	2
3. Installation	3
3.1. Setting up EasyLock	6
3.2. Setting up a Password	7
3.3. Password retries	9
3.4. Display Settings	9
3.5. Using Drag & Drop to copy files	10
3.6. Opening and modifying files within EasyLock	12
3.7. Security settings	13
4. How EasyLock works with EPP or MyEPP ...	14
4.1. File Tracing on EasyLock TrustedDevices	15
5. Configuring TrustedDevice use in EPP or MyEPP	16
6. Safely Remove Hardware	17
7. Support	19
8. 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) 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, MAC or Linux computer.

2. System Requirements

Operating Systems:

- Windows 7 (all versions)
- Windows Vista (all versions)
- Windows XP (Service Pack 2 is recommended)
- Mac OS 10.5 or higher
- Linux - openSUSE 11.2 (other distributions may be available on demand)

Available USB port

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

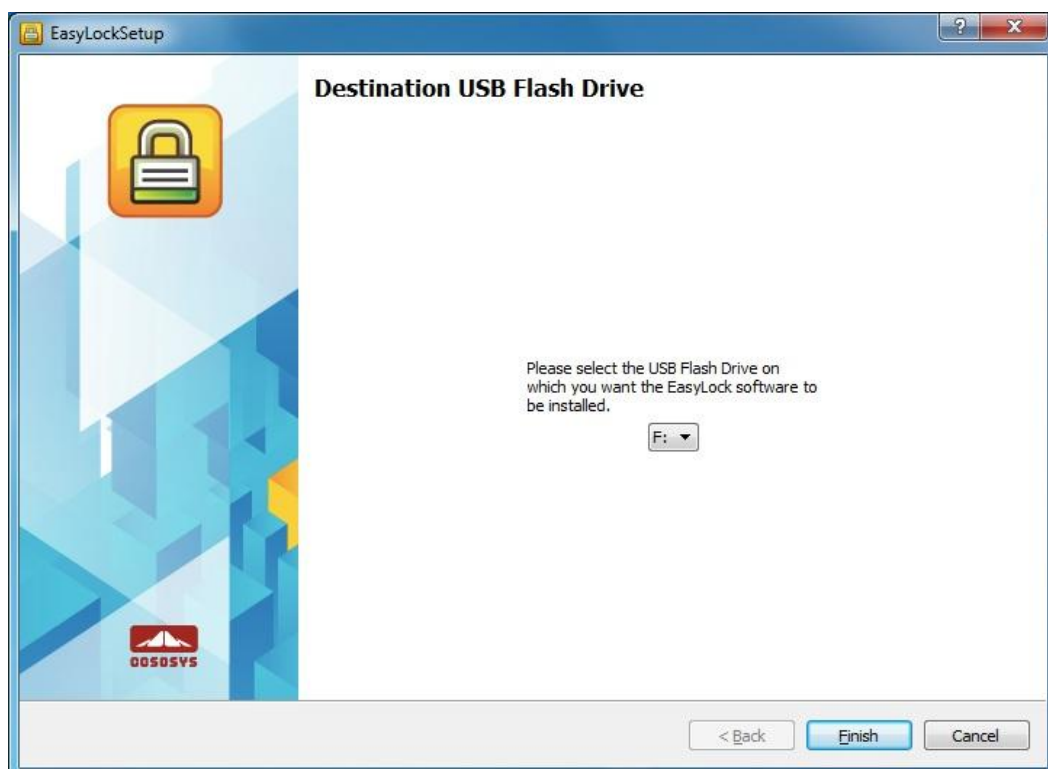
If the portable storage device has a manual write protection switch (lock), it must be in the unprotected (writable) position to be able to use EasyLock.

EasyLock does not require Administrative rights

3. Installation

To install EasyLock on a USB flash drive (or other portable USB storage device):

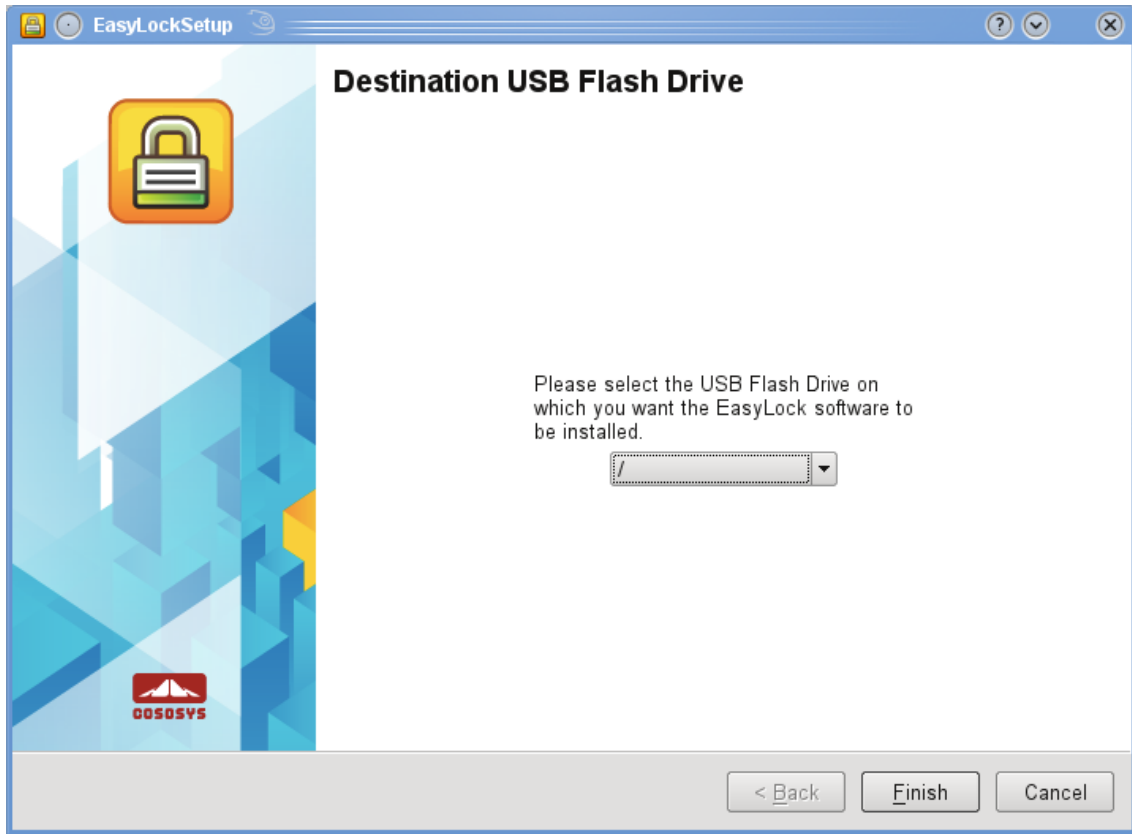
- **On Windows OS:** run the "EasyLockSetup.exe" file, select the drive letter corresponding to the USB device and press <Finish>. The EasyLock application will automatically be installed in the Root folder of the selected device.



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



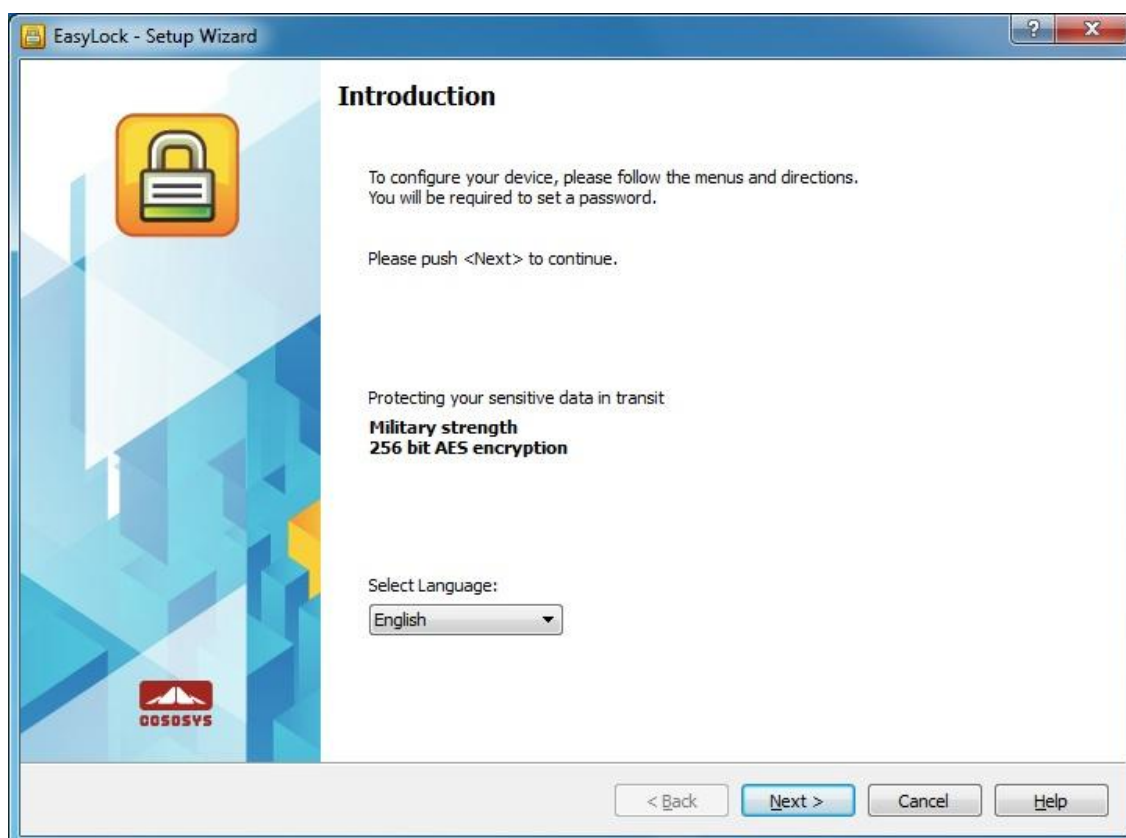
- **On Linux OS:** run the EasyLockSetup file, select the drive letter corresponding to the USB device and press <Finish>. The EasyLock application will automatically be installed in the Root folder of the selected device.



3.1. Setting up EasyLock

To start EasyLock simply double-click the EasyLock file 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 to which the device is connected must have received authorization from the Endpoint Protector server, otherwise the device will not be accessible on an Endpoint Protector protected PC or EasyLock will not autostart.



3.2. 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.



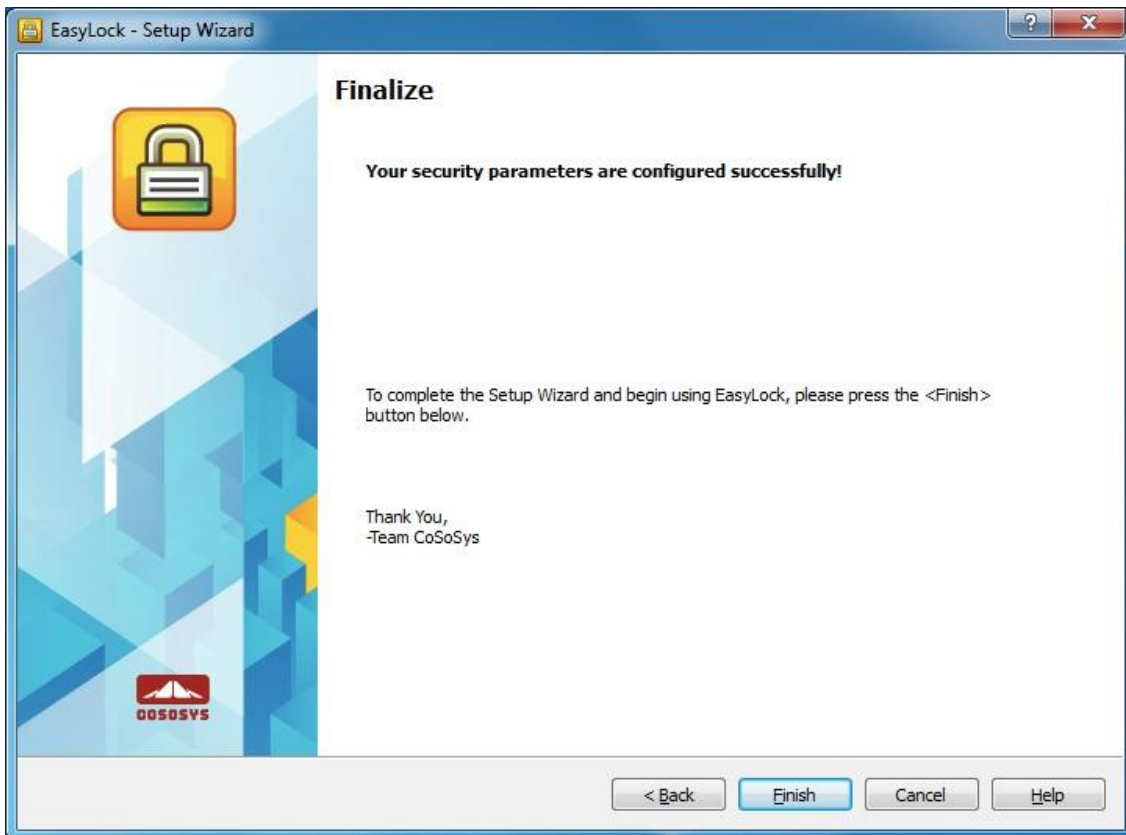
Enter your password, and then confirm it.

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

Click "Next" to continue.



Click "Finish" to complete the password settings and start using the application.



3.3. 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.

3.4. Display Settings

In the toolbar area of EasyLock there are several options available for customizing the EasyLock display window.



Swap Panels – to interchange the display of the USB Drive and My Computer panels

Show or hide My Computer Panel – to display the My Computer Panel

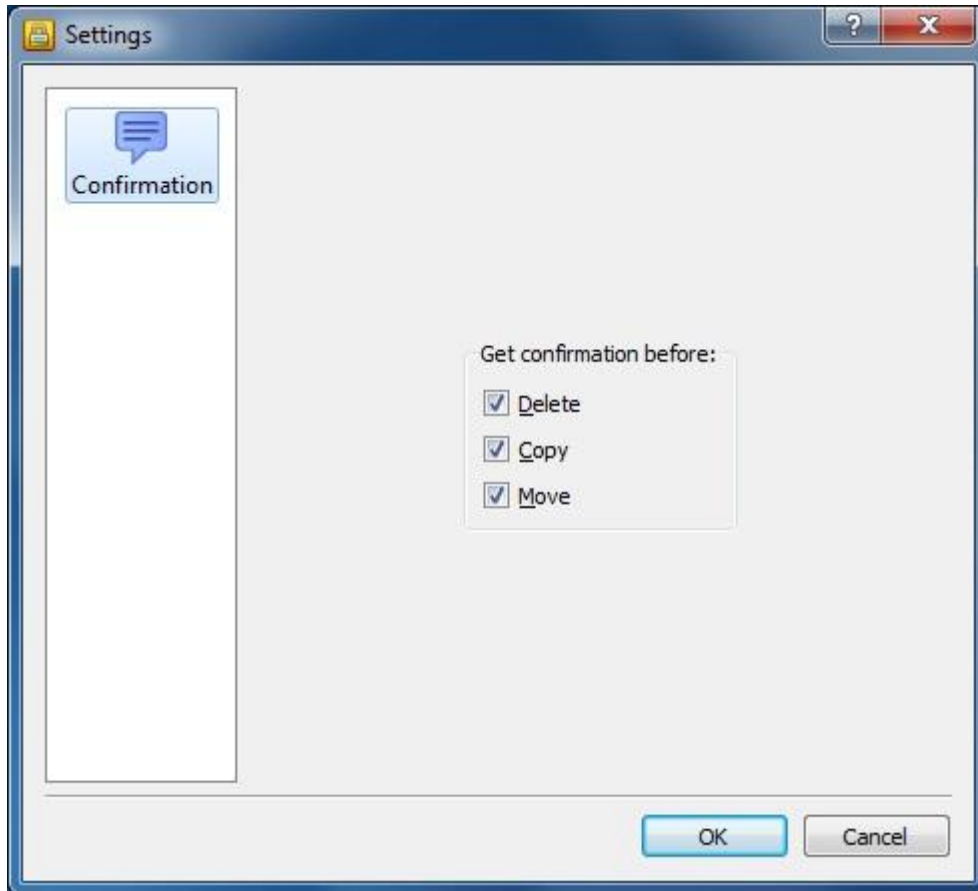
Show Tree View – to display a tree-like structure

Show Detailed View – to show additional information about the files

Show List View – to display the items as a list

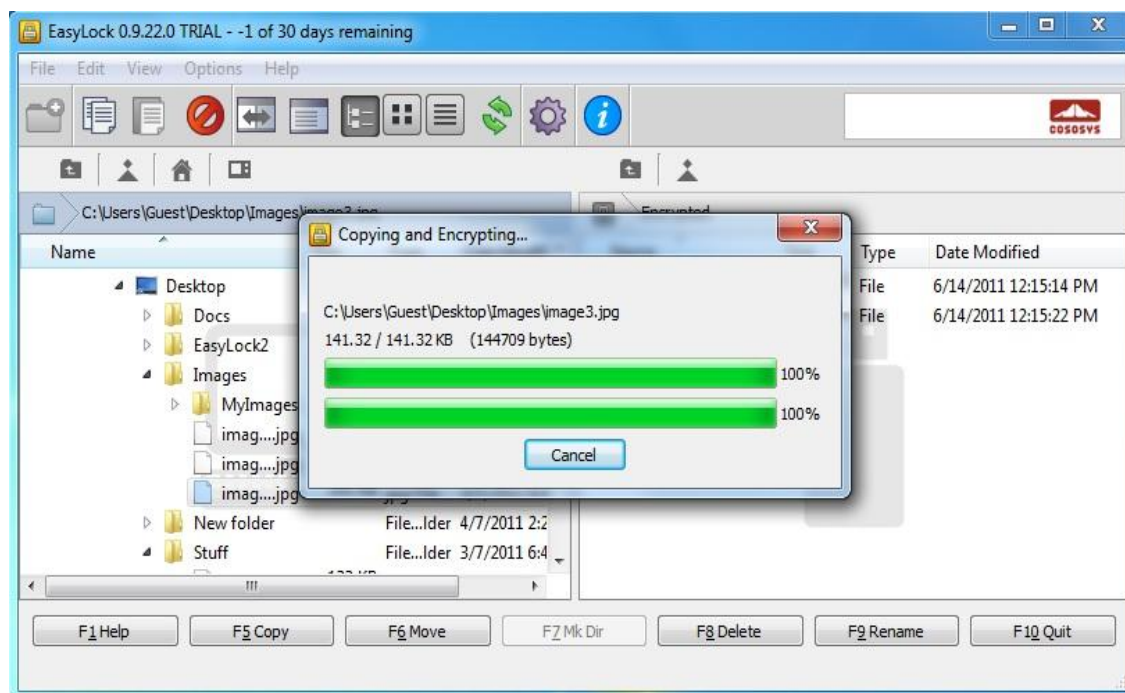
The available options can be selected also directly from the main menu, under the View section.

A new option, Preferences, allows you to select whether you want to have a confirmation message displayed before deleting, copying or moving files.

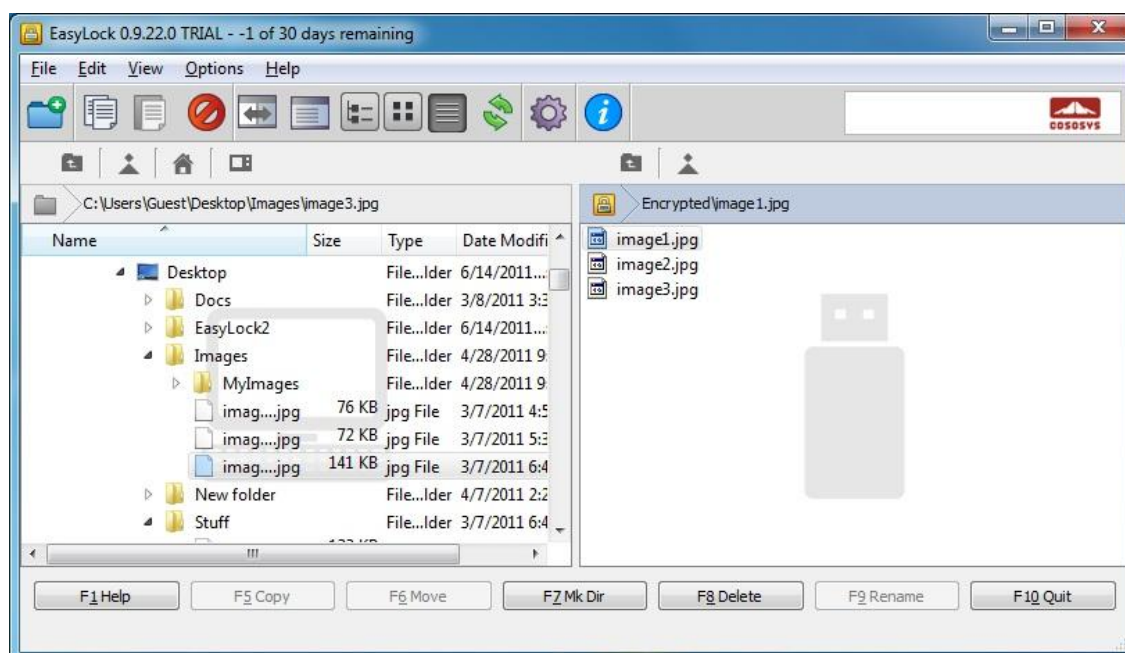


3.5. Using Drag & Drop to copy files

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.



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.

3.6. 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

3.7. 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.



4. How EasyLock works with EPP or MyEPP

When using EasyLock on a portable storage device as a TrustedDevice Level 1, in combination with Endpoint Protector (or My Endpoint Protector the hosted SaaS Solution) it 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 it will not be usable by the user. The device will be blocked and the user will not be able to access the device.

4.1. File Tracing on EasyLock TrustedDevices

File Tracing on EasyLock TrustedDevices is a new feature of Endpoint Protector 4 used in combination with EasyLock that allows monitoring of files copied in an encrypted way on portable devices.

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 Endpoint Protector Server if Endpoint Protector Client is present on that computer and there is a working Internet connection.

In case that Endpoint Protector Client is not present, the information is stored locally in an encrypted format on the device and it will be sent at a later time from any other computer with Endpoint Protector Client installed.

For more details on activating and using File Tracing on EasyLock TrustedDevices, please consult the Endpoint Protector 4 User Manual.

Note

The File Tracing feature on EasyLock TrustedDevices is available at the moment only for Windows OS.

5. Configuring TrustedDevice use in EPP or MyEPP

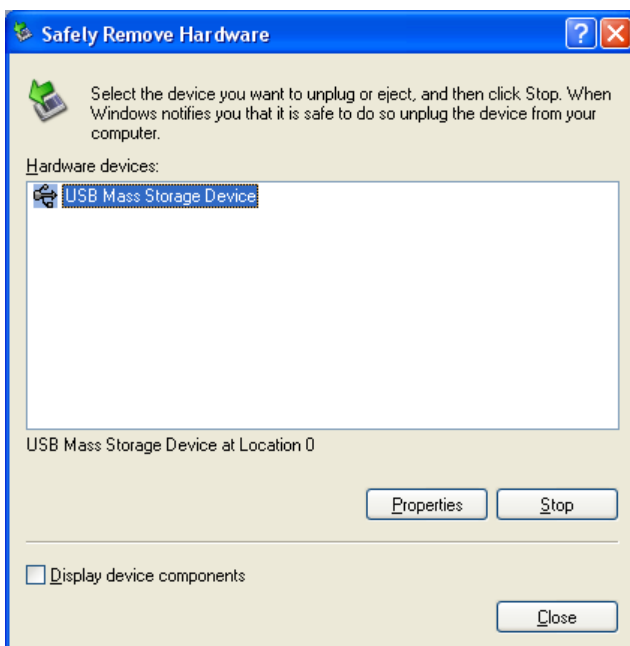
To learn how to configure the use of TrustedDevice in combination with Endpoint Protector please consult the Endpoint Protector User Manual.

To find out more about Endpoint Protector visit: www.EndpointProtector.com

6. 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.

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.

7. 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>

8. 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.